aws

Manual do usuário

EventBridge Agendador

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

EventBridge Agendador: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

O que é o Agendador do EventBridge? 1
Principais características do Agendador do EventBridge 1
Acessando o Agendador do EventBridge 2
Configurar 3
Inscreva-se para AWS 3
Inscreva-se para um Conta da AWS 3
Políticas gerenciadas pelo uso 3
Configurar o perfil de execução 4
Configurar um destino 8
Próximas etapas 11
Introdução 12
Pré-requisitos 13
Utilizar o console 13
Como usar o AWS CLI 17
Usar SDKs da 17
Próximas etapas 19
Tipos de agendamento 20
Rate-based horários 21
Sintaxe 21
Exemplos 21
Cron-based horários 22
Sintaxe 22
Exemplos 23
One-time horários 24
Sintaxe 24
Exemplos 24
Fusos horários 25
Horário de verão 25
Gerenciando um agendamento 27
Alterando o estado do agendamento 28
Configurando janelas de tempo flexíveis 29
Configurar uma DLQ 30
Criar uma fila do Amazon SQS 31
Configure as permissões da função de execução 32

Especificar uma fila de mensagens não entregues ... 33
Recuperar o evento de mensagens não entregues ... 34
Excluir um agendamento. ... 37
Exclusão após a conclusão do agendamento ... 37
Exclusão manual ... 38
Próximas etapas ... 39
Gerenciando um grupo de agendamento ... 40
Criando um grupo de agendamento ... 41
Etapa 1: criar um novo grupo de agendamento ... 41
Associando um agendamento ... 43
Excluindo um grupo de agendamento ... 44
Recursos relacionados ... 46
Gerenciando destinos ... 47
Uso de destinos modelados ... 48
Amazon SQS `SendMessage` ... 49
`Lambda Invoke` ... 51
Funções de Etapa `StartExecution` ... 53
Usando destinos universais ... 55
Ações não compatíveis ... 56
Exemplos ... 57
Adicionando atributos de contexto ... 59
Próximas etapas ... 60
AWS PrivateLink ... 61
Considerações ... 61
Como criar um endpoint de interface ... 61
Criar uma política de endpoint ... 62
Segurança ... 64
Gerenciamento de acesso ... 65
Público ... 65
Autenticação com identidades ... 65
Gerenciar o acesso usando políticas ... 67
Integração com o IAM ... 69
Usar políticas baseadas em identidade ... 74
Prevenção contra representante confuso ... 85
Solução de problemas ... 88
Proteção de dados ... 90

Criptografia em repouso ... 91
Criptografia em trânsito ... 98
Validação de conformidade ... 98
Resiliência ... 99
Segurança da infraestrutura ... 99
Monitoramento e métricas ... 100
Monitoramento com CloudWatch ... 100
Termos ... 101
Dimensões ... 102
Acesso às métricas do ... 102
Lista de métricas ... 103
Métricas de uso ... 109
Monitorar com logs do CloudTrail ... 113
Informações do Agendador do EventBridge no CloudTrail ... 113
Noções básicas sobre as entradas de arquivos de log do Agendador do EventBridge ... 114
Cotas ... 115
Solução de problemas de cotas ... 122
ServiceQuotaExceededException ... 122
Solução de problemas ... 124
Erros de destino ... 124
Causas comuns: ... 124
Etapas de solução de problemas ... 124
Permissões de perfil ... 126
Causas comuns ... 126
Sintomas ... 126
Etapas de solução de problemas ... 126
Cotas de serviço ... 129
Identificar problemas de cota ... 129
Solucionar problemas de cota ... 129
Padrão e tempo de gatilho ... 130
Causas comuns ... 130
Etapas de solução de problemas ... 130
Criação de padrões ... 131
Problemas comuns ... 132
Etapas de solução de problemas ... 132
Meu destino está sendo acionado? ... 132

Destinos modelados versus destinos universais 133
Entrada de destino universal inválida 133
Sintomas 133
Exemplos 134
Como resolver 135
Agendar atualizações acionando invocações inesperadas 135
Desabilitar ou habilitar agendamentos únicos 135
Histórico do documento 137
..... cxli

O que é o Agendador do Amazon EventBridge?

O Agendador do Amazon EventBridge utiliza a tecnologia sem servidor que permite criar, executar e gerenciar tarefas a partir de um serviço central gerenciado. Altamente escalável, o Agendador do EventBridge permite que você agende milhões de tarefas que podem invocar mais de 270 serviços da AWS e mais de 6.000 operações de API. Sem a necessidade de provisionar e gerenciar a infraestrutura ou integrar-se a vários serviços, o Agendador do EventBridge oferece a capacidade de entregar agendamentos em grande escala e reduzir os custos de manutenção.

O Agendador do EventBridge entrega suas tarefas de forma confiável, com mecanismos integrados que ajustam seus agendamentos com base na disponibilidade de metas posteriores. Com o Agendador do EventBridge, você pode criar programações usando expressões cron e rate para padrões recorrentes ou configurar invocações únicas. É possível configurar janelas de tempo flexíveis para entrega, bem como definir limites de repetição e o tempo máximo de retenção para gatilhos com falha.

Tópicos

- Principais características do Agendador do EventBridge
- Acessando o Agendador do EventBridge

Principais características do Agendador do EventBridge

O Agendador do EventBridge oferece os seguintes recursos principais que você pode usar para configurar metas e escalar seus agendamentos:

- Alvos modelados: O Agendador do EventBridge aceita destinos modelados para realizar operações comuns de API usando Amazon SQS, Amazon SNS, Lambda e EventBridge. Com destinos predefinidos, você pode configurar seus agendamentos rapidamente usando o console do Agendador do EventBridge, o Agendador do EventBridge SDK ou a AWS CLI.
- Alvos universais: O Agendador do EventBridge fornece um parâmetro de destino universal (UTP) que você pode usar para criar acionadores personalizados que visam mais de 270 serviços da AWS e mais de 6.000 operações de API em um agendamento. Com o UTP, você pode configurar seus acionadores personalizados usando o console do Agendador do EventBridge, o Agendador do EventBridge SDK ou a AWS CLI.

- Janelas de horário flexíveis: O Agendador do EventBridge aceita janelas de horário flexíveis, permitindo que você disperse seus agendamentos e melhore a confiabilidade de seus gatilhos para casos de uso que não exigem invocação programada precisa de destinos.
- Tentativas repetidas: O Agendador do EventBridge fornece pelo menos uma vez a entrega do evento aos destinos, o que significa que pelo menos uma entrega é bem-sucedida com uma resposta do destino. O Agendador do EventBridge permite que você defina o número de novas tentativas para seu agendamento para uma tarefa com falha. O Agendador do EventBridge repete tarefas que falharam com tentativas atrasadas para melhorar a confiabilidade de seu agendamento e garantir que as metas estejam disponíveis.

Acessando o Agendador do EventBridge

Você pode usar o Agendador do EventBridge por meio do console do EventBridge, do SDK do Agendador do EventBridge, do AWS CLI ou usando diretamente a API do Agendador do EventBridge.

Configurando o Amazon EventBridge Scheduler

Antes de usar o EventBridge Scheduler, você deve concluir as etapas a seguir.

Tópicos

- Inscreva-se para AWS
- Políticas gerenciadas pelo uso
- Configurar o perfil de execução
- Configurar um destino
- Próximas etapas

Inscreva-se para AWS

Inscreva-se para um Conta da AWS

Para começar AWS, você precisa de um Conta da AWS. Para obter informações sobre como criar um Conta da AWS, consulte Introdução a um Conta da AWS no Guia de AWS Gerenciamento de contas referência.

Políticas gerenciadas pelo uso

Depois de configurar sua AWS conta e seu usuário administrativo, recomendamos que você crie usuários, grupos ou funções separados apenas com as permissões necessárias para usar o EventBridge Agendador. EventBridge O Scheduler oferece suporte às seguintes políticas gerenciadas para casos de uso comuns.

- AmazonEventBridgeSchedulerFullAccess — Concede acesso total ao EventBridge Scheduler usando o console e a API.
- AmazonEventBridgeSchedulerReadOnlyAccess — Concede acesso somente para leitura ao Scheduler. EventBridge

Você pode anexar essas políticas gerenciadas aos seus diretores do IAM. Para obter mais informações sobre como gerenciar o acesso ao EventBridge Scheduler usando políticas do IAM baseadas em identidade, consulte. the section called “Usar políticas baseadas em identidade”

Configurar o perfil de execução

Uma função de execução é uma função do IAM que o EventBridge Scheduler assume para interagir com outras pessoas Serviços da AWS em seu nome. Você anexa políticas de permissão a essa função para conceder ao EventBridge Agendador acesso para invocar alvos.

Você também pode criar uma nova função de execução ao usar o console para criar uma nova agenda. Se você usa o console, o EventBridge Scheduler cria uma função em seu nome com permissões com base no alvo escolhido. Quando o EventBridge Scheduler cria uma função para você, a política de confiança da função inclui chaves de condição que limitam quais diretores podem assumir a função em seu nome. Isso evita o potencial problema de segurança delegada confusa.

As etapas a seguir descrevem como criar uma nova função de execução e como conceder acesso ao EventBridge Scheduler para invocar um destino. Este tópico descreve as permissões para destinos modelados populares. Para obter informações sobre como adicionar permissões para outros destinos, consulte the section called “Uso de destinos modelados”.

Para criar uma função de execução usando o AWS CLI

1. Copie a seguinte política JSON de assumir a função e salve-a localmente como `Scheduler-Execution-Role.json`. Essa política de confiança permite que o EventBridge Scheduler assuma a função em seu nome.

   JSON

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

> **Important**
>
> Para configurar uma função de execução em um ambiente de produção, recomendamos a implementação de salvaguardas adicionais para evitar problemas de segurança delegada confusa. Para obter mais informações e um exemplo de política, consulte the section called “Prevenção contra representante confuso”.

2. No AWS Command Line Interface (AWS CLI), insira o comando a seguir para criar uma nova função. Substitua *SchedulerExecutionRole* pelo nome que você deseja atribuir a essa função.

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

Se o teste for bem-sucedido, você verá o seguinte resultado:

```
{
    "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. Para criar uma nova política que permita que o EventBridge Scheduler invoque um alvo, escolha um dos seguintes alvos comuns. Copie a política de permissão JSON e salve-a localmente como um arquivo `.json`.

   Amazon SQS – SendMessage

   O seguinte permite que o EventBridge Scheduler chame a `sqs:SendMessage` ação em todas as filas do Amazon SQS em sua conta.

   JSON

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

   Amazon SNS – Publish

   O seguinte permite que o EventBridge Scheduler execute a `sns:Publish` ação em todos os tópicos do Amazon SNS em sua conta.

   JSON

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

```
            "Resource": "*"
        }
    ]
}
```

Lambda – Invoke

O seguinte permite que o EventBridge Scheduler chame a `lambda:InvokeFunction` ação em todas as funções do Lambda em sua conta.

JSON

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

4. Execute o seguinte comando para criar a nova política de permissão: Substitua *PolicyName* pelo nome que você deseja atribuir a essa política.

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

Se for bem-sucedido, você verá o seguinte resultado: Observe o ARN da política. Você usa esse ARN na próxima etapa para anexar a política à nossa função de execução.

```
{
    "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. Para associar a política à sua função de execução, execute o comando a seguir. Substitua *your-policy-arn* pelo ARN da política que você criou na etapa anterior. Substitua *SchedulerExecutionRole* pelo nome da sua função de execução.

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

   A operação `attach-role-policy` não retorna uma resposta na linha de comando.

Configurar um destino

Antes de criar uma agenda do EventBridge Scheduler, você precisa de pelo menos uma meta para sua agenda invocar. Você pode usar um AWS recurso existente ou criar um novo. As etapas a seguir mostram como criar uma nova fila padrão do Amazon SQS com. CloudFormation

Criar uma nova fila do Amazon SQS

1. Copie o CloudFormation modelo JSON a seguir e salve-o localmente como`Scheduler-Target-SQS.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. A partir do AWS CLI, execute o comando a seguir para criar uma CloudFormation pilha a partir do `Scheduler-Target-SQS.json` modelo.

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

Se o teste for bem-sucedido, você verá o seguinte resultado:

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

3. Execute o comando a seguir para ver as informações resumidas da sua CloudFormation pilha. Essas informações incluem o status da pilha e as saídas especificadas no modelo.

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

Se for bem-sucedido, o comando cria a fila Amazon SQS e retorna a seguinte saída:

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

Posteriormente neste guia, você usará o valor de `QueueARN` para configurar a fila como destino para o EventBridge Scheduler.

Próximas etapas

Depois de concluir a etapa de configuração, use o guia de introdução para criar seu primeiro EventBridge agendador do Scheduler e invocar um alvo.

Introdução ao Agendador do EventBridge

Este tópico descreve a criação de um novo agendamento do Agendador do EventBridge. Você usa o console do Agendador do EventBridge, AWS Command Line Interface (AWS CLI) ou AWS SDKs para criar um agendamento com um modelo de destino do Amazon SQS. Em seguida, você configurará o log, configurará novas tentativas e definirá um tempo máximo de retenção para tarefas com falha. Depois de criar o agendamento, você verificará se seu agendamento invoca com sucesso o destino e envia uma mensagem para a fila de destino.

> **Note**
>
> Para seguir esse guia, recomendamos que você configure os usuários do IAM com as permissões mínimas exigidas descritas em the section called “Usar políticas baseadas em identidade”. Depois de criar e configurar um usuário, execute o comando a seguir para definir suas credenciais de acesso. Você precisa de seu ID de chave de acesso da e de uma chave de acesso secreta para configurar a 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
> ```
>
> Para obter mais informações sobre as diferentes maneiras de definir suas credenciais, consulte Configurações e precedência no Guia do usuário da versão 2 do AWS Command Line Interface.

Tópicos

- Pré-requisitos
- Criar um agendamento usando o console do Agendador do EventBridge
- Crie um agendamento usando a AWS CLI
- Criar um agendamento usando os SDKs do Agendador do EventBridge
- Próximas etapas

Pré-requisitos

Antes de executar as etapas nesta seção, você deverá fazer o seguinte:

- Conclua as tarefas descritas em Configurar

Criar um agendamento usando o console do Agendador do EventBridge

Para criar uma nova programação usando o console

1. Faça login no Console de gerenciamento da AWS e, em seguida, escolha o seguinte link para abrir a seção Agendador do EventBridge do console EventBridge: https://us-west-2.console.aws.amazon.com/scheduler/home?region=us-west-2#home

   > **Note**
   >
   > Você pode mudar sua Região da AWS usando o seletor de região do Console de gerenciamento da AWS.

2. Na página Programações, clique em Criar programação.
3. Na página Especificar detalhes da programação, na seção Nome e descrição da programação, faça o seguinte:

   a. Em Nome da programação, insira um nome para a programação. Por exemplo, ., **`MyTestSchedule`**

   b. Para Descrição - opcional, insira uma descrição para a seu agendamento. Por exemplo, **`My first schedule`**.

   c. Para Grupo de agendamento, escolha um grupo de agendamento na lista suspensa. Se você ainda não criou nenhum grupo de agendamento, pode escolher o grupo `default` para sua agenda. Para criar um novo grupo de agendamento, escolha o link criar seu próprio agendamento na descrição do console. Para adicionar tags a grupos de programação, você usa os grupos de programação.
4. Na seção Schedule details (Detalhes do agendamento), faça o seguinte:

a. Em Ocorrência, selecione uma das opções de padrão a seguir. As opções de configuração mudam dependendo do padrão selecionado.

   - Agendamento único: Um agendamento único invoca um destino somente uma vez na data e hora que você especificar.

     Em Data e hora, insira uma data válida no formato `YYYY/MM/DD`. Em seguida, especifique um carimbo de data e hora no formato `hh:mm` de 24 horas. Por fim, escolha um fuso horário nas opções suspensas.
   - Agendamento recorrente: Um agendamento recorrente invoca uma meta em uma taxa que você especifica usando uma expressão cron ou expressão rate.

     Escolha Cronograma baseado em cron para configurar um cronograma usando uma expressão cron. Para usar uma expressão rate, escolha Cronograma baseado em intervalos e insira um número positivo para Valor, depois escolha uma Unidade nas opções da lista suspensa.

   Para obter mais informações sobre o uso de expressões rate e cron, consulte Tipos de agendamento.

b. Para Janela de tempo flexível, escolha Desativado para desativar a opção ou escolher uma das janelas de tempo predefinidas da lista em cascata. Por exemplo, se você escolher 15 minutos e definir uma programação recorrente para invocar o destino uma vez a cada hora, a programação será executada em até 15 minutos após o início de cada hora.

