aws

Benutzerhandbuch

# EventBridge Scheduler

# EventBridge Scheduler: Benutzerhandbuch

# Table of Contents

# Was ist Amazon EventBridge Scheduler?

Amazon EventBridge Scheduler ist ein serverloser Scheduler, mit dem Sie Aufgaben von einem zentralen, verwalteten Service aus erstellen, ausführen und verwalten können. EventBridge Scheduler ist hochgradig skalierbar und ermöglicht es Ihnen, Millionen von Aufgaben zu planen, die mehr als 270AWS Dienste und über 6.000 API-Operationen aufrufen können. Ohne die Infrastruktur bereitstellen und verwalten oder mehrere Dienste integrieren zu müssen, bietet Ihnen EventBridge Scheduler die Möglichkeit, Zeitpläne in großem Maßstab zu erstellen und die Wartungskosten zu senken.

EventBridge Der Scheduler erledigt Ihre Aufgaben zuverlässig und verfügt über integrierte Mechanismen, die Ihre Zeitpläne an die Verfügbarkeit nachgeordneter Ziele anpassen. Mit EventBridge Scheduler können Sie Zeitpläne mithilfe von Cron- und Rate-Ausdrücken für wiederkehrende Muster erstellen oder einmalige Aufrufe konfigurieren. Sie können flexible Zeitfenster für die Zustellung einrichten, Wiederholungslimits definieren und die maximale Aufbewahrungszeit für fehlgeschlagene Trigger festlegen.

Themen



## Hauptfunktionen von EventBridge Scheduler

EventBridge Der Scheduler bietet die folgenden Hauptfunktionen, mit denen Sie Ziele konfigurieren und Ihre Zeitpläne skalieren können.

- Vorgeschlagene Ziele — EventBridge Der Scheduler unterstützt Ziele mit Vorlagen, um allgemeine API-Operationen mit Amazon SQS, Amazon SNS, Lambda und auszuführen EventBridge. Mit vordefinierten Zielen können Sie Ihre Zeitpläne schnell mit der EventBridge Scheduler-Konsole, dem EventBridge Scheduler SDK oder dem konfigurierenAWS CLI.
- Universelle Ziele — Der EventBridge Scheduler bietet einen universellen Zielparameter (UTP), mit dem Sie benutzerdefinierte Trigger erstellen können, die nach einem Zeitplan auf mehr als 270AWS Dienste und über 6.000 API-Operationen abzielen. Mit UTP können Sie Ihre benutzerdefinierten Trigger mithilfe der EventBridge Scheduler-Konsole, des EventBridge Scheduler SDK oder des konfigurierenAWS CLI.

- Flexible Zeitfenster — Der EventBridge Scheduler unterstützt flexible Zeitfenster, sodass Sie Ihre Zeitpläne verteilen und die Zuverlässigkeit Ihrer Trigger für Anwendungsfälle verbessern können, die keinen genauen geplanten Aufruf von Zielen erfordern.
- Wiederholungsversuche — EventBridge Der Scheduler ermöglicht die Übertragung von at-least-once Ereignissen an die Ziele, d. h., dass mindestens eine Zustellung erfolgreich ist und das Ziel eine Antwort erhält. EventBridge Mit dem Scheduler können Sie die Anzahl der Wiederholungsversuche für Ihren Zeitplan für eine fehlgeschlagene Aufgabe festlegen. EventBridge Der Scheduler versucht fehlgeschlagene Aufgaben mit verzögerten Versuchen erneut, um die Zuverlässigkeit Ihres Zeitplans zu verbessern und sicherzustellen, dass Ziele verfügbar sind.

# Zugreifen auf den EventBridge Scheduler

Sie können EventBridge Scheduler über die EventBridge Scheduler-Konsole, das EventBridge Scheduler SDKAWS CLI, das oder direkt über die EventBridge Scheduler-API verwenden.

# Amazon EventBridge Scheduler einrichten

Bevor Sie EventBridge Scheduler verwenden können, müssen Sie die folgenden Schritte ausführen.

Themen



## Melden Sie sich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

## Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

| Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus. | Bis | Von | Sie können auch |
| --- | --- | --- | --- |
| Im IAM Identity Center<br><br>(Empfohlen) | Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS.<br><br>Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch. | Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch. | Konfigurieren Sie den programmatischen Zugriff, indem Sie den AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch AWS CLI zu verwendenden konfigurieren. |
| In IAM<br><br>(Nicht empfohlen) | Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS. | Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch. | Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren. |

# Verwenden Sie verwaltete Richtlinien

Im vorherigen Schritt haben Sie einen IAM-Benutzer mit den Anmeldeinformationen für den Zugriff auf Ihre AWS Ressourcen eingerichtet. Um EventBridge Scheduler sicher verwenden zu können, empfehlen wir in den meisten Fällen, separate Benutzer, Gruppen oder Rollen zu erstellen, die nur über die für die Verwendung EventBridge von Scheduler erforderlichen Berechtigungen verfügen. EventBridge Scheduler unterstützt die folgenden verwalteten Richtlinien für allgemeine Anwendungsfälle.