5. Se você escolheu agendamento recorrente na etapa anterior, na seção Prazo, especifique um fuso horário e, opcionalmente, defina uma data e hora de início e uma data e hora de término para o agendamento. Um agendamento recorrente sem data de início começará assim que for criada e disponibilizada. Um agendamento recorrente sem data de término continuará a invocar sua meta indefinidamente.
6. Escolha Próximo.
7. Na página Selecionar destino, faça o seguinte:

   a. Selecione destinos modelados e escolha uma API-destino. Neste exemplo, escolheremos o destino modelado **`SendMessage`** do Amazon SQS.

   b. Na seção SendMessage, para a fila SQS, escolha um ARN de fila existente do Amazon SQS, como `arn:aws:sqs:us-west-2:123456789012:TestQueue` na lista suspensa. Para criar uma nova fila, escolha Criar nova fila SQS para navegar até o console do

Amazon SQS. Depois de terminar de criar uma fila, retorne ao console do Agendador do EventBridge e atualize o menu suspenso. O novo ARN da fila aparece e pode ser selecionado.

c. Em Target, insira a carga útil que você deseja que o Agendador do EventBridge entregue ao destino. Neste exemplo, enviaremos a seguinte mensagem para a fila de destino: **`Hello, it's EventBridge Scheduler.`**

8. Escolha Avançar e, na página Configurações - opcional, faça o seguinte:

9.

a. Na seção Estado do agendamento, em Ativar agendamento, ative ou desative o atributo usando o botão. Por padrão, o Agendador do EventBridge habilita seu agendamento.

b. Na seção Ação após a conclusão do agendamento, configure a ação que o Agendador do EventBridge executará após a conclusão do agendamento:

- Escolha EXCLUIR se quiser que o agendamento seja excluído automaticamente. Para agendamentos únicos, isso ocorre depois que o agendamento invocar o destino uma vez. Para agendamentos recorrentes, isso ocorre após a última invocação planejada do agendamento. Para obter mais informações sobre a exclusão automática, consulte the section called “Exclusão após a conclusão do agendamento”.
- Escolha NENHUM, ou não escolha um valor, se você não quiser que o Agendador do EventBridge execute nenhuma ação após a conclusão do agendamento.

c. Na seção Política de novas tentativas e fila de mensagens não entregues (DLQ), em Política de novas tentativas, ative novas tentativas para configurar uma política de novas tentativas para a seu agendamento. Com as políticas de novas tentativas, se a programação não conseguir invocar o destino, o Agendador do EventBridge tentará executar novamente a programação. Se configurado, você deve definir o tempo máximo de retenção e as novas tentativas da programação.

d. Para Idade máxima do evento - opcional, insira as horas e os minutos máximos que o Agendador do EventBridge deve manter um evento não processado.

> **Note**
>
> O valor máximo é 24 horas.

e. Em Máximo de tentativas, insira o número máximo de vezes que o Agendador do EventBridge tentará executar a programação se o destino retornar um erro.

> **Note**
>
> O valor máximo é 185 tentativas.

f. Para Fila de mensagens não entregues (DLQ), selecione uma das seguintes opções:

- Nenhuma: Escolha essa opção se você não quiser configurar uma DLQ.
- Selecione uma fila do Amazon SQS em minha conta da AWS como DLQ: Escolha essa opção e, em seguida, selecione um ARN de fila na lista suspensa e configure uma DLQ com uma Conta da AWS igual àquela onde você está criando o agendamento.
- Especifique uma fila do Amazon SQS em outra conta da AWS como DLQ: Escolha essa opção e, em seguida, insira o ARN da fila configurada como DLQ, se a fila estiver em outra Conta da AWS. Você deve inserir o ARN exato da fila para usar essa opção.

g. Na seção de Criptografia, selecione Personalizar configurações de criptografia (avançado) para utilizar uma chave de KMS gerenciada pelo cliente para criptografar sua entrada de destino. Se você escolher essa opção, insira uma chave ARN do KMS existente ou escolha Criar uma chave KMS da AWS para navegar para o console do AWS KMS. Para obter mais informações sobre como o Agendador do EventBridge criptografa seus dados em repouso, consulte the section called “Criptografia em repouso”.

h. Em Permissões, escolha Usar função existente e selecione a função que você criou durante o procedimento de configuração na lista suspensa. Você também pode escolher Ir para o console do IAM para criar uma nova função.

   Para que o Agendador do EventBridge crie um novo perfil de execução para você, escolha Criar um novo perfil para este agendamento. Depois, insira um nome em Nome do perfil. Se você escolher essa opção, o Agendador do EventBridge adicionará as permissões necessárias para seu destino de exemplo ao perfil.

10. Escolha Próximo.
11. Na página Revisar e criar programação, revise os detalhes da programação. Em cada seção, escolha Editar para voltar a essa etapa e editar seus detalhes.
12. Escolha Criar agendamento para concluir a criação da nova agenda. Você pode ver a lista com as programações novas e existentes na página Programações. Na coluna Status, verifique se a nova programação está Ativada.
13. Para verificar se seu agendamento invoca o destino do Amazon SQS, abra o console do Amazon SQS e faça o seguinte:

a. Escolha a fila de destino na lista Filas.
b. Escolha Enviar e receber mensagens.
c. Na página Enviar e receber mensagens, em Receber mensagens, escolha Sondar mensagens para recuperar as mensagens de teste que seu agendamento enviou para a fila de destino.

Crie um agendamento usando a AWS CLI

O exemplo a seguir mostra como usar o comando de AWS CLI `create-schedule` para criar um agendamento do Agendador do EventBridge com um destino modelo do Amazon SQS. Substitua os valores do espaço reservado para os seguintes parâmetros por suas informações:

- --name: Insira um nome para o agendamento.
- RoleArn: Insira o ARN da função de execução que você deseja associar ao agendamento.
- Arn: Insira o ARN do destino. Nesse caso, o destino é uma fila do Amazon SQS.
- Entrada: Insira uma mensagem que o Agendador do EventBridge entrega à fila de destino.

```
$ 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"}'
```

Criar um agendamento usando os SDKs do Agendador do EventBridge

No exemplo a seguir, você usa os SDKs do Agendador do EventBridge para criar um agendamento do Agendador do EventBridge com um destino modelo do 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 SDK do Java

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

```
                        .build())
                .build();

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

Próximas etapas

- Para obter mais informações sobre como gerenciar seu agendamento usando o console, a AWS CLI, ou o SDK do Agendador do EventBridge, consulte Gerenciando um agendamento.
- Para obter mais informações sobre como configurar destinos modelados e aprender a usar o parâmetro de destino universal, consulte Gerenciando destinos.
- Para obter mais informações sobre os tipos de dados e as operações da API do Agendador do EventBridge, consulte a Referência da API do Agendador do EventBridge.

Tipos de EventBridge agendamento no Scheduler

O tópico a seguir descreve os diferentes tipos de EventBridge agendamento que o Amazon Scheduler suporta, bem como a forma como o EventBridge Scheduler lida com o horário de verão e a programação em diferentes fusos horários. Você pode escolher entre três tipos de agendamento ao configurar seu agendamento: agendamentos baseados em taxas, em cron e horários únicos.

Tanto os agendamentos baseados em taxas quanto os baseados em cron são recorrentes. Você configura cada tipo de agendamento recorrente usando uma expressão de agendamento para o tipo de agendamento que você deseja configurar e especificando um fuso horário no qual o EventBridge Agendador avalia a expressão.

Um agendamento único é um agendamento que invoca um destino somente uma vez. Você configura um agendamento único ao especificar a hora, a data e o fuso horário em que o EventBridge Agendador avalia o agendamento.

> **Note**
>
> Todos os tipos de EventBridge agendamento no Scheduler invocam seus alvos com precisão de 60 segundos. Isso significa que, se você definir seu cronograma para ser executado à `1:00`, ela invocará a API de destino entre `1:00:00` e `1:00:59`, supondo que não haja uma janela de tempo flexível definida.

Use as seções a seguir para aprender sobre como configurar expressões de agendamento para cada tipo de agendamento recorrente e como configurar um agendamento único no Scheduler. EventBridge

Tópicos

- Rate-based horários
- Cron-based horários
- One-time horários
- Fusos horários no EventBridge Scheduler
- Horário de verão no EventBridge Scheduler

Rate-based horários

Um agendamento baseado em taxas começa após a data de início que você especificou para seu agendamento e é executado com uma taxa regular que você define até a data de término do agendamento. Você pode configurar os casos de uso mais comuns de agendamento recorrente usando um agendamento baseado em taxas. Por exemplo, se você quiser um cronograma que invoque sua meta a cada 15 minutos, uma vez a cada duas horas ou uma vez a cada cinco dias, você pode usar um cronograma baseado em taxas para conseguir isso. Você configura um agendamento baseado em taxa usando uma expressão rate.

Com agendamentos baseados em taxas, você usa a propriedade `StartDate` para definir a primeira ocorrência do agendamento. Se você não fornecer uma `StartDate` para um agendamento baseado em taxas, seu agendamento começará a invocar a meta imediatamente.

As expressões de taxa têm dois campos obrigatórios separados por um espaço em branco, conforme mostrado a seguir.

Sintaxe

```
rate(value unit)
```

valor

Um número positivo.

unidade

A unidade de tempo em que você deseja que sua agenda invoque sua meta.

Entradas válidas: `minutes` | `hours` | `days`

Exemplos

O exemplo a seguir mostra como usar expressões de taxa com o AWS CLI `create-schedule` comando para configurar uma programação baseada em taxas. Este exemplo cria um agendamento que é executado a cada cinco minutos e entrega uma mensagem para uma fila do Amazon SQS, usando o tipo de destino de `SqsParameters` modelado.

Como esse exemplo não define um valor para o parâmetro `--start-date`, o agendamento começa a invocar seu destino imediatamente após você criá-lo e ativá-lo.

```
$ 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"}'
```

Cron-based horários

Uma expressão cron cria uma programação recorrente refinada que é executada em um horário específico de sua escolha. EventBridge O Scheduler suporta a configuração de agendas baseadas em cron no Tempo Coordenado Universal (UTC) ou no fuso horário que você especifica ao criar sua agenda. Com agendamentos baseados em cron, você tem mais controle sobre quando e com que frequência seu agendamento é executado. Use agendas baseadas em cron quando precisar de uma programação de recorrência personalizada que não seja suportada por uma das expressões de taxa do EventBridge Scheduler. Por exemplo, é possível criar um agendamentos baseados em cron que seja executada às 8h00 PST na primeira segunda-feira de cada mês. Você configura um agendamento baseado em cron usando uma expressão cron.

Uma expressão cron consiste em seis campos obrigatórios separados por espaço em branco: minutos, horas, dia do mês, mês, dia da semana e ano, conforme mostrado a seguir.

Sintaxe

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

Campo	Valores	Curingas
minutos	0-59	, - * /
Horas	0-23	, - * /
Day-of-month	1-31	, - * ? / L W
Mês	1-12 ou JAN-DEC	, - * /
Day-of-week	1-7 ou SUN-SAT	, - * ? L #
Ano	1970-2199	, - * /

Curingas

- A , (vírgula) curinga inclui valores adicionais. No campo Mês, JAN, FEV, MAR inclui janeiro, fevereiro e março.
- O - (traço) curinga especifica intervalos. No campo Dia, 1-15 inclui os dias 1 a 15 do mês especificado.
- O * (asterisco) curinga inclui todos os valores no campo. No campo Hours (Horas), * inclui todas as horas. Você não pode usar * nos Day-of-week campos Day-of-month e. Se você usá-lo em um deles, utilize ? no outro.
- A / (barra) curinga especifica incrementos. No campo Minutos, você pode inserir 1/10 para especificar cada décimo minuto, começando pelo primeiro minuto da hora (por exemplo, 11º, 21º e 31º minutos e assim por diante).
- O curinga ? (interrogação) especifica qualquer um. No Day-of-month campo você poderia inserir 7 e se algum dia da semana fosse aceitável, você poderia inserir? no Day-of-week campo.
- O caractere curinga L nos Day-of-week campos Day-of-month ou especifica o último dia do mês ou da semana.
- O **`W`** caractere curinga no Day-of-month campo especifica um dia da semana. No Day-of-month campo, **`3W`** especifica o dia da semana mais próximo do terceiro dia do mês.
- O caractere curinga # no Day-of-week campo especifica uma determinada instância do dia da semana especificado em um mês. Por exemplo, 3#2 seria a segunda terça-feira do mês: o 3 refere-se a terça-feira, porque é o terceiro dia de cada semana, e o 2 refere-se ao segundo dia desse tipo dentro do mês.

> **Note**
>
> Se você usar um caractere “#”, poderá definir apenas uma expressão no campo do dia da semana. Por exemplo, o valor `"3#1,6#3"` não é válido porque é interpretado como duas expressões.

Exemplos

O exemplo a seguir mostra como usar expressões cron com o AWS CLI `create-schedule` comando para configurar uma programação baseada em cron. Este exemplo cria um agendamento que é executado às 10h15 UTC+0 na última sexta-feira de cada mês durante os anos de 2022 a

2023 e entrega uma mensagem para uma fila do Amazon SQS, usando o tipo de destino modelado `SqsParameters`.

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

One-time horários

Um agendamento único invocará um alvo somente uma vez na data e hora que você especificar usando uma data válida e um carimbo de data/hora. EventBridge O Scheduler oferece suporte ao agendamento no Horário Coordenado Universal (UTC) ou no fuso horário que você especifica ao criar sua agenda.

> **Note**
>
> Uma programação única ainda conta na cota da sua conta depois de concluir a execução e a invocação de sua meta. Recomendamos excluir seus agendamentos únicos depois que eles concluírem a execução.

Você configura um agendamento único usando uma expressão at. Uma expressão at consiste na data e na hora em que você deseja que o EventBridge Scheduler invoque sua agenda, conforme mostrado a seguir.

Sintaxe

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

Quando você configura um EventBridge agendamento único, o Agendador ignora o `StartDate` e `EndDate` você especifica para o agendamento.

Exemplos

O exemplo a seguir mostra como usar expressões at com o AWS CLI `create-schedule` comando para configurar um agendamento único. Este exemplo cria uma programação que é executada

uma vez às 13h do UTC-8 dia 20 de novembro de 2022 e entrega uma mensagem para uma fila do Amazon SQS, usando o `SqsParameters` tipo de destino modelado.

```
$ 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"}'
```

Fusos horários no EventBridge Scheduler

EventBridge O Scheduler suporta a configuração de agendamentos únicos e baseados em cron em qualquer fuso horário que você especificar. EventBridge O Scheduler usa o banco de dados de fuso horário mantido pela Internet Assigned Numbers Authority (IANA).

Com o AWS CLI, você pode definir o fuso horário no qual deseja que o EventBridge Scheduler avalie sua agenda usando o `--schedule-expression-timezone` parâmetro. Por exemplo, o comando a seguir cria uma programação baseada em cron que invoca um alvo modelo do Amazon SQS America/Newem _York todos os `SendMessage` dias às 8h30.

```
$ 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"}'
```

Horário de verão no EventBridge Scheduler

EventBridge O agendador ajusta automaticamente sua programação para o horário de verão. Quando o tempo avança na primavera, se uma expressão cron cair em uma data e hora inexistentes, a invocação do agendamento será ignorada. Quando o tempo muda para trás no outono, seu agendamento é executado apenas uma vez e não repete sua invocação. As invocações a seguir ocorrem normalmente na data e hora especificadas.

EventBridge O agendador ajusta sua agenda de acordo com o fuso horário especificado ao criar a agenda. Se você configurar uma programação em America/New_York, sua programação será ajustada quando a hora mudar nesse fuso horário, enquanto uma programação em America/Los_Angeles será ajustada três horas depois, quando a hora mudar na costa oeste.

Para horários baseados em taxas que usam `days` como unidade, por exemplo `rate(1 days)`, `days` representa uma duração de 24 horas no relógio. Isso significa que, quando o horário de verão faz com que um dia diminua para 23 horas ou se estenda para 25 horas, o EventBridge Scheduler ainda avalia a expressão da taxa 24 horas após a última invocação da programação.

> **Note**
>
> Alguns fusos horários não observam o horário de verão, de acordo com as regras e regulamentos locais. Se você criar uma programação em um fuso horário que não observe o horário de verão, o EventBridge Scheduler não ajustará sua programação. Daylight-savings os ajustes de horário não se aplicam aos horários no horário coordenado universal (UTC).

Exemplo

Considere um cenário em que você cria um cronograma usando a seguinte expressão cron em America/Los_Angeles:. `cron(30 2 * * ? *)` Esse agendamento é executado todos os dias às 2h30 no fuso horário especificado.

- Spring-forward— Quando o horário avança na primavera, das 1h59 às 3h, o EventBridge Scheduler pula a invocação da programação naquele dia e retoma a execução da programação normalmente no dia seguinte.
- Fall-back— Quando o horário muda para trás no outono, das 2h59 às 2h, o EventBridge Scheduler executa a programação apenas uma vez às 2h30 antes da ocorrência do turno, mas não repete a invocação da programação novamente às 2h30 após a mudança de horário.

Gerenciando uma agenda no EventBridge Scheduler

Um cronograma é o principal recurso que você cria, configura e gerencia usando o Amazon EventBridge Scheduler.

Cada agendamento tem uma expressão de cronograma que determina quando e com que frequência o cronograma é executado. EventBridge O Scheduler oferece suporte a três tipos de agendamentos: tarifário, cron e horários únicos. Para obter mais informações sobre os diferentes tipos de agendamento, consulte Tipos de agendamento.

Ao criar um agendamento, você configura uma meta para o agendamento a ser invocado. Um alvo é uma operação de API que o EventBridge Scheduler chama em seu nome sempre que sua agenda é executada. EventBridge O Scheduler suporta dois tipos de destinos: alvos modelados chamam operações de API comuns em um grupo principal de serviços e o parâmetro de destino universal (UTP) que você pode usar para chamar mais de 6.000 operações em mais de 270 serviços. Para obter mais informações sobre a configuração de destinos, consulte Gerenciando destinos.

Você configura como sua agenda lida com as falhas, quando o EventBridge Scheduler não consegue entregar um evento com êxito a um destino, usando dois mecanismos principais: uma política de repetição e uma fila de cartas mortas (DLQ). Uma política de repetição determina o número de vezes que o EventBridge Agendador deve repetir um evento com falha e por quanto tempo manter um evento não processado. Um DLQ é um padrão que o Amazon SQS EventBridge queue Scheduler usa para entregar eventos com falha, após o esgotamento da política de repetição. Você pode usar uma DLQ para solucionar problemas com seu agendamento ou sua meta posterior. Para ter mais informações sobre, consulte the section called “Configurar uma DLQ”.

Nesta seção, você pode encontrar exemplos para gerenciar seus EventBridge agendamentos do Scheduler usando o console, o AWS CLI e o EventBridge Scheduler. SDKs

Tópicos

- Alterando o estado do EventBridge agendamento no Scheduler
- Configurando janelas de horário flexíveis no EventBridge Scheduler
- Configurando a fila de mensagens mortas de uma agenda no Scheduler EventBridge
- Excluindo uma agenda no Scheduler EventBridge
- Próximas etapas

Alterando o estado do EventBridge agendamento no Scheduler

Uma EventBridge agenda do Scheduler tem dois estados: ativada e desativada. O exemplo a seguir usa o `UpdateSchedule` para desativar um agendamento que é acionado a cada cinco minutos e invoca um destino Lambda.

Ao usar`UpdateSchedule`, você deve fornecer todos os parâmetros necessários. EventBridge O Scheduler substitui sua agenda pelas informações que você fornece. Se você não especificar um parâmetro definido anteriormente, definirá `null` como padrão.

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"
}
```

O exemplo a seguir usa o SDK do Python e a operação de `UpdateSchedule` para desativar um agendamento direcionado ao Amazon SQS usando um destino modelado.