- the section called “`AmazonEventBridgeSchedulerFullAccess`”— Gewährt vollen Zugriff auf EventBridge Scheduler über die Konsole und die API.
- the section called “`AmazonEventBridgeSchedulerReadOnlyAccess`”— Gewährt schreibgeschützten Zugriff auf den Scheduler. EventBridge

Sie können diese verwalteten Richtlinien auf dieselbe Weise an Ihre IAM-Prinzipale anhängen, wie Sie die `AdministratorAccess` Richtlinie im vorherigen Schritt angehängt haben. Weitere Informationen zur Verwaltung des Zugriffs auf EventBridge Scheduler mithilfe identitätsbasierter IAM-Richtlinien finden Sie unter. the section called “Verwenden identitätsbasierter Richtlinien”

# Einrichten der Ausführungsrolle

Eine Ausführungsrolle ist eine IAM-Rolle, die EventBridge Scheduler übernimmt, um in Ihrem Namen mit anderen zu interagieren. AWS-Services Sie fügen dieser Rolle Berechtigungsrichtlinien hinzu, um EventBridge Scheduler Zugriff zum Aufrufen von Zielen zu gewähren.

Sie können auch eine neue Ausführungsrolle erstellen, wenn Sie die Konsole verwenden, um einen neuen Zeitplan zu erstellen. Wenn Sie die Konsole verwenden, erstellt EventBridge Scheduler in Ihrem Namen eine Rolle mit Berechtigungen, die auf dem von Ihnen ausgewählten Ziel basieren. Wenn EventBridge Scheduler eine Rolle für Sie erstellt, enthält die Vertrauensrichtlinie der Rolle Bedingungsschlüssel, die einschränken, welche Prinzipale die Rolle in Ihrem Namen übernehmen können. Dies schützt vor dem potenziellen Sicherheitsproblem mit dem verwirrten Stellvertreter.

In den folgenden Schritten wird beschrieben, wie Sie eine neue Ausführungsrolle erstellen und dem EventBridge Scheduler Zugriff gewähren, um ein Ziel aufzurufen. In diesem Thema werden Berechtigungen für beliebte Ziele mit Vorlagen beschrieben. Informationen zum Hinzufügen von Berechtigungen für andere Ziele finden Sie unterthe section called “Verwenden von Vorlagenzielen”.

Um eine Ausführungsrolle mit dem zu erstellen AWS CLI

1. Kopieren Sie die folgende JSON-Richtlinie „Rolle übernehmen“ und speichern Sie sie lokal unter`Scheduler-Execution-Role.json`. Diese Vertrauensrichtlinie ermöglicht es EventBridge Scheduler, die Rolle in Ihrem Namen zu übernehmen.

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

> **Important**
>
> Um eine Ausführungsrolle in einer Produktionsumgebung einzurichten, empfehlen wir die Implementierung zusätzlicher Sicherheitsvorkehrungen, um Probleme mit unübersichtlichen Stellvertretern zu vermeiden. Weitere Informationen und ein Beispiel für eine Richtlinie finden Sie unterthe section called “Confused-Deputy-Prävention”.

2. Geben Sie AWS Command Line Interface unter (AWS CLI) den folgenden Befehl ein, um eine neue Rolle zu erstellen. *`SchedulerExecutionRole`*Ersetzen Sie es durch den Namen, den Sie dieser Rolle geben möchten.

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

Bei Erfolg wird die folgende Ausgabe angezeigt:

```
{
    "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. Um eine neue Richtlinie zu erstellen, die es EventBridge Scheduler ermöglicht, ein Ziel aufzurufen, wählen Sie eines der folgenden allgemeinen Ziele aus. Kopieren Sie die JSON-Berechtigungsrichtlinie und speichern Sie sie lokal als `.json` Datei.

   Amazon SQS – SendMessage

   Im Folgenden kann EventBridge Scheduler die `sqs:SendMessage` Aktion für alle Amazon SQS SQS-Warteschlangen in Ihrem Konto aufrufen.

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

Amazon SNS – Publish

Im Folgenden kann EventBridge Scheduler die `sns:Publish` Aktion für alle Amazon SNS SNS-Themen in Ihrem Konto aufrufen.

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

Lambda – Invoke

Im Folgenden kann EventBridge Scheduler die `lambda:InvokeFunction` Aktion für alle Lambda-Funktionen in Ihrem Konto aufrufen.

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

4. Führen Sie den folgenden Befehl aus, um die neue Berechtigungsrichtlinie zu erstellen. *`PolicyName`*Ersetzen Sie sie durch den Namen, den Sie dieser Richtlinie geben möchten.

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

Bei Erfolg wird die folgende Ausgabe angezeigt. Beachten Sie den Richtlinien-ARN. Sie verwenden diesen ARN im nächsten Schritt, um die Richtlinie an unsere Ausführungsrolle anzuhängen.

```
{
    "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. Führen Sie den folgenden Befehl aus, um die Richtlinie an Ihre Ausführungsrolle anzuhängen. *your-policy-arn*Ersetzen Sie es durch den ARN der Richtlinie, die Sie im vorherigen Schritt erstellt haben. *SchedulerExecutionRole*Ersetzen Sie ihn durch den Namen Ihrer Ausführungsrolle.

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

Der `attach-role-policy` Vorgang gibt keine Antwort in der Befehlszeile zurück.