Example SDK da para Python

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

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

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

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

Configurando janelas de horário flexíveis no EventBridge Scheduler

Quando você configura sua agenda com uma janela de tempo flexível, o EventBridge Scheduler invoca a meta dentro da janela de tempo que você definiu. Isso é útil em casos que não exigem invocação programada precisa de destinos. Definir uma janela de horário flexível melhora a confiabilidade de seu agendamento ao dispersar suas invocações de destino.

Por exemplo, se você configurar uma janela de horário flexível de 15 minutos para um agendamento que é executado a cada hora, ela invoca o destino dentro de 15 minutos após o horário agendado. Os exemplos a seguir AWS CLI e o SDK EventBridge do Scheduler são usados `UpdateSchedule` para definir uma janela de tempo flexível de 15 minutos para uma programação que é executada uma vez a cada hora.

> **Note**
>
> Você deve especificar se deseja definir uma janela de horário flexível ou não. Se você não quiser definir essa opção, especifique `OFF`. Se você definir o valor como `FLEXIBLE`, deverá especificar uma janela máxima de tempo durante a qual seu agendamento será executada.

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 SDK da para Python

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

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

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

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

Configurando a fila de mensagens mortas de uma agenda no Scheduler EventBridge

O Amazon EventBridge Scheduler oferece suporte a filas de cartas mortas (DLQ) usando o Amazon Simple Queue Service. Quando um EventBridge agendamento falha em invocar seu destino, o Scheduler entrega uma carga JSON contendo detalhes da invocação e qualquer resposta recebida do destino para uma fila padrão do Amazon SQS que você especificar.

O tópico a seguir se refere a esse JSON como um evento de mensagens não entregues. Um evento de mensagens não entregues permite que você solucione problemas com seu agendamento ou metas. Se você configurar uma política de repetição para sua agenda, o EventBridge Scheduler entregará o evento de carta morta que ele tem, esgotando o número máximo de novas tentativas que você definiu.

Os tópicos a seguir descrevem como você pode configurar uma fila do Amazon SQS como DLQ para sua programação, configurar as permissões que o EventBridge Agendador precisa para entregar mensagens ao Amazon SQS e receber eventos de carta morta do DLQ.

Tópicos

- Criar uma fila do Amazon SQS
- Configure as permissões da função de execução
- Especificar uma fila de mensagens não entregues
- Recuperar o evento de mensagens não entregues

Criar uma fila do Amazon SQS

Antes de configurar uma DLQ para seu agendamento, você deve criar uma fila padrão do Amazon SQS. Para obter instruções sobre criar uma fila utilizando o Amazon SQS, consulte o tópico sobre como Criar uma fila do Amazon SQS, no Guia do desenvolvedor do Amazon Simple Queue Service.

> **Note**
>
> EventBridge O Scheduler não suporta o uso de uma fila FIFO como DLQ da sua agenda.

Use o AWS CLI comando a seguir para criar uma fila padrão.

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

Se o for bem-sucedido, você verá `QueueURL` no resultado.

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

Depois de criar a fila, anote o ARN da fila. Você precisará do ARN ao especificar uma DLQ para sua EventBridge programação do Scheduler. Você pode encontrar o ARN da fila no console do Amazon SQS ou usando o comando. `get-queue-attributes` AWS CLI

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

Se for bem-sucedido, você verá o ARN da fila na saída.

```
{
    "Attributes": {
```

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

Na próxima seção, você adicionará as permissões necessárias à sua função de execução do cronograma para permitir que o EventBridge Scheduler entregue eventos sem saída para o Amazon SQS.

Configure as permissões da função de execução

Para permitir que o EventBridge Scheduler entregue eventos com data limite para o Amazon SQS, sua função de execução do cronograma precisa da seguinte política de permissão. Para obter mais informações sobre como anexar uma nova política de permissão à sua função de execução do agendamento, consulte Configurando a função de execução.

JSON

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

> **Note**
>
> Sua função de execução do cronograma pode já ter as permissões necessárias anexadas se você usar o EventBridge Scheduler para invocar um destino de API do Amazon SQS.

Na próxima seção, você usará o console do EventBridge Scheduler e especificará uma DLQ para sua agenda.

Especificar uma fila de mensagens não entregues

Para especificar um DLQ, use o console do EventBridge Scheduler ou o AWS CLI para atualizar um agendamento existente ou criar um novo.

Console

Para especificar uma DLQ usando o console

1. Faça login no e escolha o Console de gerenciamento da AWS link a seguir para abrir a seção EventBridge Agendador do EventBridge console: https://console.aws.amazon.com/scheduler/home
2. No console do EventBridge Agendador, crie um novo agendamento ou escolha um agendamento existente na sua lista de agendamentos para edição.
3. Na página Configurações, para Dead-letter fila (DLQ), faça o seguinte:
   - Escolha Selecionar uma fila do Amazon SQS em minha AWS conta como DLQ e, em seguida, escolha o ARN da fila para seu DLQ na lista suspensa.
   - Escolha Especificar uma fila do Amazon SQS em outras AWS contas como DLQ e, em seguida, insira o ARN da fila para sua DLQ. Se você escolher uma fila em outra AWS conta, o console do EventBridge Scheduler não poderá exibir os ARNs da fila em uma lista suspensa.
4. Revise suas seleções e escolha Criar agendamento ou Salvar agendamento para concluir a configuração de uma DLQ.
5. (Opcional) Para ver os detalhes do DLQ de uma agenda, escolha o nome da agenda na lista e, em seguida, escolha a guia Dead-letter fila na página de detalhes da programação.

AWS CLI

Para atualizar um cronograma existente usando o AWS CLI

- Use o comando `update-schedule` para atualizar sua agenda. Especifique a fila do Amazon SQS que você criou anteriormente como DLQ. Especifique o ARN do perfil do IAM ao qual você anexou as permissões necessárias do Amazon SQS como função de execução. Substitua todos os outros valores de espaço reservado por suas informações.

```
$ 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"}'
```

Para criar um novo agendamento com um DLQ usando o AWS CLI

- Para criar um agendamento, use o comando `create-schedule`. Substitua todos os valores de espaço reservado por suas informações.

```
$ 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"}'
```

Na próxima seção, você usará o AWS CLI para receber um evento de carta morta do DLQ.

Recuperar o evento de mensagens não entregues

Use o comando `receive-message`, conforme mostrado a seguir, para recuperar um evento de mensagens não entregues da DLQ. Você pode definir o número de mensagens a serem recuperadas usando o atributo `--max-number-of-messages`.

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

Se for bem-sucedido, você verá uma saída semelhante à seguinte:

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

Observe os atributos a seguir no evento dead-letter para ajudá-lo a identificar e solucionar possíveis motivos pelos quais a invocação do alvo falhou.

- **`ERROR_CODE`**— Contém o código de erro que o EventBridge Scheduler recebe da API de serviço do alvo. No exemplo anterior, o código de erro retornado pelo Amazon SQS é `AWS.SimpleQueueService.NonExistentQueue`. Se o agendamento falhar em invocar um alvo devido a um problema com o EventBridge Scheduler, você verá o seguinte código de erro em vez disso:. `AWS.Scheduler.InternalServerError`
- **`ERROR_MESSAGE`**— Contém a mensagem de erro que o EventBridge Scheduler recebe da API de serviço do alvo. No exemplo anterior, a mensagem de erro retornada pelo Amazon SQS é `The specified queue does not exist for this wsdl version`. Se o agendamento falhar devido a um problema com o EventBridge Scheduler, você verá a seguinte mensagem de erro em vez disso:`Unexpected error occurred while processing the request`.
- **`TARGET_ARN`**: O ARN do destino que seu agendamento invoca, no seguinte formato de ARN de serviço: `arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.
- **`EXHAUSTED_RETRY_CONDITION`**: Indica por que o evento foi entregue à DLQ. Esse atributo estará presente se o erro da API-destino for um erro que pode ser repetido e não permanente. O atributo pode conter os valores `MaximumRetryAttempts` se o EventBridge Scheduler o tiver enviado para a DLQ depois de exceder o máximo de tentativas que você configurou para o agendamento ou`MaximumEventAgeInSeconds`, se o evento for maior que a idade máxima que você configurou na programação e ainda não está sendo entregue.

No exemplo anterior, podemos determinar, com base no código de erro e na mensagem de erro, que a fila de destino que especificamos para o agendamento não existe.

> **Note**
>
> Se você usa destinos universais, saiba que o EventBridge Scheduler não valida o conteúdo do `Input` campo no momento da criação do cronograma. Um agendamento com parâmetros

de entrada inválidos será criado com sucesso, mas falhará em cada invocação. A mensagem DLQ conterá o código de erro e a mensagem do serviço de destino, o que pode ajudá-lo a identificar o parâmetro inválido. Para obter mais informações, consulte Configurações inválidas de entrada de destino universal.

Excluindo uma agenda no Scheduler EventBridge

Você pode excluir um agendamento configurando a exclusão automática ou excluindo manualmente um agendamento individual. Use os tópicos a seguir para saber como excluir um agendamento usando os dois métodos e por que você pode escolher um método em vez do outro.

Tópicos

- Exclusão após a conclusão do agendamento
- Exclusão manual

Exclusão após a conclusão do agendamento

Configure a exclusão automática após a conclusão do cronograma se quiser evitar ter que gerenciar individualmente seus recursos de EventBridge agendamento no Scheduler. Em aplicativos em que você cria milhares de agendamentos ao mesmo tempo e precisa de flexibilidade para aumentar a escala verticalmente do número de seus agendamentos sob demanda, a exclusão automática pode garantir que você não atinja a cota da sua conta para o número de agendamentos em uma região específica.

Quando você configura a exclusão automática de um EventBridge agendamento, o Scheduler exclui o agendamento após sua última invocação de destino. Para agendamentos únicos, isso ocorre após o agendamento ter invocado seu destino uma vez. Para agendamentos recorrentes que você configura com expressões rate ou cron, seu agendamento é excluído após a última invocação. A última invocação de um agendamento recorrente é a invocação que ocorre mais próxima da `EndDate` que você especificou. Se você configurar um agendamento com exclusão automática, mas não especificar um valor para`EndDate`, o EventBridge Agendador não excluirá automaticamente o agendamento.

Você pode configurar a exclusão automática ao criar um agendamento pela primeira vez ou atualizar as preferências de um agendamento existente. As etapas a seguir descrevem como configurar exclusão automática para um agendamento existente.

Console de gerenciamento da AWS

1. Abra o console do EventBridge Scheduler em. https://console.aws.amazon.com/scheduler/
2. Na lista de agendamentos, selecione o agendamento que você deseja editar e escolha Editar.
3. No painel de navegação à esquerda, selecione Configurações.
4. Na seção Ação após a conclusão do agendamento, selecione EXCLUIR na lista suspensa e salve suas alterações.

AWS CLI

1. Abra uma nova janela de prompt.
2. Use o AWS CLI comando update-schedule para atualizar uma agenda existente, conforme mostrado a seguir. O comando define o `--action-after-completion` para `DELETE`. Este exemplo pressupõe que você definiu sua configuração de destino localmente em um arquivo JSON. Para atualizar um agendamento, você deve fornecer a meta, bem como quaisquer outros parâmetros de agendamento que você queira configurar para o seu agendamento existente.

   Essa é um agendamento recorrente com uma taxa de uma invocação por hora. Portanto, você especifica uma data de término ao definir o parâmetro `--action-after-completion`.

```
$ 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"}' \
```

Exclusão manual

Quando não precisar mais de um agendamento, você pode excluí-lo usando a operação `DeleteSchedule`.

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")
```

Próximas etapas

- Para obter mais informações sobre como configurar destinos modelados para as funções Lambda e Step e aprender a usar o parâmetro de destino universal, consulte Gerenciando destinos.
- Para obter mais informações sobre os tipos de dados e as operações da API do EventBridge Scheduler, consulte a Referência da API do EventBridge Scheduler.

Gerenciar um grupo de cronogramas no Agendador do EventBridge

Um grupo de agendamento é um recurso do Agendador do Amazon EventBridge que você usa para organizar seus agendamentos.

Sua Conta da AWS vem com um grupo de agendadores `default`. Você pode associar um novo agendamento ao grupo `default` ou aos grupos de agendamentos que você cria e gerencia. Você pode criar até 500 grupos de agendamento na sua Conta da AWS. Com o Agendador do EventBridge, você organiza grupos de agendamentos, em vez de agendamentos individuais, aplicando tags.

Uma tag é um rótulo composto por uma chave com distinção entre maiúsculas e minúsculas e um valor que você define. Você pode criar tags para categorizar agendamentos por finalidade, proprietário ou ambiente. Por exemplo, você pode identificar o ambiente ao qual suas agendamentos pertencem com a seguinte tag: `environment:production`.

> **Important**
>
> Não adicione informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. As tags são acessíveis a muitos serviços da AWS, incluindo faturamento. As etiquetas não devem ser usadas para armazenar dados sensíveis ou privados.

Um grupo de agendamentos tem dois estados possíveis: ATIVO e EXCLUINDO.

Quando você cria um grupo pela primeira vez, é `ACTIVE` por padrão. Você pode adicionar agendamentos a um grupo `ACTIVE`. Quando você exclui um grupo, o estado muda para `DELETING` até que o Agendador do EventBridge conclua a exclusão dos agendamentos associados. Depois que o Agendador do EventBridge excluir os agendamentos do grupo, o grupo não estará mais disponível em sua conta.

Use os tópicos a seguir para criar um grupo de agendamentos e aplicar uma tag a ele. Você também associará um cronograma ao grupo. Por fim, você excluirá o grupo.

Tópicos

- Criar um grupo de cronogramas no Agendador do EventBridge
- Excluir um grupo de cronogramas no Agendador do EventBridge
- Recursos relacionados

Criar um grupo de cronogramas no Agendador do EventBridge

Use grupos de agendamentos e marcações para organizar agendamentos que compartilhem um propósito comum ou pertençam ao mesmo ambiente. Nas etapas a seguir, você cria um novo grupo de agendamentos e o rotula usando uma tag. Em seguida, você associa um novo agendamento a esse grupo.

> **Note**
>
> Depois de criar um grupo, você não pode remover um agendamento desse grupo nem associar o agendamento a um grupo diferente. Você só pode associar um agendamento a um grupo ao criar o agendamento pela primeira vez.

Etapa 1: criar um novo grupo de agendamento

Os seguintes tópicos descrevem como criar um novo grupo de agendamento e rotulá-lo com a seguinte tag: `environment:development`.

Console de gerenciamento da AWS

Para criar um novo grupo utilizando o Console de gerenciamento da AWS

1. Faça login noConsole de gerenciamento da AWSe abra o console do Amazon EventBridge emhttps://console.aws.amazon.com/events/.
2. No painel de navegação esquerdo, escolha Grupos de agendamento.
3. Na página agendamentos, escolha Criar um agendamento.
4. Na seção Detalhes do grupo de agendamento, em Nome, insira um nome para o grupo. Por exemplo, **`TestGroup`**.
5. Na seção Tags, faça o seguinte:

   a. Selecione Adicionar nova tag.

b. Em Chave, insira o nome que você deseja atribuir a essa chave. Neste tutorial, para rotular o ambiente ao qual esse grupo de agendamentos pertence, insira **`environment`**.

c. Em Valor - opcional, insira o valor que você deseja atribuir a essa chave. Para este tutorial, insira o valor **`development`** da sua chave de ambiente.

> **Note**
>
> Você pode adicionar outras tags ao seu grupo depois de criá-lo.

6. Para terminar, escolha Criar grupo de agendamento. Seu novo grupo aparece na lista de grupos de agendamento.
7. (Opcional) Para editar um grupo ou gerenciar suas tags, marque a caixa de seleção do novo grupo e escolha Editar.

> **Note**
>
> Não é possível editar o grupo de agendamento `default`.

AWS CLI

Para criar um novo grupo utilizando a AWS CLI

1. Abra uma nova janela do prompt de comando.
2. Do AWS Command Line Interface (AWS CLI), insira o seguinte comando de `create-schedule-group` para criar um novo grupo: Esse comando cria um grupo com uma tag: `environment:development`. Você pode usar essa tag ou um sistema de marcação similar para rotular seus grupos de agendamento de acordo com o ambiente ao qual eles pertencem.

   Substitua o nome do agendamento e a chave e o valor da tag por suas informações.

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

Por padrão, seu novo grupo está no estado `ACTIVE`. Agora você pode associar novos agendamentos ao novo grupo que você criou.

Etapa 2: associar um agendamento ao grupo

Use as etapas a seguir para associar um novo agendamento ao grupo que você criou na etapa anterior.

Console de gerenciamento da AWS

Para associar um agendamento a um grupo usando o Console de gerenciamento da AWS

1. Faça login noConsole de gerenciamento da AWSe abra o console do Amazon EventBridge emhttps://console.aws.amazon.com/events/.
2. No painel de navegação à esquerda, escolha agendamentos no painel de navegação à esquerda.
3. Na tabela Agendamentos, escolha Criar agendamento para criar um novo agendamento.
4. Na página Especificar detalhes da agenda, em Grupo da agenda, selecione o nome do seu novo grupo na lista suspensa. Por exemplo, consulte `TestGroup`.
5. Especifique um padrão de agendamento, meta e configurações e, em seguida, revise sua seleção na página Revisar e salvar o agendamento. Para obter mais informações sobre como configurar um novo agendamento, consulte Introdução.
6. Para finalizar e salvar sua agenda, escolha Salvar agenda.

AWS CLI

Para associar um agendamento a um grupo usando a AWS CLI

1. Abra uma nova janela do prompt de comando.
2. Do AWS Command Line Interface (AWS CLI), insira o seguinte comando de `create-schedule`. Isso cria um agendamento e o associa ao grupo da etapa anterior, denominada `sqs-test-schedule`. Esse agendamento usa o tipo de destino modelo do Amazon SQS para invocar a operação de `SendMessage`. Substitua o nome da agenda, o destino e o nome do grupo por suas informações.

```
$ 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"}'
```

Seu novo agendamento agora está associado ao grupo de agendamentos do `TestGroup`.

Excluir um grupo de cronogramas no Agendador do EventBridge

A seguir, você pode aprender como excluir um grupo de agendamentos usando o Console de gerenciamento da AWS e o AWS Command Line Interface. Quando você exclui um grupo, ele permanece no estado `DELETING` até que o Agendador do EventBridge exclua todos os agendamentos do grupo. Depois que o Agendador do EventBridge excluir os agendamentos do grupo, o grupo não estará mais disponível em sua conta.

> **Note**
>
> Depois de criar um grupo, você não pode remover um agendamento desse grupo nem associar o agendamento a um grupo diferente. Você só pode associar um agendamento a um grupo ao criar o agendamento pela primeira vez.

Console de gerenciamento da AWS

Para excluir um grupo usando o Console de gerenciamento da AWS

1. Faça login noConsole de gerenciamento da AWSe abra o console do Amazon EventBridge emhttps://console.aws.amazon.com/events/.
2. No painel de navegação à esquerda, escolha agendamentos no painel de navegação à esquerda.
3. Na página Grupos de agendamento, na lista de grupos existentes na Região da AWS atual, localize o grupo que você deseja excluir. Se não encontrar o grupo que estava buscando, escolha outra Região da AWS.

   > **Note**
   >
   > Você não pode excluir, ou editar, o grupo padrão.

4. Marque a caixa de seleção para o grupo que deseja excluir.
5. Escolha Excluir.

6. Na caixa de diálogo Excluir grupo de agendamento, insira o nome do grupo para confirmar sua escolha e escolha Excluir.
7. Na lista Grupos de agendamento, a coluna Status muda para indicar que seu grupo agora está excluindo. O grupo permanece nesse estado até que o Agendador do EventBridge exclua todos os agendamentos associados ao grupo.
8. Para atualizar a lista e confirmar que o grupo foi excluído, escolha o ícone Atualizar.

AWS CLI

Para excluir um grupo usando a AWS CLI

1. Abra uma nova janela do prompt de comando.
2. Do AWS Command Line Interface (AWS CLI), digite o comando de `delete-schedule-group` a seguir para excluir o grupo de agendamentos. Substitua o valor de `--name` por suas informações.

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

   Se for bem-sucedida, essa operação da AWS CLI não retornará uma resposta.
3. Para verificar se o grupo está no estado `DELETING`, execute o comando a seguir `get-schedule-group`.

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

   Se for executado com êxito, você receberá um resultado semelhante a este.

```
{
    "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"
}
```

   O Agendador do EventBridge exclui o grupo depois de excluir os agendamentos associados ao grupo. Se você executar `get-schedule-group` novamente, receberá a seguinte resposta de `ResourceNotFoundException`:

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

Recursos relacionados

Para obter mais informações sobre grupos de agendamento, consulte os seguintes recursos:

- Operação CreateScheduleGroup na Referência da API do Agendador do EventBridge.
- Operação DeleteScheduleGroup na Referência da API do Agendador do EventBridge.

Gerenciando alvos no EventBridge Scheduler

Os tópicos a seguir descrevem como usar alvos modelados e universais com o EventBridge Scheduler e fornecem uma lista dos AWS serviços suportados que você pode configurar usando o parâmetro de destino universal do EventBridge Scheduler.

Os alvos modelados são um conjunto de operações de API comuns em um grupo de AWS serviços principais, como Amazon SQS, Lambda e Step Functions. Por exemplo, você pode direcionar a operação de Invocar de API do Lambda fornecendo o ARN da função ou a operação de `SendMessage` do Amazon SQS usando o ARN do destino.

O alvo universal é um conjunto personalizável de parâmetros que permite invocar um conjunto mais amplo de operações de API para muitos AWS serviços. Por exemplo, você pode usar o parâmetro de destino universal (UTP) do EventBridge Scheduler para criar uma nova fila do Amazon SQS usando a operação. `CreateQueue`

Para configurar metas padronizadas ou universais, seu agendamento deve ter permissão para chamar a operação de API que você configura como sua meta. Para fazer isso, anexe as permissões necessárias ao perfil de execução de seu agendamento. Por exemplo, para direcionar a operação de `SendMessage` do Amazon SQS, a função de execução recebe permissão para realizar a ação de `sqs:SendMessage`. Na maioria dos casos, você pode adicionar as permissões necessárias usando as políticas gerenciadas da AWS aceitas pelo serviço de destino. No entanto, você também pode criar suas próprias políticas gerenciadas pelo cliente ou adicionar permissões embutidas a uma política existente anexada à função de execução. Os tópicos a seguir demonstram exemplos de adição de permissões para tipos de destino modelados e universais.

Para obter mais informações sobre como configurar uma função de execução para um agendamento, consulte the section called “Configurar o perfil de execução”.

Tópicos

- Usando alvos modelados no EventBridge Scheduler
- Usando alvos universais no EventBridge Scheduler
- Adicionar atributos de contexto no Agendador do EventBridge
- Próximas etapas

Usando alvos modelados no EventBridge Scheduler

Os alvos modelados são um conjunto de operações de API comuns em um grupo de AWS serviços principais, como Amazon SQS, Lambda e Step Functions. Por exemplo, você pode direcionar a operação do Lambda de `Invoke` fornecendo o ARN da função ou a operação do Amazon SQS de `SendMessage` usando o ARN da fila. Para configurar um destino modelado, você também deve conceder permissões à função de execução do agendamento para realizar a operação de API direcionada.

Para configurar um alvo modelado de forma programática usando o AWS CLI ou um dos SDKs do EventBridge Scheduler, você precisa especificar o ARN da função de execução, o ARN do recurso de destino, uma entrada opcional que você deseja que o EventBridge Scheduler entregue ao destino e, para alguns destinos modelados, um conjunto exclusivo de parâmetros com opções adicionais de configuração para esse destino. Quando você especifica o ARN para um recurso de destino modelado, o EventBridge Scheduler assume automaticamente que você deseja chamar a operação de API compatível para esse serviço. Se você quiser que o EventBridge Scheduler direcione uma operação de API diferente para o serviço, você deve configurar o destino como um destino universal.

A seguir está uma lista completa de todos os alvos modelados que o EventBridge Scheduler suporta e, se aplicável, o conjunto exclusivo de parâmetros associados de cada alvo. Escolha o link para cada conjunto de parâmetros para ver os campos obrigatórios e opcionais na Referência da API EventBridge Scheduler.

- CodeBuild – `StartBuild`
- CodePipeline – `StartPipelineExecution`
- Amazon ECS: `RunTask`
  - Parâmetros: `EcsParameters`
- EventBridge – `PutEvents`
  - Parâmetros: `EventBridgeParameters`

> **Important**
>
> EventBridge O Scheduler não oferece suporte à entrega entre regiões quando usado EventBridge `PutEvents` como um destino modelado. Você pode usar esse destino para enviar eventos para um ônibus de eventos em outro local Conta da AWS somente se o ônibus de eventos estiver no Região da AWS mesmo horário. Para enviar eventos para

um ônibus de eventos em uma região diferente, crie uma programação na região em que o ônibus de eventos de destino está localizado.

- Amazon Inspector: `StartAssessmentRun`
- Kinesis: `PutRecord`
  - Parâmetros: `KinesisParameters`
- Firehose: `PutRecord`
- Lambda: `Invoke`
- SageMaker IA — `StartPipelineExecution`
  - Parâmetros: `SageMakerPipelineParameters`
- Amazon SNS: `Publish`
- Amazon SQS: `SendMessage`
  - Parâmetros: `SqsParameters`
- Step Functions: `StartExecution`

Use os exemplos a seguir para aprender a configurar diferentes destinos modelados e as permissões necessárias do IAM para cada destino descrito.

Amazon SQS **SendMessage**

Example Política de permissão para função de execução

JSON

```
{
    "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 SDK da para Java

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

```
                .build();

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

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

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

Lambda Invoke

Example Política de permissão para função de execução

JSON

```
{
    "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 SDK da para Java

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

```
                .build();

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

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

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

Funções de Etapa **`StartExecution`**

Example Política de permissão para função de execução

JSON

```
{
    "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 SDK da para Java

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

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

Usando alvos universais no EventBridge Scheduler

Um alvo universal é um conjunto personalizável de parâmetros que permite invocar um conjunto mais amplo de operações de API para muitos AWS serviços. Por exemplo, você pode usar um parâmetro de destino universal (UTP) para criar uma nova fila do Amazon SQS usando a operação `CreateQueue`.

Para configurar uma meta universal para sua agenda usando o AWS CLI ou um dos SDKs do EventBridge Scheduler, você precisa especificar as seguintes informações:

- RoleArn— O ARN da função de execução que você deseja usar para o destino. A função de execução que você especificar deve ter as permissões para chamar a operação de API que você deseja que seu agendamento vise.
- Arn: O ARN completo do serviço, incluindo a operação de API que você deseja atingir, no seguinte formato: `arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.

  Por exemplo, para o Amazon SQS, o nome do serviço que você especifica é `arn:aws:scheduler:::aws-sdk:`**`sqs:sendMessage`**.

> **Note**
>
> O *`service`* valor no ARN de destino universal deve corresponder ao identificador de serviço do AWS SDK para o serviço de destino. Esse identificador pode ser diferente do prefixo do endpoint do serviço. Por exemplo, para o Amazon Cognito Identity Provider, use `cognitoidentityprovider` (não`cognito-idp`). Para encontrar o identificador de serviço correto, consulte a documentação do AWS SDK para o serviço que você deseja segmentar.

- Entrada — Um JSON bem formado que você especifica com os parâmetros de solicitação que o EventBridge Scheduler envia para a API de destino. Os parâmetros e a forma do JSON que você configura em `Input` são determinados pela API de serviço que seu agendamento invoca. Para obter essas informações, consulte a referência da API do serviço da que você deseja segmentar.

Ações não compatíveis

EventBridge O Scheduler não suporta ações de API somente para leitura, como `GET` operações comuns, que começam com a seguinte lista de prefixos:

```
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
```

Por exemplo, o ARN do serviço para a ação da API de `GetQueueUrl` seria o seguinte: `arn:aws:scheduler:::aws-sdk:sqs:getQueueURL`. Como a ação da API começa com o `get` prefixo, o EventBridge Scheduler não é compatível com esse destino. Da mesma forma, a ação `ListBrokers` do Amazon MQ não é aceita como destino porque a operação começa com o prefixo `list`.

Exemplos usando o destino universal

Os parâmetros transmitidos no campo de agendamento de `Input` dependem dos parâmetros de solicitação que a API de serviço que você deseja invocar aceita. Por exemplo, para visar o `Invoke` Lambda, você pode definir os parâmetros listados na Referência API de AWS Lambda. Isso inclui a carga útil do JSON opcional que você pode passar para uma função do Lambda.

Para determinar os parâmetros que você pode definir para diferentes APIs, consulte a referência da API para esse serviço. Semelhante ao `Invoke` Lambda, algumas APIs aceitam parâmetros de URI, bem como uma carga útil do corpo da solicitação. Nesses casos, você especifica os parâmetros do caminho do URI, bem como a carga útil do JSON na `Input` de sua agenda.

Os exemplos a seguir mostram como usar o destino universal para invocar operações comuns de API com Lambda, Amazon SQS e 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");
    }
}
```

Adicionar atributos de contexto no Agendador do EventBridge

Use as seguintes palavras-chave na carga útil que você passa para o destino para coletar metadados sobre o agendamento: O Agendador do EventBridge substitui cada palavra-chave por seu respectivo valor quando seu agendamento invoca o destino.

- **<aws.scheduler.schedule-arn>**: O ARN do agendamento.
- **<aws.scheduler.scheduled-time>**: O horário que você especificou para o agendamento invocar sua meta, por exemplo, `2022-03-22T18:59:43Z`.
- **<aws.scheduler.execution-id>**: O ID exclusivo que o Agendador do EventBridge atribui para cada tentativa de invocação de um destino, por exemplo, `d32c5kddcf5bb8c3`.
- **<aws.scheduler.attempt-number>**: Um contador que identifica o número da tentativa para a invocação atual, por exemplo, `1`.

Este exemplo mostra a criação de um agendamento que é acionada a cada cinco minutos e invoca a operação de `SendMessage` do Amazon SQS como uma meta universal. O corpo da mensagem inclui o valor para `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)
```

Próximas etapas

Para obter mais informações sobre os tipos de dados e as operações da API do EventBridge Scheduler, consulte a Referência da API do EventBridge Scheduler.

Acesse o Agendador do Amazon EventBridge usando um endpoint de interface (AWS PrivateLink)

Você pode usar AWS PrivateLink para criar uma conexão privada entre a sua VPC e o Agendador do Amazon EventBridge. Você pode acessar o Agendador do EventBridge como se estivesse em sua VPC, sem o uso de gateway da internet, dispositivo NAT, conexão VPN ou conexão do Direct Connect. As instâncias na sua VPC não precisam de endereços IP públicos para acessar o Agendador do EventBridge.

Estabeleça essa conectividade privada criando um endpoint de interface, habilitado pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Agendador do EventBridge.

Para obter mais informações, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink.

Considerações para o Agendador do EventBridge

Antes de configurar um endpoint de interface para o Agendador do EventBridge, revise as Considerações no Guia do AWS PrivateLink.

O Agendador do EventBridge permite fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Criar um endpoint de interface para o Agendador do EventBridge

Você pode criar um endpoint de interface para o Agendador do EventBridge usando o console da Amazon VPC ou o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink.

Como criar um endpoint de interface para o Agendador do EventBridge usando o seguinte nome de serviço:

```
com.amazonaws.region.scheduler
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API ao Agendador do EventBridge usando seu nome DNS regional padrão. Por exemplo, `scheduler.us-east-1.amazonaws.com`.

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um recurso do IAM que pode ser anexado ao endpoint de interface. A política de endpoint padrão permite acesso total ao Agendador do EventBridge por meio de endpoint de interface. Para controlar o acesso permitido ao Agendador do EventBridge pela VPC, anexe uma política de endpoint personalizada ao endpoint de interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o acesso aos serviços usando políticas de endpoint no Guia do AWS PrivateLink.

Exemplo: política de endpoint da VPC para ações do Agendador do EventBridge

Veja a seguir um exemplo de uma política de endpoint personalizado. Quando anexada ao endpoint da sua interface, essa política concede acesso às ações do Agendador do EventBridge listadas para todas as entidades principais em todos os recursos.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "scheduler:GetSchedule",
            "scheduler:ListSchedules",
            "scheduler:GetScheduleGroup",
            "scheduler:ListScheduleGroups"
         ],
         "Resource":"*"
```

```
        }
    ]
}
```

Segurança no Amazon EventBridge Scheduler

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Third-party auditores testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon EventBridge Scheduler, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o EventBridge Scheduler. Os tópicos a seguir mostram como configurar o EventBridge Scheduler para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do EventBridge Scheduler.