## Richten Sie ein Ziel ein

Bevor Sie einen EventBridge Scheduler-Zeitplan erstellen, benötigen Sie mindestens ein Ziel, das Ihr Zeitplan aufrufen kann. Sie können eine vorhandene AWS Ressource verwenden oder eine neue erstellen. Die folgenden Schritte zeigen, wie Sie eine neue Amazon SQS SQS-Standardwarteschlange mit AWS CloudFormation erstellen.

So erstellen Sie eine neue Amazon SQS SQS-Warteschlange

1. Kopieren Sie die folgende AWS CloudFormation JSON-Vorlage und speichern Sie sie lokal unter. `SchedulerTargetSQS.json`

```
{
   "AWSTemplateFormatVersion": "2010-09-09",
   "Resources": {
      "MyQueue": {
         "Type": "AWS::SQS::Queue",
         "Properties": {
            "QueueName": "MyQueue"
             }
         }
      },
   "Outputs": {
      "QueueName": {
         "Description": "The name of the queue",
         "Value": {
            "Fn::GetAtt": [
               "MyQueue",
               "QueueName"
            ]
         }
      },
      "QueueURL": {
         "Description": "The URL of the queue",
         "Value": {
            "Ref": "MyQueue"
         }
      },
      "QueueARN": {
         "Description": "The ARN of the queue",
         "Value": {
            "Fn::GetAtt": [
               "MyQueue",
               "Arn"
            ]
         }
      }
   }
}
```

2. Führen Sie in der den folgenden Befehl aus AWS CLI, um einen AWS CloudFormation Stack aus der `Scheduler-Target-SQS.json` Vorlage zu erstellen.

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

Bei Erfolg wird die folgende Ausgabe angezeigt:

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

3. Führen Sie den folgenden Befehl aus, um die Übersichtsinformationen für Ihren AWS CloudFormation Stack anzuzeigen. Zu diesen Informationen gehören der Status des Stacks und die in der Vorlage angegebenen Ausgaben.

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

Bei Erfolg erstellt der Befehl die Amazon SQS SQS-Warteschlange und gibt die folgende Ausgabe zurück:

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

Später in diesem Handbuch werden Sie den Wert für verwenden, `QueueARN` um die Warteschlange als Ziel für EventBridge Scheduler einzurichten.

## Als nächstes

Nachdem Sie den Einrichtungsschritt abgeschlossen haben, verwenden Sie den Leitfaden Erste Schritte, um Ihren ersten EventBridge Scheduler-Scheduler zu erstellen und ein Ziel aufzurufen.

# Erste Schritte mit EventBridge Scheduler

In diesem Thema wird die Erstellung eines neuen Scheduler-Zeitplans beschrieben. EventBridge Sie verwenden die EventBridge Scheduler-Konsole AWS Command Line Interface (AWS CLI) oder AWS SDKs, um einen Zeitplan mit einem Amazon SQS-Ziel als Vorlage zu erstellen. Anschließend richten Sie die Protokollierung ein, konfigurieren Wiederholungsversuche und legen eine maximale Aufbewahrungszeit für fehlgeschlagene Aufgaben fest. Nachdem Sie den Zeitplan erstellt haben, überprüfen Sie, ob Ihr Zeitplan das Ziel erfolgreich aufruft und eine Nachricht an die Zielwarteschlange sendet.

> **Note**
>
> Um diesem Leitfaden zu folgen, empfehlen wir Ihnen, IAM-Benutzer mit den unter beschriebenen Mindestberechtigungen einzurichten. the section called “Verwenden identitätsbasierter Richtlinien” Nachdem Sie einen Benutzer erstellt und konfiguriert haben, führen Sie den folgenden Befehl aus, um Ihre Zugangsdaten festzulegen. Sie benötigen Ihre Zugriffsschlüssel-ID und Ihren geheimen Zugriffsschlüssel, um den zu konfigurierenAWS 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
> ```
>
> Weitere Informationen zu den verschiedenen Möglichkeiten, wie Sie Ihre Anmeldeinformationen festlegen können, finden Sie unter Konfigurationseinstellungen und Rangfolge im AWS Command Line InterfaceBenutzerhandbuch für Version 2.

Themen

# Voraussetzungen

Bevor Sie die Schritte in diesem Abschnitt ausführen, müssen Sie Folgendes tun:

- Führen Sie die unter beschriebenen Aufgaben aus Einrichtung

# Erstellen Sie mit der EventBridge Scheduler-Konsole einen Zeitplan

Um einen neuen Zeitplan mit der Konsole zu erstellen

1. Melden Sie sich bei der an AWS Management Console und wählen Sie dann den folgenden Link, um den EventBridge Scheduler-Bereich der EventBridge Konsole zu öffnen: https://us-west-2.console.aws.amazon.com/scheduler/home?region=us-west-2#home

   > **Note**
   >
   > Sie können Ihre ändern, AWS-Region indem Sie die Regionsauswahl AWS Management Console von verwenden.

2. Wählen Sie auf der Seite Zeitpläne die Option Zeitplan erstellen aus.
3. Gehen Sie auf der Seite Zeitplandetails angeben im Abschnitt Zeitplanname und -beschreibung wie folgt vor:

   a. Geben Sie unter Zeitplanname einen Namen für Ihren Zeitplan ein. Beispiel: **`MyTestSchedule`**

   b. Geben Sie unter Beschreibung — optional eine Beschreibung für Ihren Zeitplan ein. Zum Beispiel **`My first schedule`**.

   c. Wählen Sie unter Zeitplangruppe eine Zeitplangruppe aus den Drop-down-Optionen aus. Wenn Sie noch keine Zeitplangruppen erstellt haben, können Sie die `default` Gruppe für Ihren Zeitplan auswählen. Um eine neue Zeitplangruppe zu erstellen, klicken Sie in der Konsolenbeschreibung auf den Link Eigenen Zeitplan erstellen. Sie verwenden Zeitplangruppen, um Tags zu Zeitplangruppen hinzuzufügen.

4. Gehen Sie im Abschnitt Zeitplanmuster wie folgt vor:

   a. Wählen Sie für Vorkommen eine der folgenden Musteroptionen aus. Die Konfigurationsoptionen ändern sich je nachdem, welches Muster Sie auswählen.

- Einmaliger Zeitplan — Ein einmaliger Zeitplan ruft ein Ziel nur einmal an dem von Ihnen angegebenen Datum und zu der von Ihnen angegebenen Uhrzeit auf.

  Geben Sie für Datum und Uhrzeit ein gültiges Datum im `YYYY/MM/DD` Format ein. Geben Sie dann einen Zeitstempel im `hh:mm` 24-Stunden-Format an. Wählen Sie abschließend eine Zeitzone aus den Drop-down-Optionen aus.
- Wiederkehrender Zeitplan — Ein wiederkehrender Zeitplan ruft ein Ziel mit einer Geschwindigkeit auf, die Sie mithilfe eines cron Ausdrucks oder eines Kursausdrucks angeben.

  Wählen Sie Cron-basierter Zeitplan, um einen Zeitplan mithilfe eines cron Ausdrucks zu konfigurieren. Um einen Ratenausdruck zu verwenden, wählen Sie Ratenbasierter Zeitplan und geben Sie eine positive Zahl für Wert ein. Wählen Sie dann eine Einheit aus den Dropdownoptionen aus.

  Weitere Informationen zur Verwendung von Cron- und Ratenausdrücken finden Sie unter. Arten von Zeitplänen

b. Wählen Sie für „Flexibles Zeitfenster“ die Option „Aus“, um die Option zu deaktivieren, oder wählen Sie eines der vordefinierten Zeitfenster aus der Dropdownliste. Wenn Sie beispielsweise 15 Minuten auswählen und einen wiederkehrenden Zeitplan festlegen, der sein Ziel einmal pro Stunde aufruft, wird der Zeitplan innerhalb von 15 Minuten nach Beginn jeder Stunde ausgeführt.

5. 
> **Note**
>
> Die Funktion „Flexibles Zeitfenster“ ist bei einmaligen Zeitplänen nicht verfügbar.

Wenn Sie im vorherigen Schritt Wiederkehrender Zeitplan ausgewählt haben, geben Sie im Abschnitt Zeitrahmen eine Zeitzone an und legen Sie optional ein Startdatum und eine Startzeit sowie ein Enddatum und eine Endzeit für den Zeitplan fest. Ein wiederkehrender Zeitplan ohne Startdatum beginnt, sobald er erstellt und verfügbar ist. Bei wiederkehrenden Zeitplänen ohne Enddatum wird das Ziel weiterhin auf unbestimmte Zeit aktiviert.

6. Wählen Sie Weiter aus.
7. Gehen Sie auf der Seite „Ziel auswählen“ wie folgt vor:

a. Wählen Sie Ziele mit Vorlagen und wählen Sie eine Ziel-API aus. Für dieses Beispiel wählen wir das Amazon SQS SQS-Vorlagenziel **`SendMessage`** aus.

b. Wählen Sie im SendMessageAbschnitt für SQS-Warteschlange einen vorhandenen Amazon SQS SQS-Warteschlangen-ARN aus, z. B. `arn:aws:sqs:us-west-2:123456789012:TestQueue` aus der Drop-down-Liste. Um eine neue Warteschlange zu erstellen, wählen Sie Neue SQS-Warteschlange erstellen, um zur Amazon SQS SQS-Konsole zu navigieren. Nachdem Sie die Erstellung einer Warteschlange abgeschlossen haben, kehren Sie zur EventBridge Scheduler-Konsole zurück und aktualisieren Sie das Drop-down-Menü. Ihr neuer Warteschlangen-ARN wird angezeigt und kann ausgewählt werden.

c. Geben Sie für Target die Payload ein, die EventBridge Scheduler an das Ziel liefern soll. In diesem Beispiel senden wir die folgende Nachricht an die Zielwarteschlange: **`Hello, it's EventBridge Scheduler.`**

8. Wählen Sie Weiter und gehen Sie dann auf der Seite Einstellungen — optional wie folgt vor:

9.

a. Schalten Sie im Abschnitt Zeitplanstatus unter Zeitplan aktivieren die Funktion mithilfe des Schalters ein oder aus. Standardmäßig aktiviert der EventBridge Scheduler Ihren Zeitplan.

b. Konfigurieren Sie im Abschnitt Aktion nach Abschluss des Zeitplans die Aktion, die der EventBridge Scheduler nach Abschluss des Zeitplans ausführt:

- Wählen Sie LÖSCHEN, wenn der Zeitplan automatisch gelöscht werden soll. Bei einmaligen Zeitplänen erfolgt dies, nachdem der Zeitplan das Ziel einmal aufgerufen hat. Bei wiederkehrenden Zeitplänen erfolgt dies nach dem letzten geplanten Aufruf des Zeitplans. Weitere Hinweise zum automatischen Löschen finden Sie unterthe section called “Löschen nach Abschluss des Zeitplans”.
- Wählen Sie KEINE oder wählen Sie keinen Wert, wenn Sie nicht möchten, dass der EventBridge Scheduler nach Abschluss des Zeitplans weitere Aktionen ausführt.

c. Aktivieren Sie im Abschnitt Wiederholungsrichtlinie und Warteschlange für unzulässige Briefe (DLQ) für Wiederholungsrichtlinie die Option Wiederholen, um eine Wiederholungsrichtlinie für Ihren Zeitplan zu konfigurieren. Bei Wiederholungsrichtlinien führt Scheduler den Zeitplan erneut aus, wenn ein Zeitplan sein Ziel nicht aufrufen kann. EventBridge Falls konfiguriert, müssen Sie die maximale Aufbewahrungszeit und Wiederholungsversuche für den Zeitplan festlegen.

d. Geben Sie unter Maximales Alter des Ereignisses — optional die maximale (n) Stunde (n) und Minute (n) ein, für die der EventBridge Scheduler ein unbearbeitetes Ereignis speichern muss.

> **Note**
>
> Der Höchstwert ist 24 Stunden.

e. Geben Sie unter Maximale Anzahl an Wiederholungen ein, wie oft der EventBridge Scheduler den Zeitplan maximal wiederholt, wenn das Ziel einen Fehler zurückgibt.

> **Note**
>
> Der Maximalwert beträgt 185 Wiederholungen.

f. Wählen Sie für Dead-Letter Queue (DLQ) eine der folgenden Optionen aus:

- Keine — Wählen Sie diese Option, wenn Sie keinen DLQ konfigurieren möchten.
- Wählen Sie eine Amazon SQS SQS-Warteschlange in meinem AWS Konto als DLQ aus — Wählen Sie diese Option, wählen Sie dann einen Warteschlangen-ARN aus der Drop-down-Liste und konfigurieren Sie einen DLQ genauso AWS-Konto wie den, in dem Sie den Zeitplan erstellen.
- Geben Sie eine Amazon SQS SQS-Warteschlange in einem anderen AWS Konto als DLQ an — Wählen Sie diese Option und geben Sie dann den ARN der als DLQ konfigurierten Warteschlange ein, falls sich die Warteschlange in einer anderen befindet. AWS-Konto Sie müssen den genauen ARN für die Warteschlange eingeben, um diese Option verwenden zu können.

g. Wählen Sie im Abschnitt Verschlüsselung die Option Verschlüsselungseinstellungen anpassen (erweitert), um Ihre Zieleingabe mit einem vom Kunden verwalteten KMS-Schlüssel zu verschlüsseln. Wenn Sie diese Option wählen, geben Sie einen vorhandenen KMS-Schlüssel-ARN ein oder wählen Sie AWS KMS-Schlüssel erstellen, um zur AWS KMS Konsole zu navigieren. Weitere Informationen darüber, wie EventBridge Scheduler Ihre Daten im Ruhezustand verschlüsselt, finden Sie unter. the section called “Verschlüsselung im Ruhezustand”

h. Wählen Sie für Berechtigungen die Option Bestehende Rolle verwenden aus und wählen Sie dann die Rolle, die Sie während des Einrichtungsvorgangs erstellt haben, aus der

Dropdownliste aus. Sie können auch „Gehe zur IAM-Konsole“ wählen, um eine neue Rolle zu erstellen.

Wenn Sie möchten, dass EventBridge Scheduler eine neue Ausführungsrolle für Sie erstellt, wählen Sie stattdessen Neue Rolle für diesen Zeitplan erstellen. Geben Sie dann einen Namen für Rollenname ein. Wenn Sie diese Option wählen, fügt EventBridge Scheduler der Rolle die erforderlichen Berechtigungen hinzu, die für Ihr vorgegebenes Ziel erforderlich sind.

10. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Zeitplan überprüfen und erstellen die Details Ihres Zeitplans. Wählen Sie in jedem Abschnitt Bearbeiten aus, um zu diesem Schritt zurückzukehren und seine Details zu bearbeiten.
12. Wählen Sie Zeitplan erstellen aus, um die Erstellung Ihres neuen Zeitplans abzuschließen. Auf der Seite Zeitpläne können Sie eine Liste Ihrer neuen und vorhandenen Zeitpläne anzeigen. Überprüfen Sie in der Spalte Status, ob Ihr neuer Zeitplan aktiviert ist.
13. Um zu überprüfen, ob Ihr Zeitplan das Amazon SQS SQS-Ziel aufruft, öffnen Sie die Amazon SQS SQS-Konsole und gehen Sie wie folgt vor:

    a. Wählen Sie die Zielwarteschlange aus der Warteschlangenliste aus.

    b. Wählen Sie Nachrichten senden und empfangen.

    c. Wählen Sie auf der Seite Nachrichten senden und empfangen unter Nachrichten empfangen die Option Nachrichten abfragen aus, um die Testnachrichten abzurufen, die Ihr Zeitplan an die Zielwarteschlange gesendet hat.