Tópicos

- Gerenciando o acesso ao Amazon EventBridge Scheduler
- Proteção de dados no Amazon EventBridge Scheduler
- Validação de conformidade para Amazon EventBridge Scheduler
- Resiliência no Amazon Scheduler EventBridge
- Segurança da infraestrutura no Amazon EventBridge Scheduler

Gerenciando o acesso ao Amazon EventBridge Scheduler

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do EventBridge Scheduler. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticação com identidades
- Gerenciar o acesso usando políticas
- Como o EventBridge Scheduler funciona com o IAM
- Usando políticas baseadas em identidade no Scheduler EventBridge
- Prevenção delegada confusa no EventBridge Scheduler
- Solução de problemas de identidade e acesso ao Amazon EventBridge Scheduler

Público

A forma como você usa AWS Identity and Access Management (IAM) difere com base na sua função:

- Usuário do serviço: solicite permissões ao seu administrador se você não conseguir acessar os atributos (consulte Solução de problemas de identidade e acesso ao Amazon EventBridge Scheduler).
- Administrador do serviço: determine o acesso do usuário e envie solicitações de permissão (consulte Como o EventBridge Scheduler funciona com o IAM)
- Administrador do IAM: escreva políticas para gerenciar o acesso (consulte Usando políticas baseadas em identidade no Scheduler EventBridge)

Autenticação com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte Como fazer login em sua Conta da AWS no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte AWS Signature Version 4 para solicitações de API no Guia do usuário do IAM.

Conta da AWS usuário-raiz

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em Tarefas que exigem credenciais de usuário-raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte O que é o IAM Identity Center? no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias no Guia do usuário do IAM.

Um grupo do IAM especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte Casos de uso de usuários do IAM no Guia do usuário do IAM.

Perfis do IAM

Uma perfil do IAM é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função mudando de um usuário para uma função do IAM (console) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte Métodos para assumir um perfil no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte Visão geral das políticas JSON no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Identity-based políticas

Identity-based políticas são documentos de políticas de permissões JSON que você anexa a uma identidade (usuário, grupo ou função). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Identity-based as políticas podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Resource-based políticas

Resource-based políticas são documentos de política JSON que você anexa a um recurso. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário especificar uma entidade principal em uma política baseada em recursos.

Resource-based políticas são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do usuário do IAM.
- Políticas de Controle de Serviços (SCPs): as SCPs especificam o número máximo de permissões para uma organização ou uma unidade organizacional no AWS Organizations. Para saber mais, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs): definem o número máximo de permissões disponíveis para recursos em suas contas. Consulte mais informações em Resource control policies (RCPs) no Guia do usuário do AWS Organizations .
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como o EventBridge Scheduler funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao EventBridge Scheduler, saiba quais recursos do IAM estão disponíveis para uso com o EventBridge Scheduler.

Recursos do IAM que você pode usar com o Amazon EventBridge Scheduler

Recurso do IAM	EventBridge Suporte ao agendador
Identity-based políticas	Sim
Resource-based políticas	Não
Ações de políticas	Sim
Recursos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC (tags em políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Sim
Perfis de serviço	Sim
Service-linked funções	Não

Para ter uma visão de alto nível de como o EventBridge Scheduler e outros AWS serviços funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Identity-based políticas para o EventBridge Scheduler

Compatível com políticas baseadas em identidade: sim

Identity-based políticas são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como um usuário do IAM, um grupo de usuários ou uma função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais atributos e em que condições. Para saber como criar uma política baseada em identidade, consulte Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elemento de política JSON do IAM no Guia do usuário do IAM.

Identity-based exemplos de políticas para o EventBridge Scheduler

Para ver exemplos de políticas baseadas em identidade do EventBridge Scheduler, consulte. Usando políticas baseadas em identidade no Scheduler EventBridge

Resource-based políticas dentro do EventBridge Scheduler

Compatibilidade com políticas baseadas em recursos: não

Resource-based políticas são documentos de política JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. É necessário especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, é possível especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em recursos. Consulte mais informações em Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações de política para o EventBridge Scheduler

Compatível com ações de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do EventBridge Agendador, consulte Ações definidas pelo Amazon EventBridge Scheduler na Referência de Autorização de Serviço.

As ações de política no EventBridge Scheduler usam o seguinte prefixo antes da ação:

```
scheduler
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Você também pode especificar várias ações usando caracteres-curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

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

Recursos de política para o EventBridge Scheduler

Compatível com recursos de políticas: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Para ações que não oferecem compatibilidade com permissões em nível de recurso, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do EventBridge Scheduler e seus ARNs, consulte Recursos definidos pelo Amazon EventBridge Scheduler na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas pelo Amazon EventBridge Scheduler.

Para ver exemplos de políticas baseadas em identidade do EventBridge Scheduler, consulte. Usando políticas baseadas em identidade no Scheduler EventBridge

Chaves de condição de política para o EventBridge Scheduler

Compatível com chaves de condição de política específicas de serviço: sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` especifica quando as instruções são executadas com base em critérios definidos. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do EventBridge Scheduler, consulte Chaves de condição do Amazon EventBridge Scheduler na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon EventBridge Scheduler.

Para ver exemplos de políticas baseadas em identidade do EventBridge Scheduler, consulte. Usando políticas baseadas em identidade no Scheduler EventBridge

ACLs no Scheduler EventBridge

Compatível com ACLs: não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com Scheduler EventBridge

Compatível com ABAC (tags em políticas): parcial

Attribute-based controle de acesso (ABAC) é uma estratégia de autorização que define permissões com base em atributos chamados de tags. Você pode anexar tags a entidades e AWS recursos do IAM e, em seguida, criar políticas ABAC para permitir operações quando a tag do diretor corresponder à tag no recurso.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço for compatível com as três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço for compatível com as três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para saber mais sobre o ABAC, consulte Definir permissões com autorização do ABAC no Guia do usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Usar controle de acesso por atributo (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com EventBridge o Scheduler

Compatível com credenciais temporárias: sim

As credenciais temporárias fornecem acesso de curto prazo aos AWS recursos e são criadas automaticamente quando você usa a federação ou troca de funções. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para ter mais informações, consulte Credenciais de segurança temporárias no IAM e Serviços da Serviços da AWS que funcionam com o IAM no Guia do usuário do IAM.

Cross-service permissões principais para o EventBridge Scheduler

Compatibilidade com o recurso de encaminhamento de sessões de acesso (FAS): sim

As sessões de acesso direto (FAS) usam as permissões do principal chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) de fazer solicitações aos serviços posteriores. Para obter detalhes da política ao fazer solicitações de FAS, consulte Sessões de acesso direto.

Funções de serviço do EventBridge Scheduler

Compatível com perfis de serviço: sim

O perfil de serviço é um perfil do IAM que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para saber

mais, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do EventBridge Agendador. Edite as funções de serviço somente quando o EventBridge Agendador fornecer orientação para fazer isso.

Service-linked funções para o EventBridge Scheduler

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir a função de realizar uma ação em seu nome. Service-linked as funções aparecem no seu Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte Serviços da AWS que funcionam com o IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna de Service-linked função. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Usando políticas baseadas em identidade no Scheduler EventBridge

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do EventBridge Agendador. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM.

Para aprender a criar uma política baseada em identidade do IAM ao usar esses documentos de política em JSON de exemplo, consulte Criar políticas do IAM (console) no Guia do usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo EventBridge Scheduler, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição do Amazon EventBridge Scheduler na Referência de Autorização de Serviço.

Tópicos

- Práticas recomendadas de política

- EventBridge Permissões do agendador
- AWS políticas gerenciadas para o EventBridge Scheduler
- Políticas gerenciadas pelo cliente para o EventBridge Scheduler
- AWS atualizações de políticas gerenciadas

Práticas recomendadas de política

Identity-based as políticas determinam se alguém pode criar, acessar ou excluir recursos do EventBridge Scheduler em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para saber mais, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para saber mais sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: é possível adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, é possível escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como CloudFormation. Para saber mais, consulte Elementos da política JSON do IAM: condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a criar políticas seguras e funcionais. Para saber mais, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para saber mais, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para saber mais sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

EventBridge Permissões do agendador

Para que um diretor do IAM (usuário, grupo ou função) crie EventBridge agendamentos no Scheduler e acesse os recursos do EventBridge Scheduler por meio do console ou da API, o diretor deve ter um conjunto de permissões adicionado à sua política de permissões. Você pode configurar essas permissões dependendo da função de trabalho da entidade principal. Por exemplo, um usuário ou função que usa apenas o console do EventBridge Scheduler para visualizar uma lista de agendamentos existentes não precisa ter as permissões necessárias para chamar a operação da `CreateSchedule` API. Recomendamos personalizar suas permissões baseadas em identidade para fornecer somente o acesso com privilégio mínimo.

A lista a seguir mostra os recursos do EventBridge Scheduler e suas ações suportadas correspondentes.

- Programação
  - `scheduler:ListSchedules`
  - `scheduler:GetSchedule`
  - `scheduler:CreateSchedule`
  - `scheduler:UpdateSchedule`
  - `scheduler:DeleteSchedule`
- Grupo de agendamento
  - `scheduler:ListScheduleGroups`
  - `scheduler:GetScheduleGroup`
  - `scheduler:CreateScheduleGroup`
  - `scheduler:DeleteScheduleGroup`
  - `scheduler:ListTagsForResource`
  - `scheduler:TagResource`

- `scheduler:UntagResource`

Você pode usar as permissões do EventBridge Scheduler para criar suas próprias políticas gerenciadas pelo cliente para usar com o EventBridge Scheduler. Você também pode usar as políticas AWS gerenciadas descritas na seção a seguir para conceder as permissões necessárias para casos de uso comuns sem precisar gerenciar suas próprias políticas.

AWS políticas gerenciadas para o EventBridge Scheduler

AWS aborda muitos casos de uso comuns fornecendo políticas autônomas do IAM que AWS criam e administram. Políticas gerenciadas, ou predefinidas, concedem as permissões necessárias para casos de uso comuns para que você não precise investigar quais permissões são necessárias. Para saber mais, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM. As seguintes políticas AWS gerenciadas que você pode anexar aos usuários em sua conta são específicas do EventBridge Scheduler:

- AmazonEventBridgeSchedulerFullAccess

  Concede permissões para usar todas as ações EventBridge do Agendador para agendas e grupos de agendas.

  Para visualizar as permissões para esta política, consulte AmazonEventBridgeSchedulerFullAccess na Referência de políticas gerenciadas pela AWS .
- AmazonEventBridgeSchedulerReadOnlyAccess

  Concede permissões somente leitura para visualizar detalhes sobre seus agendamentos e grupos de agendamentos.

  Para visualizar as permissões para esta política, consulte AmazonEventBridgeSchedulerReadOnlyAccess na Referência de políticas gerenciadas pela AWS .

Políticas gerenciadas pelo cliente para o EventBridge Scheduler

Use os exemplos a seguir para criar suas próprias políticas gerenciadas pelo cliente para o EventBridge Scheduler. As políticas gerenciadas pelo cliente permitem que você conceda permissões somente para as ações e recursos necessários para aplicativos e usuários em sua equipe, de acordo com a função de trabalho da entidade principal.

Tópicos

- Exemplo: CreateSchedule
- Exemplo: GetSchedule
- Exemplo: UpdateSchedule
- Exemplo: DeleteScheduleGroup

Exemplo: `CreateSchedule`

Ao criar um novo agendamento, você escolhe se deseja criptografar seus dados no EventBridge Scheduler usando uma chave gerenciada pelo cliente ou uma Chave pertencente à AWSchave gerenciada pelo cliente.

A política a seguir permite que uma entidade principal crie um agendamento e aplique criptografia usando uma Chave pertencente à AWS. Com um Chave pertencente à AWS, AWS gerencia recursos ativados AWS Key Management Service (AWS KMS) para você, para que você não precise de permissões adicionais para interagir AWS KMS.

JSON

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

Use a política a seguir para permitir que um diretor crie uma agenda e use uma chave gerenciada pelo AWS KMS cliente para criptografia. Para usar uma chave gerenciada pelo cliente, o diretor deve ter permissão para acessar os AWS KMS recursos em sua conta. Essa política concede acesso a uma única chave KMS especificada para ser usada para criptografar dados no EventBridge Scheduler. Como alternativa, você pode usar um caractere curinga (*) para conceder acesso a todas as chaves em uma conta ou a um subconjunto que corresponda a um determinado padrão de nome.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:CreateSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
            "arn:aws:scheduler:us-east-1:123456789012: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"
            ],
            "Condition": {
                "StringLike": {
                "kms:ViaService": "scheduler.us-east-1.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"
                }
            }
        }
    ]
}
```

Exemplo: **`GetSchedule`**

Use a política a seguir para permitir que uma entidade principal obtenha informações sobre um agendamento.

JSON

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

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

Exemplo: **`UpdateSchedule`**

Use as políticas a seguir para permitir que uma entidade principal atualize um agendamento chamando a ação `scheduler:UpdateSchedule`. Da mesma forma`CreateSchedule`, a política depende se o cronograma usa uma chave gerenciada pelo cliente AWS KMS Chave pertencente à AWS ou uma chave gerenciada pelo cliente para criptografia. Para um agendamento configurado com um Chave pertencente à AWS, use a seguinte política:

JSON

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

Para um agendamento configurado com uma chave gerenciada pelo cliente, use a política a seguir. Essa política inclui permissões adicionais que permitem que um diretor acesse AWS KMS recursos em sua conta:

JSON

```
{
    "Version":"2012-10-17",
    "Statement":
    [
        {
            "Action":
            [
                "scheduler:UpdateSchedule"
            ],
            "Effect": "Allow",
            "Resource":
            [
            "arn:aws:scheduler:us-east-1:123456789012: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"
            ],
```

```
            "Condition": {
                "StringLike": {
                "kms:ViaService": "scheduler.us-east-1.amazonaws.com",
                    "kms:EncryptionContext:aws:scheduler:schedule:arn":
 "arn:aws:scheduler:us-east-1:123456789012:schedule/my-group/my-schedule-name"
            }
        }
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/*",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "scheduler.amazonaws.com"
                }
            }
        }
    ]
}
```

Exemplo: **`DeleteScheduleGroup`**

Use a política a seguir para permitir que uma entidade principal exclua um grupo de agendamentos. Ao excluir um grupo, você também exclui os agendamentos associados a esse grupo. A entidade principal que exclui o grupo deve ter permissão para também excluir os agendamentos associados a esse grupo. Essa política concede uma permissão da entidade principal para chamar a ação `scheduler:DeleteScheduleGroup` nos grupos de agendamentos especificados, bem como em todos as agendamentos do grupo:

> **Note**
>
> EventBridge O Scheduler não suporta a especificação de permissões em nível de recurso para agendas individuais. Por exemplo, a declaração a seguir é inválida e não deve ser incluída em sua política.
> `"Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"`

JSON

```
{
    "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 atualizações de políticas gerenciadas

Alteração	Descrição	Data
AmazonEventBridgeSchedulerFullAccess: Nova política gerenciada	EventBridge O Scheduler adiciona suporte a uma nova política gerenciada que concede aos usuários acesso total a todos os recursos,	10 de novembro de 2022

Alteração	Descrição	Data
	incluindo agendas e grupos de agendamentos.	
AmazonEventBridgeSchedulerReadOnlyAccess: Nova política gerenciada	EventBridge O Scheduler adiciona suporte a uma nova política gerenciada que concede aos usuários acesso somente de leitura a todos os recursos, incluindo agendas e grupos de agendamentos.	10 de novembro de 2022
AmazonEventBridgeSchedulerReadOnlyAccess— Política gerenciada atualizada	EventBridge O Scheduler atualizou a política `AmazonEventBridgeSchedulerReadOnlyAccess` gerenciada para usar ações curinga (`scheduler:List* escheduler:Get*`) para garantir que a política permaneça atualizada à medida que novas ações somente para leitura forem adicionadas.	25 de março de 2026
EventBridge O agendador começou a rastrear as alterações	EventBridge O Scheduler começou a monitorar as alterações em suas políticas AWS gerenciadas.	10 de novembro de 2022

Prevenção delegada confusa no EventBridge Scheduler

O problema "confused deputy" é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. Cross-service a representação pode ocorrer quando um serviço (o serviço de chamada) chama

outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as `aws:SourceArn`chaves de contexto de condição `aws:SourceAccount`global em sua função de execução do cronograma para limitar as permissões que o EventBridge Agendador concede a outro serviço para acessar o recurso. Use `aws:SourceArn` se quiser que apenas um recurso seja associado ao acesso entre serviços. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema do substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o ARN completo do recurso. A seguinte condição tem como escopo um grupo de agendamento individual: `arn:aws:scheduler:*:`*`123456789012`*`:schedule-group/`*`your-schedule-group`*

Se você não souber o ARN completo do recurso ou especificar vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curinga (`*`) para as partes desconhecidas do ARN. Por exemplo: `arn:aws:scheduler:*:`*`123456789012`*`:schedule-group/*`.

O valor de `aws:SourceArn` deve ser o ARN do grupo de EventBridge agendamentos do Scheduler para o qual você deseja definir o escopo dessa condição.

> **Important**
>
> Não defina o escopo da instrução `aws:SourceArn` para um agendamento específico ou um prefixo de nome de agendamento. O ARN que você especificar deve ser um grupo de agendamentos.

O exemplo a seguir mostra como é possível usar as chaves de contexto de condição globais `aws:SourceArn` e `aws:SourceAccount` na sua função de política de confiança de execução para evitar o problema de segurança delegada confusa.

JSON

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

Se você usar caracteres curinga no valor de`aws:SourceArn`, deverá usar `ArnLike` em vez de `StringEquals` como operador de condição. Por exemplo, a política de confiança a seguir é usada `ArnLike` para corresponder a qualquer grupo de agendamento na conta:

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