# Erstellen Sie einen Zeitplan mit dem AWS CLI

Das folgende Beispiel zeigt, wie Sie den AWS CLI Befehl verwenden `create-schedule`, um einen EventBridge Scheduler-Zeitplan mit einem Amazon SQS-Ziel als Vorlage zu erstellen. Ersetzen Sie die Platzhalterwerte für die folgenden Parameter durch Ihre Informationen:

- --name — Geben Sie einen Namen für den Zeitplan ein.
- RoleArn— Geben Sie den ARN für die Ausführungsrolle ein, die Sie dem Zeitplan zuordnen möchten.
- Arn — Geben Sie den ARN für das Ziel ein. In diesem Fall ist das Ziel eine Amazon SQS SQS-Warteschlange.

- Eingabe — Geben Sie eine Nachricht ein, die der EventBridge Scheduler an die Zielwarteschlange übermittelt.

```
$ 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"}'
```

# Erstellen Sie mit den Scheduler-SDKs einen EventBridge Zeitplan

Im folgenden Beispiel verwenden Sie die EventBridge Scheduler-SDKs, um einen EventBridge Scheduler-Zeitplan mit einem Amazon SQS-Ziel als Vorlage zu erstellen.

Example Python-SDK

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

flex_window = { "Mode": "OFF" }

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

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

Example Java-SDK

```
package com.example;

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

```
public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

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

# Als nächstes

- Weitere Informationen zur Verwaltung Ihres Zeitplans mithilfe der Konsole oder des EventBridge Scheduler-SDK finden Sie unterVerwaltung eines Zeitplans. AWS CLI
- Weitere Informationen zur Konfiguration von Zielvorlagen und zur Verwendung des Parameters Universal Target finden Sie unter. Ziele verwalten
- Weitere Informationen zu den EventBridge Scheduler-Datentypen und API-Vorgängen finden Sie in der EventBridge Scheduler-API-Referenz.

# Zeitplantypen im EventBridge Scheduler

Im folgenden Thema werden die verschiedenen Zeitplantypen beschrieben, die Amazon EventBridge Scheduler unterstützt, sowie die Art und Weise, wie EventBridge Scheduler mit der Sommerzeit umgeht und die Planung in verschiedenen Zeitzonen durchführt. Bei der Konfiguration Ihres Zeitplans können Sie zwischen drei Zeitplantypen wählen: tarifbasierte, cron-basierte und einmalige Zeitpläne.

Sowohl ratenbasierte als auch cron-basierte Zeitpläne sind wiederkehrende Zeitpläne. Sie konfigurieren jeden Typ eines wiederkehrenden Zeitplans mithilfe eines Zeitplanausdrucks für den Typ des Zeitplans, den Sie konfigurieren möchten, und geben eine Zeitzone an, in der EventBridge Scheduler den Ausdruck auswertet.

Ein einmaliger Zeitplan ist ein Zeitplan, der ein Ziel nur einmal aufruft. Sie konfigurieren einen einmaligen Zeitplan, wenn Sie die Uhrzeit, das Datum und die Zeitzone angeben, in der der EventBridge Scheduler den Zeitplan auswertet.

> **Note**
>
> Alle Zeitplantypen im EventBridge Scheduler rufen ihre Ziele mit einer Genauigkeit von 60 Sekunden auf. Das heißt, wenn Sie Ihren Zeitplan so einrichten, dass er am läuft`1:00`, wird die Ziel-API zwischen und aufgerufen. `1:00:00` `1:00:59`

In den folgenden Abschnitten erfahren Sie, wie Sie Zeitplanausdrücke für jeden wiederkehrenden Zeitplantyp konfigurieren und wie Sie einen einmaligen Zeitplan im EventBridge Scheduler einrichten.

Themen

# Ratenbasierte Zeitpläne

Ein ratenbasierter Zeitplan beginnt nach dem Startdatum, das Sie für Ihren Zeitplan angegeben haben, und läuft mit einem von Ihnen definierten regulären Tarif bis zum Enddatum des Zeitplans. Mithilfe eines ratenbasierten Zeitplans können Sie die gängigsten Anwendungsfälle für die wiederkehrende Terminplanung einrichten. Wenn Sie beispielsweise einen Zeitplan verwenden möchten, bei dem das Ziel alle 15 Minuten, alle zwei Stunden oder alle fünf Tage aufgerufen wird, können Sie einen ratenbasierten Zeitplan verwenden, um dies zu erreichen. Sie konfigurieren einen ratenbasierten Zeitplan mithilfe eines Preisausdrucks.

Bei tarifbasierten Zeitplänen verwenden Sie die `StartDate`Eigenschaft, um das erste Vorkommen des Zeitplans festzulegen. Wenn Sie `StartDate` für einen ratenbasierten Zeitplan keinen Plan angeben, ruft Ihr Zeitplan das Ziel sofort auf.

Preisausdrücke enthalten zwei Pflichtfelder, die durch ein Leerzeichen getrennt sind, wie im Folgenden dargestellt.

## Syntax

```
rate(value unit)
```

Wert

Eine positive Zahl.

Einheit

Die Zeiteinheit, in der Ihr Zeitplan das Ziel aufrufen soll.