```
                    "aws:SourceAccount": "123456789012"
                }
            }
        }
    ]
}
```

Solução de problemas de identidade e acesso ao Amazon EventBridge Scheduler

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o EventBridge Scheduler e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no EventBridge Scheduler
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS para acessar meus recursos do EventBridge Scheduler

Não estou autorizado a realizar uma ação no EventBridge Scheduler

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para exibir detalhes sobre um recurso do *`my-example-widget`* fictício, mas não tem as permissões fictícias do `scheduler:`*`GetWidget`*.

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

Nesse caso, a política de Mateo deve ser atualizada para permitir que ele tenha acesso ao recurso *`my-example-widget`* usando a ação `scheduler:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o EventBridge Agendador.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no EventBridge Scheduler. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS para acessar meus recursos do EventBridge Scheduler

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), é possível usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o EventBridge Scheduler oferece suporte a esses recursos, consulteComo o EventBridge Scheduler funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.

- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Proteção de dados no Amazon EventBridge Scheduler

O modelo de responsabilidade AWS compartilhada O modelo de se aplica à proteção de dados no Amazon EventBridge Scheduler. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Perguntas frequentes sobre privacidade de dados . Para obter informações sobre proteção de dados na Europa, consulte o Centro de Regulamento Geral sobre a Proteção de Dados (RGPD).

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.

- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o EventBridge Scheduler ou outro Serviços da AWS usando o console, a API ou os AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Criptografia em repouso no EventBridge Scheduler

Esta seção descreve como o Amazon EventBridge Scheduler criptografa e descriptografa seus dados em repouso. Os dados em repouso são dados armazenados no EventBridge Scheduler e nos componentes subjacentes do serviço. EventBridge O Scheduler se integra com AWS Key Management Service (AWS KMS) para criptografar e descriptografar seus dados usando um. AWS KMS key EventBridge O Scheduler oferece suporte a dois tipos de chaves KMS: Chaves pertencentes à AWSe chaves gerenciadas pelo cliente.

> **Note**
>
> EventBridge O Scheduler só suporta o uso de chaves KMS de criptografia simétrica.

Chaves pertencentes à AWSsão chaves KMS que um AWS serviço possui e gerencia para uso em várias AWS contas. Embora os usos do Chaves pertencentes à AWS EventBridge Agendador não estejam armazenados em sua AWS conta, o EventBridge Agendador os usa para proteger seus dados e recursos. Por padrão, o EventBridge Scheduler criptografa e descriptografa todos os seus dados usando uma chave própria. AWS Você não precisa gerenciar sua Chave pertencente à AWS ou a política de acesso dela. Você não incorre em nenhuma taxa quando o EventBridge Scheduler usa Chaves pertencentes à AWS para proteger seus dados, e o uso deles não conta como parte de suas AWS KMS cotas em sua conta.

As chaves gerenciadas pelo cliente são chaves KMS armazenadas em sua AWS conta que você cria, possui e gerencia. Se seu caso de uso específico exigir que você controle e audite as chaves

de criptografia que protegem seus dados no EventBridge Scheduler, você pode usar uma chave gerenciada pelo cliente. Se você escolher uma chave gerenciada pelo cliente, será necessário gerenciar sua política de chave. Chaves gerenciadas pelo cliente geram uma taxa mensal e uma taxa para uso que excede o nível gratuito. Usar uma chave gerenciada pelo cliente também conta como parte da sua cota do AWS KMS. Para obter mais informações sobre a definição de preço, consulte Definição de preço do AWS Key Management Service.

Tópicos

- Artefatos de criptografia
- Gerenciando chaves KMS
- CloudTrail exemplo de evento

Artefatos de criptografia

A tabela a seguir descreve os diferentes tipos de dados que o EventBridge Scheduler criptografa em repouso e que tipo de chave KMS ele suporta para cada categoria.

Tipo de dados	Description	Chave pertencente à AWS	chave gerenciada pelo cliente
Carga útil (até 256 KB)	Os dados que você especifica no parâmetro `TargetInput` do agendamento ao configurar o agendamento para ser entregue ao destino.	Compatível	Compatível
Identificador e estado	O nome exclusivo e o estado (ativar, desativar) da agenda.	Compatível	Não compatível
Configuração de agendamento.	A expressão de agendamento, como a expressão cron ou	Compatível	Não compatível

Tipo de dados	Description	Chave pertencente à AWS	chave gerenciada pelo cliente
	rate para agendamentos recorrentes, e o carimbo de data/hora para invocações únicas, bem como a data de início, a data de término e o fuso horário do agendamento.		
Configurações de destino	O nome do recurso da Amazon (ARN) e outros detalhes de configuração relacionados ao destino.	Compatível	Não compatível
Configuração de invocação e comportamento de falha	Configuração de janela de tempo flexível, a política de repetição do agendamento e os detalhes da fila de mensagens não entregues usados para entregas malsucedidas.	Compatível	Não compatível

EventBridge O Scheduler usa suas chaves gerenciadas pelo cliente somente ao criptografar e descriptografar a carga de destino, conforme descrito na tabela anterior. Se você optar por usar uma chave gerenciada pelo cliente, o EventBridge Scheduler criptografará e descriptografará a carga duas vezes: uma usando o padrão Chave pertencente à AWS e outra usando a chave gerenciada pelo cliente que você especificar. Para todos os outros tipos de dados, o EventBridge Scheduler usa apenas o padrão Chave pertencente à AWS para proteger seus dados em repouso.

Use a the section called “Gerenciando chaves KMS” seção a seguir para saber como você deve gerenciar seus recursos e políticas de chaves do IAM para usar uma chave gerenciada pelo cliente com o EventBridge Scheduler.

Gerenciando chaves KMS

Opcionalmente, você pode fornecer uma chave gerenciada pelo cliente para criptografar e descriptografar a carga útil que sua agenda entrega ao destino. EventBridge O Scheduler criptografa e descriptografa sua carga útil de até 256 KB de dados. Utilizar uma chave gerenciada pelo cliente gera uma taxa mensal e uma taxa que excede o nível gratuito. Usar uma chave gerenciada pelo cliente conta como parte da sua cota do AWS KMS. Para obter mais informações sobre a definição de preço, consulte Definição de preço do AWS Key Management Service.

EventBridge O Scheduler usa permissões do IAM associadas ao principal que cria um cronograma para criptografar seus dados. Isso significa que você deve anexar as permissões AWS KMS relacionadas necessárias ao usuário ou função que chama a API EventBridge Scheduler. Além disso, o EventBridge Scheduler usa políticas baseadas em recursos para descriptografar seus dados. Isso significa que a função de execução associada à sua agenda também deve ter as permissões AWS KMS relacionadas necessárias para chamar a AWS KMS API ao descriptografar dados.

> **Note**
>
> EventBridge O Scheduler não suporta o uso de concessões para permissões temporárias.

Use a seção a seguir para saber como você pode gerenciar sua política de AWS KMS chaves e as permissões necessárias do IAM para usar uma chave gerenciada pelo cliente no EventBridge Scheduler.

Tópicos

- Adicionar permissões do IAM
- Gerenciar a política de chave

Adicionar permissões do IAM

Para usar uma chave gerenciada pelo cliente, você deve adicionar as seguintes permissões à entidade principal do IAM baseado em identidade que cria um agendamento, bem como à função de execução que você associa ao agendamento:

Identity-based permissões para chaves gerenciadas pelo cliente

Você deve adicionar as seguintes AWS KMS ações à política de permissão associada a qualquer principal (usuários, grupos ou funções) que chame a API EventBridge Scheduler ao criar um agendamento.

- **`kms:DescribeKey`**: necessário para validar se a chave fornecida é uma chave do KMS de criptografia simétrica.
- **`kms:GenerateDataKey`**— Necessário para gerar a chave de dados que o EventBridge Scheduler usa para realizar a criptografia do lado do cliente.
- **`kms:Decrypt`**— É necessário descriptografar a chave de dados criptografada que o EventBridge Scheduler armazena junto com seus dados criptografados.

Estas ações se somam às seguintes:

- **`scheduler:*`**
- **`iam:PassRole`**: necessário para passar o perfil de execução.

Permissões da função de execução para chaves gerenciadas pelo cliente

Você deve adicionar a ação a seguir à política de permissões da função de execução do seu cronograma para fornecer acesso ao EventBridge Scheduler para chamar a AWS KMS API ao descriptografar seus dados.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowEventBridgeSchedulerToDecryptDataUsingCMKMS",
            "Effect": "Allow",
            "Action": [
```

```
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:123456789012:key/your-key-id"
        }
    ]
}
```

- **`kms:Decrypt`**— É necessário descriptografar a chave de dados criptografada que o EventBridge Scheduler armazena junto com seus dados criptografados.

Se você usar o console do EventBridge Scheduler para criar uma nova função de execução ao criar um novo EventBridge agendamento, o Scheduler anexará automaticamente a permissão necessária à sua função de execução. No entanto, se você escolher uma função de execução existente, deverá adicionar as permissões necessárias à função para poder usar suas chaves gerenciadas pelo cliente.

Gerenciar a política de chave

Quando você cria uma chave gerenciada pelo cliente usando AWS KMS, por padrão, sua chave tem a seguinte política de chaves para fornecer acesso às funções de execução de seus cronogramas.

Opcionalmente, você pode limitar o escopo da sua política de chave para fornecer acesso somente à função de execução. Você pode fazer isso se quiser usar sua chave gerenciada pelo cliente somente com os recursos do EventBridge Scheduler. Use o exemplo de política de chaves a seguir para limitar quais recursos do EventBridge Scheduler podem usar sua chave.

CloudTrail exemplo de evento

AWS CloudTrail captura todos os eventos de chamadas de API. Isso inclui chamadas de API sempre que o EventBridge Scheduler usa sua chave gerenciada pelo cliente para descriptografar seus dados. O exemplo a seguir mostra uma entrada de CloudTrail evento que demonstra o EventBridge Scheduler usando a `kms:Decrypt` ação usando uma chave gerenciada pelo cliente.

```
{
  "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"
  }
}
```

Criptografia em trânsito no EventBridge Scheduler

EventBridge O Scheduler criptografa seus dados em trânsito enquanto eles viajam pela rede. O Transport Layer Security (TLS) criptografa seus dados quando você chama qualquer operação da API do EventBridge Scheduler, bem como quando o EventBridge Scheduler chama qualquer API de destino ao invocar sua agenda. Por padrão, o EventBridge Scheduler usa o TLS 1.2 ao criptografar seus dados em trânsito. Você não precisa configurar a criptografia em trânsito e não pode escolher uma versão diferente do TLS ao usar o EventBridge Scheduler.

Usando a API EventBridge Scheduler — Quando você executa uma operação de API, como`CreateSchedule`, por exemplo, o EventBridge Scheduler criptografa toda a solicitação HTTP, incluindo o corpo e os cabeçalhos da solicitação. EventBridge O Scheduler também criptografa todo o objeto de resposta que você recebe de nossas APIs.

Usando APIs de destino — Quando o EventBridge Scheduler invoca sua agenda, ele chama a API de destino que você especificou ao criar a agenda. Ao entregar um evento a um destino, o EventBridge Scheduler criptografa toda a solicitação, incluindo o corpo da solicitação e todos os cabeçalhos, bem como a resposta que recebe do destino.

Validação de conformidade para Amazon EventBridge Scheduler

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a Documentação AWS de segurança.

Resiliência no Amazon Scheduler EventBridge

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o EventBridge Scheduler oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

Segurança da infraestrutura no Amazon EventBridge Scheduler

Como um serviço gerenciado, o Amazon EventBridge Scheduler é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o EventBridge Scheduler pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Suítes de criptografia com sigilo direto perfeito (PFS), como DHE (Ephemeral) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Monitoramento e métricas do Agendador do Amazon EventBridge

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance do Agendador do Amazon EventBridge e das outras soluções da AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar o Agendador do EventBridge, informar quando algo está errado e realizar ações automaticamente quando apropriado.

- O Amazon CloudWatch monitora os recursos da AWS e os aplicativos que você executa na AWS em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Para mais informações, consulte o Guia do usuário do Amazon CloudWatch.
- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 especificado por você. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem no qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Tópicos

- Monitorando o Amazon EventBridge Scheduler com a Amazon CloudWatch
- Registro de chamadas da API Agendador do Amazon EventBridge usando o AWS CloudTrail

Monitorando o Amazon EventBridge Scheduler com a Amazon CloudWatch

Você pode monitorar o Amazon EventBridge Scheduler usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. EventBridge O Scheduler emite um conjunto de métricas para todos os agendamentos e um conjunto adicional de métricas para agendamentos que têm uma fila de cartas mortas (DLQ) associada. Se você configurar uma DLQ para sua agenda, o EventBridge Scheduler publicará métricas adicionais quando sua agenda esgotar sua política de repetição.

Essas estatísticas são mantidas por 15 meses, para que você possa acessar informações históricas e obter uma perspectiva melhor sobre por que um agendamento está falhando e solucionar

problemas subjacentes. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

> **Best-effort CloudWatch entrega de métricas**
>
> CloudWatch as métricas são fornecidas com base no melhor esforço. A maioria das operações EventBridge do Scheduler resulta no envio de um ponto de dados para CloudWatch. A integridade e pontualidade das métricas não são garantidas. Um ponto de dados de um determinado minuto pode demorar para ser CloudWatch disponibilizado ou pode não ser entregue. CloudWatch as métricas dão uma ideia da natureza da atividade quase em tempo real. Eles não pretendem ser uma contabilidade completa de todas as operações.

Tópicos

- Termos
- Dimensões
- Acesso às métricas do
- Lista de métricas
- EventBridge Métricas de uso do agendador

Termos

Namespace

Um namespace é um contêiner para as CloudWatch métricas de um AWS serviço. Para o EventBridge Scheduler, o namespace é. `AWS/Scheduler`

CloudWatch métricas

Uma CloudWatch métrica representa um conjunto ordenado por tempo de pontos de dados específicos de CloudWatch.

Dimensão

Uma dimensão é um name/value par que faz parte da identidade de uma métrica.

Unidade

Uma estatística tem uma unidade de medida. Para o EventBridge Scheduler, as unidades incluem Count.

Dimensões

Esta seção descreve o agrupamento de CloudWatch dimensões para métricas do EventBridge Scheduler em. CloudWatch

Dimensão	Description
ScheduleGroup	O grupo de agendamentos para o qual você deseja visualizar as métricas usando CloudWatch. Se você ainda não criou nenhum grupo, o EventBridge Scheduler associa suas agendas ao grupo. `default`

Acesso às métricas do

Esta seção descreve como acessar as métricas de desempenho de um cronograma específico do EventBridge Scheduler. CloudWatch

Para visualizar as métricas de desempenho para uma dimensão

1. Abra a página Métricas no CloudWatch console.
2. Use o seletor de AWS região para escolher a região para sua programação
3. Escolha o Agendador do namespace.
4. Na guia Todas as métricas, escolha uma dimensão, por exemplo, Agendar métricas do grupo. Para ver as métricas de todos os agendamentos que você criou na região selecionada, escolha Métricas da conta.
5. Escolha uma CloudWatch métrica para uma dimensão. Por exemplo, InvocationAttemptCountou InvocationDroppedCount, em seguida, escolha Pesquisa gráfica.
6. Escolha a guia Métricas representadas graficamente para visualizar as estatísticas de desempenho das métricas do EventBridge Scheduler.

Lista de métricas

As tabelas a seguir listam as métricas de todas as EventBridge programações do Scheduler, bem como métricas adicionais das programações para as quais você configurou uma DLQ.

Métricas para todos os agendamentos

Namespace	Métrica	Unidade	Description
AWS/Scheduler	InvocationAttemptCount	Contagem	Emitido para cada tentativa de invocação. Use essa métrica para verificar se o EventBridge Scheduler está tentando invocar suas agendas e para ver quando as invocações se aproximam das cotas de sua conta.
AWS/Scheduler	TargetErrorCount	Contagem	Emitido quando o destino retorna uma exceção após o EventBridge Scheduler chamar a API de destino. Use isso para verificar quando a entrega para um destino falha.
AWS/Scheduler	TargetErrorThrottledCount	Contagem	Emitido quando a invocação do destino falha devido ao controle de utilização da API pelo destino. Use isso para diagnosticar falhas

Namespace	Métrica	Unidade	Description
			de entrega quando o motivo subjacent e são as chamadas de limitação da API de destino feitas pelo Scheduler. EventBrid ge
AWS/Scheduler	InvocationThrottleCount	Contagem	Emitido quando o EventBridge Scheduler limita uma invocação de destino porque excede suas cotas de serviço definidas pelo Scheduler. EventBrid ge Use isso para identificar situações em que você excedeu sua cota limite de controle de utilização de invocações. Para obter mais informaçõ es sobre Service Quotas, consulte Cotas.

Namespace	Métrica	Unidade	Description
AWS/Scheduler	InvocationDroppedCount	Contagem	Emitido quando o EventBridge Scheduler para de tentar invocar o alvo após o esgotamento da política de repetição de um agendamento. Para obter mais informações sobre políticas de repetição, consulte a Referência RetryPolicyda API EventBridge Scheduler.

Métricas para agendamentos com uma DLQ

Namespace	Métrica	Unidade	Description
AWS/Scheduler	InvocationsSentToDeadLetterCount	Contagem	Emitido para cada entrega bem-sucedida na DLQ de um agendamento. Use isso para determinar quando os eventos são enviados para uma DLQ e, em seguida,

Namespace	Métrica	Unidade	Description
			verifique o evento entregue à DLQ do agendamento para obter detalhes adicionais que o ajudem a determinar a causa da falha.

Namespace	Métrica	Unidade	Description
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount	Contagem	Emitido quando o EventBridge Scheduler não consegue entregar um evento ao DLQ. Use essas duas métricas para determinar o motivo pelo qual o EventBridge Scheduler não consegue enviar um evento para a DLQ e modifique sua configuração de DLQ para resolver o problema. Veja a seguir um exemplo da métrica InvocationsFailedToBeSentToDeadLetterCount_<e
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount_<error_code>	Contagem	

Namespace	Métrica	Unidade	Description
			rror_code > quando a fila do Amazon SQS que você especifica como DLQ não existe: InvocationsFailedToBeSentToDeadLetterCount_ **AWS.SimpleQueueService.NonExistentQueue**

Namespace	Métrica	Unidade	Description
AWS/Scheduler	InvocationsSentToDeadLetterCount_Truncated_MessageSizeExceeded	Contagem	Emitido quando a carga útil do evento enviada para a DLQ excede o tamanho máximo permitido pelo Amazon SQS, e o EventBridge Scheduler trunca a carga que você especifica no atributo de uma programação. Input

EventBridge Métricas de uso do agendador

CloudWatch coleta métricas que rastreiam o uso de alguns AWS recursos. Essas métricas correspondem às cotas AWS de serviço. O rastreamento dessas métricas pode ajudar a gerenciar as cotas proativamente. Para obter mais informações sobre Service Quotas, consulte Cotas.

Essas métricas estão contidas no AWS/Usage namespace, em vez deAWS/Scheduler, e são coletadas a cada minuto. CloudWatch publica métricas nesse namespace com as dimensõesService,Class, e. Type Resource

Dimensões comuns para métricas de uso

Dimensão	Description
`Service`	O nome do AWS serviço que contém o recurso. Para métricas Agendador do EventBridge de uso, o valor é`Scheduler` .
`Class`	A classe do recurso sob acompanhamento. Para métricas Agendador do EventBridge de uso, o valor é`None`.
`Type`	O tipo de recurso que está sendo acompanhado. Para métricas de uso da API, o valor é`API`. Para métricas de contagem de recursos, o valor é`Resource`.
`Resource`	O recurso específico que está sendo rastreado. Para métricas de uso da API, esse é o nome da operação da API. Para métricas de contagem de recursos, esse é o tipo de recurso que está sendo contado.

Métricas de uso da API

As métricas de uso da API monitoram o número de operações de API realizadas em sua conta. Use essas métricas para monitorar o volume de chamadas de API e gerenciar suas cotas de taxa de API.

O nome da métrica é`CallCount`. A estatística mais útil para essa métrica é `SUM` a que representa a contagem total de operações no período de 1 minuto.

Métricas de uso da API

Métrica	Recurso	Description
`CallCount`	`CreateSchedule`	O número de operações de `CreateSch edule` API realizadas em sua conta.
`CallCount`	`CreateSch eduleGroup`	O número de operações de `CreateSch eduleGroup` API realizadas em sua conta.
`CallCount`	`DeleteSchedule`	O número de operações de `DeleteSch edule` API realizadas em sua conta.

Métrica	Recurso	Description
`CallCount`	`DeleteSch eduleGroup`	O número de operações de `DeleteSch eduleGroup` API realizadas em sua conta.
`CallCount`	`GetSchedule`	O número de operações de `GetSchedule` API realizadas em sua conta.
`CallCount`	`GetSchedu leGroup`	O número de operações de `GetSchedu leGroup` API realizadas em sua conta.
`CallCount`	`ListSched uleGroups`	O número de operações de `ListSched uleGroups` API realizadas em sua conta.
`CallCount`	`ListSchedules`	O número de operações de `ListSchedules` API realizadas em sua conta.
`CallCount`	`ListTagsF orResource`	O número de operações de `ListTagsF orResource` API realizadas em sua conta.
`CallCount`	`TagResource`	O número de operações de `TagResource` API realizadas em sua conta.
`CallCount`	`UntagResource`	O número de operações de `UntagResource` API realizadas em sua conta.
`CallCount`	`UpdateSchedule`	O número de operações de `UpdateSch edule` API realizadas em sua conta.

Por exemplo, a `CallCount` métrica com as dimensões a seguir indica o número de vezes que a operação da `CreateSchedule` API foi chamada em sua conta:

- "Service": "Scheduler"
- “Classe”: “Nenhuma”
- "Type": "API"
- “Recurso”: "CreateSchedule”

Métricas de contagem de recursos

As métricas de contagem de recursos monitoram o número aproximado de recursos em sua conta. Use essas métricas para monitorar quando você está se aproximando dos limites da cota de serviço, permitindo que você solicite aumentos de cota antes de ficar sem capacidade.

O nome da métrica é`ResourceCount`. A estatística mais útil para essa métrica é `Maximum`.

Métricas de contagem de recursos

Métrica	Recurso	Description
`ResourceCount`	`ApproximateSchedule`	Número aproximado de agendamentos em sua conta. Use essa métrica para monitorar quando você está se aproximando do limite da cota de agendamentos, para ajudar a evitar `ServiceQuotaExceededException` erros ao ligar. `CreateSchedule` Quando o número de agendamentos é menor que 1 milhão, essa métrica pode mostrar zero. Para que um alarme notifique quando sua cota de agendamentos estiver se aproximando, recomendamos usar a `Maximum` estatística com um limite de 5 milhões ou mais, já que a cota padrão de agendamentos é de 10 milhões.
`ResourceCount`	`ApproximateScheduleGroup`	Número aproximado de grupos de agendamento em sua conta. Use essa métrica para monitorar quando você está se aproximando do limite de cota de seus grupos de agendamento, para ajudar a evitar `ServiceQuotaExceededException` erros ao ligar. `CreateScheduleGroup`

Por exemplo, a `ResourceCount` métrica com as seguintes dimensões e a `Maximum` estatística indicam o número aproximado de agendamentos em sua conta:

- "Service": "Scheduler"

- “Classe”: “Nenhuma”
- “Tipo”: “Recurso”
- “Recurso”: "ApproximateSchedule”

Registro de chamadas da API Agendador do Amazon EventBridge usando o AWS CloudTrail

O Agendador do Amazon EventBridge é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no Agendador do EventBridge. O CloudTrail captura as chamadas de API do Agendador do EventBridge como eventos. As chamadas capturadas incluem as chamadas do console do Agendador do EventBridge e as chamadas de código para as operações de API do Agendador do EventBridge. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Agendador do EventBridge. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Histórico de eventos. Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Agendador do EventBridge, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o Guia do usuário do AWS CloudTrail.

Informações do Agendador do EventBridge no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando a atividade ocorrer no Agendador do EventBridge, ela será registrada em um evento do CloudTrail juntamente com outros eventos de serviços da AWS no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos em sua Conta da AWS, incluindo eventos do Agendador do EventBridge, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, é possível configurar outros AWS serviços para melhor analisar e agir de acordo com dados coletados do evento nos logs CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configuração notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações da API do Agendador do EventBridge são registradas em log pelo CloudTrail e estão documentadas na Referência de API do Agendador do Amazon EventBridge. Por exemplo, as chamadas às ações `CreateSchedule`, `UpdateSchedule` e `DeleteSchedule` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre as entradas de arquivos de log do Agendador do EventBridge

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros da solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública, portanto, não são exibidos em uma ordem específica.

Cotas para o Amazon EventBridge Scheduler

Sua AWS conta tem cotas padrão, anteriormente chamadas de limites, para cada AWS serviço. Salvo indicação em contrário, cada cota é Region-specific. Você pode solicitar aumentos para a maioria das cotas, mas algumas não podem ser aumentadas.

Para ver as cotas do EventBridge Scheduler, abra o console Service Quotas. No painel de navegação, escolha AWS serviços e selecione EventBridge Agendador.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

> **Note**
>
> As cotas mais comumente referenciadas para o EventBridge Scheduler são Número de agendamentos (padrão 10.000.000 por região, ajustável para bilhões), taxa de CreateSchedule solicitação (5.000 TPS padrão nas regiões primárias, ajustável para dezenas de milhares) e limite de aceleração de invocações (1.000 TPS padrão nas regiões primárias, ajustável para dezenas de milhares). Todos os três são ajustáveis — consulte Solicitando um aumento de cota no Guia do Usuário de Quotas de Serviço para obter detalhes.

Sua AWS conta tem as seguintes cotas relacionadas ao EventBridge Scheduler.

Nome	Padrão	Ajustá	Description
CreateSchedule taxa de solicitação	us-east-1: 5.000 us-east-2: 5.000 us-west-2: 5.000 ap-northeast-1: 5.000 ap-south-1:5.000	Sim	Máximo de CreateSchedule solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo. Isso é ajustável para dezenas de milhares de solicitações por segundo.

Nome	Padrão	Ajustá	Description
	ap-southeast-1:5.000 ap-southeast-2:5.000 eu-central-1:5.000 eu-west-1: 5.000 eu-west-2:5.000 sa-east-1:5.000 Cada uma das outras regiões compatíveis: 250		
CreateScheduleGroup taxa de solicitação	Cada região com suporte: 10	Sim	Máximo de CreateScheduleGroup solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo.

Nome	Padrão	Ajustá	Description
DeleteSchedule taxa de solicitação	us-east-1: 1.000 us-east-2: 1.000 us-west-2: 1.000 ap-northeast-1: 1.000 ap-south-1: 1.000 ap-southeast-1: 1.000 ap-southeast-2: 1.000 eu-central-1: 1.000 eu-west-1: 1.000 eu-west-2: 1.000 sa-east-1: 1.000 Cada uma das outras regiões compatíveis: 250	Sim	Máximo de DeleteSchedule solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo. Isso é ajustável para dezenas de milhares de solicitações por segundo.
DeleteScheduleGroup taxa de solicitação	Cada região com suporte: 10	Sim	Máximo de DeleteScheduleGroup solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo.

Nome	Padrão	Ajustá	Description
GetSchedule taxa de solicitação	us-east-1: 1.000 us-east-2: 1.000 us-west-2: 1.000 ap-northeast-1: 1.000 ap-south-1: 1.000 ap-southeast-1: 1.000 ap-southeast-2: 1.000 eu-central-1: 1.000 eu-west-1: 1.000 eu-west-2: 1.000 sa-east-1: 1.000 Cada uma das outras regiões compatíveis: 250	Sim	Máximo de GetSchedule solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo. Isso é ajustável para dezenas de milhares de solicitações por segundo.
GetScheduleGroup taxa de solicitação	Cada região com suporte: 10	Sim	Máximo de GetScheduleGroup solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo.

Nome	Padrão	Ajustá	Description
Limite de controle de utilização de invocações em transações por segundo	us-east-1: 1.000 us-east-2: 1.000 us-west-2: 1.000 ap-northeast-1: 1.000 ap-south-1: 1.000 ap-southeast-1: 1.000 ap-southeast-2: 1.000 eu-central-1: 1.000 eu-west-1: 1.000 eu-west-2: 1.000 sa-east-1: 1.000 Cada uma das outras regiões compatíveis: 500	Sim	Uma invocação é uma carga útil do cronograma que está sendo entregue ao destino definido. Depois que o limite for atingido, as invocações serão limitadas; isto é, elas ainda acontecem , mas serão atrasadas. Pode ser ajustado para dezenas de milhares de transações por segundo.
ListScheduleGroups taxa de solicitação	Cada região com suporte: 10	Sim	Máximo de ListSched uleGroups solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo.

Nome	Padrão	Ajustá	Description
ListSchedules taxa de solicitação	Cada região compatível: 50	Sim	Máximo de ListSchedules solicitações por segundo. Quando você atinge essa cota, o EventBrid ge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo.
ListTagsForResource taxa de solicitaç ão	Cada região com suporte: 10	Sim	Lista todas as tags associadas ao recurso do Scheduler.
Número de grupos de agendamento	Cada região com suporte: 500	Sim	O número máximo de grupos de cronogramas por região.
Número de esquemas	Cada região compatível: 10.000.000	Sim	O número máximo de cronogramas por região. Essa cota inclui programações únicas com execução concluída . Recomendamos configurar suas agendas para serem excluídas automaticamente após a conclusão do uso do ActionAfterCompletion recurso. Ajustável para bilhões de programações.
TagResource taxa de solicitação	Cada região compatível: 1	Sim	Atribui uma ou mais tags (pares chave-valor) ao recurso especificado do Scheduler.

Nome	Padrão	Ajustá	Description
UntagResource taxa de solicitação	Cada região compatível: 1	Sim	Remove uma ou mais tags do recurso especific ado do Scheduler.
UpdateSchedule taxa de solicitação	us-east-1: 1.000 us-east-2: 1.000 us-west-2: 1.000 ap-northeast-1: 1.000 ap-south-1: 1.000 ap-southeast-1: 1.000 ap-southeast-2: 1.000 eu-central-1: 1.000 eu-west-1: 1.000 eu-west-2: 1.000 sa-east-1: 1.000 Cada uma das outras regiões compatíveis: 250	Sim	Máximo de UpdateSch edule solicitações por segundo. Quando você atinge essa cota, o EventBridge Scheduler rejeita as solicitações dessa operação pelo restante do intervalo. Isso é ajustável para dezenas de milhares de solicitaç ões por segundo.

Para obter mais informações sobre cotas e endpoints de serviço para o EventBridge Scheduler, consulte os endpoints e cotas do Amazon EventBridge Scheduler no guia de referência geral.AWS

Solução de problemas de cotas no Agendador do EventBridge

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados em relação às cotas do Agendador do EventBridge.

ServiceQuotaExceededException

Estou recebendo erros de controle de utilização na taxa de solicitações `CreateSchedule`, `DeleteSchedule`, `GetSchedule` ou `UpdateSchedule`, mesmo estando abaixo do limite de taxa padrão.

Causa comum

Em 7 de setembro de 2023, o Agendador do EventBridge começou a oferecer suporte ao ARN (nome do recurso da Amazon) ScheduleGroup em vez do ARN Schedule nas políticas de confiança de perfil de execução. Os clientes autorizados a continuar usando ARNs Schedule em sua política de confiança podem ter limites de 50 TPS, em vez dos limites padrão de 250 a 1.000 TPS (dependendo da região).

Resolução

Entre em contato com o suporte para solicitar um limite máximo maior.

Prevenção

Modifique suas políticas de confiança existentes de uma das seguintes maneiras:

- Removendo todo o escopo do perfil.
- Definindo o escopo do perfil para que ele possa ser assumido usando o ARN Schedule ou o ARN ScheduleGroup.

  Por exemplo, suponha que você tem a seguinte política de confiança existente:

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

```
        "StringEquals": {
            "aws:SourceArn":
 "arn:aws:scheduler:region:account:schedule/schedule_group/schedule"
        }
    }
}
```

Você poderia atualizar a política de confiança para o seguinte:

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

Solução de problemas do Amazon EventBridge Scheduler

Você pode usar os tópicos desta seção para solucionar problemas comuns do Amazon EventBridge Scheduler.

Tópicos

- Minha agenda falha com erros de destino.
- Problemas com permissões de perfil de execução de agendamento
- Noções básicas e gerenciamento de Service Quotas
- Problemas de padrão de agendamento e tempo de gatilho
- Criação de padrões de agendamento e expressões cron
- Meu destino está sendo acionado?
- Destinos modelados versus destinos universais
- Configurações de entrada de destino universal inválidas
- Agendar atualizações acionando invocações inesperadas
- Desabilitar ou habilitar agendamentos únicos

Minha agenda falha com erros de destino.

As falhas de invocação do Target são um dos problemas mais comuns com EventBridge o Scheduler. Essas falhas podem ocorrer por diversos motivos:

Causas comuns:

- Parâmetros de destino ausentes ou incorretos.
- Problemas de conectividade de rede.
- Controle de utilização de API.
- Configuração de destino incorreta.