Gültige Eingaben: `minutes` | | `hours` `days`

## Beispiele

Das folgende Beispiel zeigt, wie Preisausdrücke mit dem AWS CLI `create-schedule` Befehl verwendet werden, um einen ratenbasierten Zeitplan zu konfigurieren. In diesem Beispiel wird ein Zeitplan erstellt, der alle fünf Minuten ausgeführt wird und eine Nachricht unter Verwendung des vordefinierten `SqsParameters` Zieltyps an eine Amazon SQS-Warteschlange übermittelt.

Da in diesem Beispiel kein Wert für den `--start-date` Parameter festgelegt ist, ruft der Zeitplan sein Ziel sofort auf, nachdem Sie ihn erstellt und aktiviert haben.

```
$ 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-basierte Zeitpläne

Ein Cron-Ausdruck erstellt einen detaillierten wiederkehrenden Zeitplan, der zu einem bestimmten Zeitpunkt Ihrer Wahl ausgeführt wird. EventBridge Scheduler unterstützt die Konfiguration von cron-basierten Zeitplänen in UTC (Universal Coordinated Time) oder in der Zeitzone, die Sie bei der Erstellung Ihres Zeitplans angeben. Mit cron-basierten Zeitplänen haben Sie mehr Kontrolle darüber, wann und wie oft Ihr Zeitplan ausgeführt wird. Verwenden Sie cron-basierte Zeitpläne, wenn Sie einen benutzerdefinierten Wiederholungsplan benötigen, der von keinem der Tarifausdrücke von Scheduler unterstützt wird. EventBridge Sie können beispielsweise einen cron-basierten Zeitplan erstellen, der um 8:00 Uhr ausgeführt wird. PST am ersten Montag jedes Monats Sie konfigurieren einen cron-basierten Zeitplan mithilfe eines Cron-Ausdrucks.

Ein Cron-Ausdruck besteht aus fünf Pflichtfeldern, die durch Leerzeichen getrennt sind: Minuten, Stunden day-of-month, day-of-week Monat und einem optionalen Feld, Jahr, wie im Folgenden dargestellt.

## Syntax

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

| Feld | Werte | Platzhalter |
|---|---|---|
| Minuten | 0-59 | , - * / |
| Stunden | 0-23 | , - * / |
| D ay-of-month | 1-31 | , - * ? / L W |
| Monat | 1-12 oder JAN-DEC | , - * / |
| D ay-of-week | 1-7 oder SUN-SAT | , - * ? / L # |
| Jahr | 1970-2199 | , - * / |

Platzhalter

- Das Platzhalterzeichen , (Komma) schließt zusätzliche Werte ein. Im Feld Monat steht JAN, FEB, MAR für Januar, Februar und März.
- Das Platzhalterzeichen - (Bindestrich) gibt einen Bereich an. Im Feld Tag steht 1-15 für die Tage 1 bis 15 des angegebenen Monats.
- Das Platzhalterzeichen * (Sternchen) steht für alle Werte im Feld. Im Feld für die Stundenangaben steht * für alle Stunden. Sie können * nicht sowohl in den ay-of-week Feldern D als ay-of-month auch in D verwenden. Wenn Sie es in einem der Felder eingeben, müssen Sie im anderen Feld ein ? verwenden.
- Das Platzhalterzeichen / (Schrägstrich) steht für schrittweise Steigerungen. Im Feld "Minuten" können Sie 1/10 eingeben, um einen Bereich von je 10 Minuten beginnend mit der ersten Minute der Stunde anzugeben (z. B. die 11., 21. und 31. Minute usw.).
- Das Platzhalterzeichen ? (Fragezeichen) steht für einen beliebigen Wert. In das ay-of-month D-Feld könnten Sie 7 eingeben und wenn ein beliebiger Wochentag zulässig ist, könnten Sie eingeben? im ay-of-week D-Feld.
- Der Platzhalter L in den ay-of-week Feldern D ay-of-month oder D gibt den letzten Tag des Monats oder der Woche an.
- Der **`W`** Platzhalter im ay-of-month D-Feld gibt einen Wochentag an. **`3W`**Gibt im ay-of-month Feld D den Wochentag an, der dem dritten Tag des Monats am nächsten liegt.
- Der Platzhalter # im ay-of-week Feld D gibt eine bestimmte Instanz des angegebenen Wochentags innerhalb eines Monats an. Beispiel: 3#2 steht für den zweiten Dienstag des Monats: Die 3 bezieht sich auf Dienstag, da dies der dritte Tag jeder Woche ist, und die 2 bezieht sich auf den zweiten Tag dieses Typs innerhalb des Monats.

> **Note**
>
> Wenn Sie das Zeichen '#' verwenden, können Sie nur einen Ausdruck in dem day-of-week Feld definieren. Beispiel, `"3#1,6#3"` ist ungültig, da es als zwei Ausdrücke interpretiert wird.

## Beispiele

Das folgende Beispiel zeigt, wie Cron-Ausdrücke mit dem AWS CLI `create-schedule` Befehl verwendet werden, um einen Cron-basierten Zeitplan zu konfigurieren. In diesem Beispiel wird ein

Zeitplan erstellt, der in den Jahren 2022 bis 2023 am letzten Freitag eines jeden Monats um 10:15 Uhr UTC+0 läuft und eine Nachricht unter Verwendung des vordefinierten Zieltyps an eine Amazon SQS-Warteschlange übermittelt. `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"}'
```

# Einmalige Zeitpläne

Ein einmaliger Zeitplan ruft ein Ziel nur einmal an dem Datum und der Uhrzeit auf, die Sie unter Verwendung eines gültigen Datums und eines Zeitstempels angeben. EventBridge Scheduler unterstützt die Planung in UTC (Universal Coordinated Time) oder in der Zeitzone, die Sie bei der Erstellung Ihres Zeitplans angeben.