Etapas de solução de problemas

1. Configurar uma Dead-Letter fila (DLQ)
   - Uma DLQ ajuda você a capturar e analisar invocações com falha.

- As invocações com falha são enviadas para a DLQ com mensagens de erro detalhadas.
- Para configurar uma DLQ, adicione-a à sua configuração de agendamento:

```
{
    "DeadLetterConfig": {
        "Arn": "arn:aws:sqs:region:account-id:MyDLQ"
    }
}
```

Observação: se sua DLQ estiver criptografada com uma chave KMS, certifique-se de que a política de chaves permita que o EventBridge Scheduler a use:

```
{
    "Sid": "Allow EventBridge Scheduler to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "scheduler.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

2. Verificar parâmetros da API
   - Garanta que todos os parâmetros necessários para as chamadas da API de destino estejam presentes e formatados corretamente.
   - Confira se os valores dos parâmetros estão dentro dos intervalos permitidos.
   - Verifique se o endpoint da API está acessível por meio da sua VPC, caso esteja utilizando endpoints da VPC.
3. Analisar a configuração da rede
   - Se as chamadas falharem devido a problemas transitórios de rede, implemente uma lógica de repetição.
   - Exemplo de política de repetição:

```
{
    "RetryPolicy": {
        "MaximumRetryAttempts": 3,
        "MaximumEventAgeInSeconds": 3600
    }
}
```

4. Conferir configurações específicas do destino
   - Para destinos com modelos (como tarefas do ECS), forneça substituições por meio do parâmetro `Target.Input` da API de criação de agendamento.
   - Verifique se o serviço desejado é compatível e está configurado corretamente.

Problemas com permissões de perfil de execução de agendamento

Problemas com permissões de perfil do IAM são uma causa comum de falhas na execução de agendamentos. Veja como solucionar e resolver esses problemas:

Causas comuns

- Faltam as permissões necessárias para o serviço de destino
- Configuração de perfil incorreta no agendamento
- Falta de relação de confiança com o serviço EventBridge Scheduler
- Permissões insuficientes para acessar recursos criptografados

Sintomas

- `TargetErrorCount`Métrica aumentada em CloudWatch
- Os agendamentos não são executados sem problemas aparentes na configuração do agendamento

Etapas de solução de problemas

1. Monitore CloudWatch métricas

- Verifique a `TargetErrorCount` métrica CloudWatch.

2. Use a Dead-Letter fila (DLQ) para confirmar problemas de permissão
   - Configure uma DLQ para seu agendamento.
   - Se houver problemas de permissão com seu destino e a DLQ estiver configurada corretamente, você verá as invocações com falha na DLQ com mensagens de erro relacionadas a permissões.
   - Se a DLQ permanecer vazia apesar das falhas de execução mostradas nas CloudWatch métricas, isso provavelmente indica um problema de permissões que impede o EventBridge Scheduler de gravar na própria DLQ.

> **Note**
>
> Certifique-se de que a própria DLQ tenha as permissões corretas. Se estiver criptografado, verifique se o EventBridge Agendador tem permissão para usar a chave KMS.

3. Verificar relação de confiança
   - Certifique-se de que sua função do IAM tenha a relação de confiança correta com o EventBridge Scheduler:

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

4. Verificar permissões de função de execução de agendamento
   - O perfil de execução do agendamento requer permissões específicas para invocar diferentes tipos de destino.
   - Exemplos de permissões a serem incluídos na política de perfil de execução do seu agendamento:

```
// For Lambda function targets - add to schedule execution role
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "lambda:InvokeFunction"
        ],
        "Resource": "arn:aws:lambda:region:account-id:function:function-name"
    }]
}

// For SQS queue targets - add to schedule execution role
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "sqs:SendMessage"
        ],
        "Resource": "arn:aws:sqs:region:account-id:queue-name"
    }]
}
```

5. Verificar se o acesso ao recurso está criptografado

   - Se seu destino usa recursos criptografados (por exemplo, filas KMS-encrypted SQS), certifique-se de que sua função tenha permissões para usar a chave KMS:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:region:account-id:key/key-id"
        }
```

```
    ]
}
```

6. Verificar configuração do ARN do perfil
   - Verifique se o ARN da função na sua configuração de agendamento está correto.
   - Verifique se a função existe na mesma Conta da AWS região da sua agenda.

Noções básicas e gerenciamento de Service Quotas

Se você estiver enfrentando problemas ao criar agendas ou ver invocações limitadas, talvez esteja atingindo os limites da cota de serviço. EventBridge O Scheduler tem cotas para o número de agendamentos, grupos de agendamentos e taxas de invocação, que podem variar de acordo com a região.

Identificar problemas de cota

Para determinar se você está atingindo os limites da cota:

1. Monitore CloudWatch métricas
   - Verifique a métrica `InvocationThrottleCount`. Um aumento nessa métrica indica que você está excedendo seu limite de taxa de invocação.
   - Analise a métrica `InvocationAttemptCount` para entender seu uso atual.
2. Preste atenção a mensagens de erro específicas
   - Ao criar ou modificar agendamentos, um `LimitExceededException` indica que você atingiu o número máximo de agendamentos ou grupos de agendamentos.
   - Chamadas de API que exibem erros de controle de utilização sugerem que você está excedendo a cota de solicitações da API.

Solucionar problemas de cota

Se você constatar que está atingindo os limites de cota:

1. Analise e otimize seus agendamentos atuais. Pense em consolidar agendamentos semelhantes ou remover os que não são utilizados.

2. Para controle de utilização da API, implemente a repetição com um intervalo de espera em suas chamadas de API.
3. Se precisar de cotas maiores, solicite um aumento por meio do console de Service Quotas. Selecione EventBridge Agendador, escolha a cota que você precisa aumentar e envie uma solicitação com a justificativa da sua empresa.

Problemas de padrão de agendamento e tempo de gatilho

Às vezes, os usuários encontram problemas em que os agendamentos não são acionados no tempo esperado. Isso geralmente ocorre devido a mal-entendidos sobre padrões de agendamento, mudanças no horário de verão ou janelas de tempo flexíveis.

Causas comuns

- Interpretação incorreta das expressões cron.
- Comportamento inesperado durante mudanças de horário de verão.
- Confusão sobre janelas de tempo flexíveis.
- Incompreensão das expressões rate.

Etapas de solução de problemas

1. Verificar expressões cron
   - Garanta que sua expressão cron esteja formatada corretamente.
   - Observe que não é possível especificar simultaneamente os campos de dia do mês e dia da semana em uma expressão cron.
2. Considerações sobre o fuso horário
   - Selecione o fuso horário de sua preferência ao criar o agendamento.
   - Entenda como o horário de verão afeta sua rotina, pois esse ajuste é baseado no UTC.

   Exemplo do impacto do horário de verão: se você configurar um agendamento para ser executado às 7h GMT:
   - Durante o inverno: o horário de funcionamento é às 7h AM GMT (já que GMT = UTC).
   - Durante o verão: a programação ainda funciona às 7:00 UTC, que agora é 6:00 AM GMT/BST

Se você precisa que o agendamento seja executado no mesmo horário local durante todo o ano, selecione o fuso horário apropriado ao criar o agendamento e verifique como o horário de verão pode afetar esse fuso horário.

3. Noções básicas sobre janelas de tempo flexíveis
   - Janelas de tempo flexíveis permitem que o EventBridge Scheduler otimize as invocações.
   - O agendamento talvez não seja acionado exatamente no início do período.
   - Monitore os horários reais de invocação para entender o comportamento.
4. Revisar expressões cron e rate
   - Verifique se as expressões rate estão formatadas corretamente (por exemplo, `rate(5 minutes)`, `rate(1 hour)`).
   - Tanto para expressões rate quanto para expressões cron, esteja ciente de que as invocações do agendamento não são limitadas ao segundo 0 de um minuto.
   - Os agendamentos podem ser acionados dentro do minuto especificado, mas não necessariamente no início exato do minuto.

   Por exemplo:
   - Um agendamento com `rate(1 hour)` pode começar às 14:00:45, 15:00:32, 16:00:18 etc.
   - Um agendamento cron definido para `0 * * * ? *` (a cada hora) pode ser executado às 14:00:15 PM, 15:00:07 PM, 16:00:52 PM etc.
5. Monitore CloudWatch métricas
   - Use a métrica `InvocationAttemptCount` para verificar se seu agendamento está sendo acionado.
   - Confira `TargetErrorCount` se as invocações estão falhando.
   - Se você configurou uma Dead-Letter fila, monitore `InvocationsSentToDeadLetterCount` para rastrear invocações com falha.

Criação de padrões de agendamento e expressões cron

Os usuários geralmente encontram problemas ao criar padrões de agendamento, principalmente com expressões cron. Conheça alguns problemas comuns e como resolvê-los:

Problemas comuns

- Sintaxe cron incorreta
- Tentativa de usar recursos cron não compatíveis
- Confusão sobre quais campos podem ser usados em conjunto

Etapas de solução de problemas

1. Revisar a sintaxe da expressão cron
   - Certifique-se de que sua expressão cron siga o formato correto: `Minutes Hours Day-of-month Month Day-of-week Year`.
   - Lembre-se de que o EventBridge Scheduler usa o padrão cron com um campo adicional de Ano.
2. Compreender as limitações
   - Não é possível especificar simultaneamente os campos de dia do mês e dia da semana, conforme discutido aqui.
   - As expressões cron que levam a taxas mais rápidas do que 1 minuto não têm suporte.
3. Usar o atributo de pré-visualização do agendamento
   - Ao criar ou editar um cronograma, o EventBridge Scheduler fornece uma prévia dos próximos 10 tempos de execução.
   - Use esta pré-visualização para verificar se o seu agendamento será executado nos horários pretendidos.
   - Se a pré-visualização não corresponder às suas expectativas, revise e ajuste sua expressão cron.

Meu destino está sendo acionado?

Para confirmar se o seu destino está sendo acionado:

1. Verifique CloudWatch as métricas:
   - `InvocationAttemptCount` mostra o número de tentativas de invocação.
   - `TargetErrorCount` indica se alguma invocação falhou.
   - `TargetErrorThrottledCount` mostra se a sua conexão está com controle de utilização.

- `InvocationDroppedCount` indica se alguma invocação foi descartada.

2. Configure uma Dead-Letter fila (DLQ) para capturar e analisar qualquer invocação com falha.

Destinos modelados versus destinos universais

Se você receber um erro como "Solicitação inválida fornecida: [serviço] não é um serviço compatível para o destino", você pode estar tentando usar um serviço não compatível como destino de modelo.

Para resolver esse problema:

1. Verifique se o serviço desejado é compatível como um destino com modelo.
2. Caso não seja compatível, utilize um destino universal e configure-o para fazer a chamada de API apropriada para o seu serviço.

Configurações de entrada de destino universal inválidas

Quando você cria um EventBridge agendamento com uma meta universal, o Scheduler valida o formato ARN de destino, mas não valida o conteúdo do `Input` campo em relação à API do serviço downstream. Isso significa que um agendamento pode ser criado com êxito mesmo que `Input` contenha valores que o serviço de destino rejeitará no momento da invocação.

Os agendamentos com configurações de entrada de destino inválidas são acionados em sua expressão configurada, mas falham em cada invocação. Talvez você não descubra a configuração incorreta até que a programação seja invocada, o que pode ocorrer horas ou dias após a criação.

Sintomas

- O cronograma foi criado sem erros, mas a `TargetErrorCount` CloudWatch métrica aumenta a cada invocação.
- As mensagens do DLQ contêm códigos de erro do serviço de destino (por exemplo, `InvalidParameterValueException` ou`ValidationException`), não`AWS.Scheduler.InternalServerError`.
- A mensagem `ERROR_MESSAGE` na DLQ faz referência a falhas específicas de validação de parâmetros de entrada.

Exemplos

Os exemplos a seguir mostram configurações de entrada inválidas comuns para um alvo AWS Lambda universal ()`arn:aws:scheduler:::aws-sdk:lambda:invoke`.

Qualificadores incompatíveis

Um cronograma com a seguinte entrada especifica a versão 2 no `FunctionName` e a versão 1 no `Qualifier` campo:

```
{
    "FunctionName": "MyFunction:2",
    "Qualifier": "1"
}
```

Esse agendamento foi criado com sucesso, mas todas as invocações falham. A mensagem do DLQ contém:

- `ERROR_CODE`: `InvalidParameterValueException`
- `ERROR_MESSAGE`: `The derived qualifier from the function name does not match the specified qualifier.`

Nome de função inválido

Uma agenda com a seguinte entrada especifica um valor somente de espaço em branco para: `FunctionName`

```
{
    "FunctionName": "     "
}
```

A mensagem do DLQ contém:

- `ERROR_CODE`: `ValidationException`
- `ERROR_MESSAGE`: um erro de validação indicando que o nome da função não corresponde ao padrão exigido.

Como resolver

1. Configure uma DLQ. Sempre configure uma fila de mensagens mortas para agendas que usam destinos universais. Os atributos da mensagem DLQ (`ERROR_CODEeERROR_MESSAGE`) contêm o erro específico retornado pelo serviço de destino, que identifica o parâmetro de entrada inválido.
2. Valide os parâmetros de entrada em relação à API do serviço de destino. Antes de criar um cronograma, verifique se o JSON em seu `Input` campo contém valores válidos chamando diretamente a API de destino. Por exemplo, invoque sua AWS Lambda função com os mesmos parâmetros usando a AWS Lambda `Invoke` API para confirmar se a solicitação foi bem-sucedida.
3. Teste com uma programação única. Crie um agendamento único para verificar se a invocação de destino foi bem-sucedida antes de configurar um agendamento recorrente.
4. Analise a referência da API do serviço de destino. Verifique a referência da API para o serviço que você está almejando para confirmar os parâmetros necessários, os intervalos de valores válidos e as restrições. Para isso AWS Lambda `Invoke`, consulte Invoke no Guia do AWS Lambda desenvolvedor.

Agendar atualizações acionando invocações inesperadas

Ao fazer uma alteração em um agendamento, as invocações talvez não reflitam imediatamente o agendamento atualizado. Permita um curto período para que as alterações entrem em vigor. Por exemplo, se você atualizar um agendamento próximo ao horário de acionamento original, poderá ver uma invocação baseada na configuração original do agendamento.

Desabilitar ou habilitar agendamentos únicos

Ao reativar um agendamento único após o horário originalmente agendado ter passado, o agendamento poderá invocar imediatamente seu destino. Isso pode ocorrer mesmo que o agendamento tenha sido desativado antes do horário de execução original.

Por exemplo:

- Hora atual: 13:15 UTC
- One-time horário criado para: 13:30 UTC
- O agendamento será desabilitado antes das 13:30 UTC
- O agendamento será reativado às 14:00 UTC.

- Resultado: o destino pode ser invocado imediatamente após a reativação.

Histórico de documentos do Guia do usuário do EventBridge Scheduler

A tabela a seguir descreve as versões da documentação do EventBridge Scheduler.

Alteração	Descrição	Data
Política AmazonEventBridgeSchedulerReadOnlyAccess gerenciada atualizada	Atualizou a política `AmazonEventBridgeSchedulerReadOnlyAccess` gerenciada para usar ações curinga (`scheduler:List* escheduler:Get*`). • the section called “AWS atualizações de políticas gerenciadas”	25 de março de 2026
Mudanças na função de execução e prevenção do problema de segurança delegada confusa	Esta atualização descreve as alterações na forma como a função de execução é aplicada a um recurso de grupo de agendamento quando você implementa a prevenção do problema de segurança delegada confusa na política de permissão da função. • the section called “Prevenção contra representante confuso”	7 de setembro de 2023
Exclusão automática de agendamentos após a conclusão	EventBridge O Scheduler suporta a exclusão automática. Quando você configura	2 de agosto de 2023

	a exclusão automática, o EventBridge Scheduler exclui sua agenda após a última invocação planejada. • the section called “Exclusão após a conclusão do agendamento”	
Tópico atualizado sobre o uso de destinos universais	Atualizou a lista de serviços compatíveis que o EventBridge Scheduler pode segmentar e integrar. Essa atualização também inclui uma lista de operações de API de `GET` não aceitas e inclui melhorias nos exemplos de metas universais, bem como outras pequenas melhorias em todo o guia. • the section called “Usando destinos universais”	17 de março de 2023
Informações atualizadas sobre agendamentos baseados em taxas que não têm uma data de início	Foram adicionadas informações sobre como o EventBridge Scheduler lida com agendamentos baseados em taxas se você não especificar um. `StartDate` • the section called “Rate-based horários”	17 de março de 2023

Novo tópico sobre gerenciamento de grupos de agendadores	Foi adicionado um novo capítulo sobre como criar grupos de agendadores com o EventBridge Agendador . Use este capítulo para aprender como criar um grupo, adicionar agendas ao grupo, aplicar tags para gerenciar e monitorar mais facilmente os recursos do EventBridge Scheduler e, finalmente, excluir um grupo. • Gerenciando um grupo de agendamento	17 de março de 2023
Novos tópicos sobre horário de verão e fusos horários	Foram adicionadas novas seções que descrevem como o EventBridge Scheduler lida com o horário de verão e como você pode criar horários em diferentes fusos horários. • the section called “Horário de verão” • the section called “Fusos horários”	17 de novembro de 2022

Novo tópico sobre métricas	Foi adicionado um novo tópico que descreve as métricas nas quais o EventBridge Scheduler publica. CloudWatch Você pode usar essas métricas para monitorar falhas de invocação e entender como resolver problemas com seus agendamentos. • the section called “Monitoramento com CloudWatch”	15 de novembro de 2022
Lançamento inicial	Versão inicial do Guia do usuário do EventBridge Scheduler.	10 de novembro de 2022

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.