> **Note**
>
> Ein einmaliger Zeitplan wird immer noch auf Ihr Kontingent angerechnet, nachdem er vollständig ausgeführt und sein Ziel aufgerufen hat. Wir empfehlen, deine einmaligen Zeitpläne zu löschen, nachdem sie vollständig ausgeführt wurden.

Sie konfigurieren einen einmaligen Zeitplan mithilfe eines AT-Ausdrucks. Ein at-Ausdruck besteht aus dem Datum und der Uhrzeit, zu der EventBridge Scheduler Ihren Zeitplan aufrufen soll, wie im Folgenden dargestellt.

## Syntax

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

Wenn Sie einen einmaligen Zeitplan konfigurieren, ignoriert EventBridge Scheduler den `StartDate` und, den `EndDate` Sie für den Zeitplan angeben.

## Beispiele

Das folgende Beispiel zeigt, wie AT-Ausdrücke zusammen mit dem AWS CLI `create-schedule` Befehl verwendet werden, um einen einmaligen Zeitplan zu konfigurieren. In diesem Beispiel wird

ein Zeitplan erstellt, der am 20. November 2022 einmal um 13 Uhr UTC-8 ausgeführt wird und eine Nachricht unter Verwendung des vordefinierten Zieltyps an eine Amazon SQS-Warteschlange übermittelt. `SqsParameters`

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

# EventBridge Zeitzonen im Scheduler

EventBridge Scheduler unterstützt die Konfiguration von cron-basierten und einmaligen Zeitplänen in jeder von Ihnen angegebenen Zeitzone. EventBridge Scheduler verwendet die Zeitzonendatenbank, die von der Internet Assigned Numbers Authority (IANA) verwaltet wird.

Mit dem AWS CLI können Sie mithilfe des Parameters die Zeitzone festlegen, in der der EventBridge Scheduler Ihren Zeitplan auswerten soll. `--schedule-expression-timezone` Mit dem folgenden Befehl wird beispielsweise ein cron-basierter Zeitplan erstellt, der täglich um 8:30 Uhr ein vordefiniertes Amazon SQS `SendMessage` SQS-Ziel in America/New_York aufruft.

```
$ 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"}'
```

# EventBridge Sommerzeit im Scheduler

EventBridge Der Scheduler passt Ihren Zeitplan automatisch an die Sommerzeit an. Wenn sich die Zeit im Frühling nach vorne verschiebt und ein Cron-Ausdruck auf ein Datum und eine Uhrzeit fällt, die nicht existieren, wird Ihr Zeitplanaufruf übersprungen. Wenn sich die Zeit im Herbst rückwärts verschiebt, läuft Ihr Zeitplan nur einmal und wiederholt seinen Aufruf nicht. Die folgenden Aufrufe erfolgen normalerweise zum angegebenen Datum und zur angegebenen Uhrzeit.

EventBridge Der Scheduler passt Ihren Zeitplan an die Zeitzone an, die Sie bei der Erstellung des Zeitplans angegeben haben. Wenn Sie einen Zeitplan in America/New_York konfigurieren, passt sich

Ihr Zeitplan an, wenn sich die Uhrzeit in dieser Zeitzone ändert, während ein Zeitplan in America/Los_Angeles drei Stunden später angepasst wird, wenn sich die Zeit an der Westküste ändert.

Bei tarifbasierten Zeitplänen, die als Einheit verwenden, steht z. `days` B. für eine Dauer von 24 Stunden auf der Uhr. `rate(1 days)` `days` Das heißt, wenn ein Tag aufgrund der Sommerzeit auf 23 Stunden verkürzt oder auf 25 Stunden verlängert wird, wertet EventBridge Scheduler den Preisausdruck auch 24 Stunden nach dem letzten Aufruf des Zeitplans aus.

> **Note**
>
> In einigen Zeitzonen wird die Sommerzeit gemäß den lokalen Regeln und Vorschriften nicht eingehalten. Wenn Sie einen Zeitplan in einer Zeitzone erstellen, in der die Sommerzeit nicht eingehalten wird, passt der EventBridge Scheduler Ihren Zeitplan nicht an. Anpassungen der Sommerzeit gelten nicht für Zeitpläne mit koordinierter Weltzeit (UTC).

Beispiel

Stellen Sie sich ein Szenario vor, in dem Sie einen Zeitplan mit dem folgenden Cron-Ausdruck in America/Los_Angeles erstellen:. `cron(30 2 * * ? *)` Dieser Zeitplan läuft jeden Tag um 2:30 Uhr in der angegebenen Zeitzone.

- Spring-forward — Wenn sich die Zeit im Frühling von 1:59 Uhr auf 3:00 Uhr vorwärts verschiebt, überspringt der EventBridge Scheduler den Aufruf des Zeitplans an diesem Tag und setzt die Ausführung des Zeitplans am nächsten Tag normal fort.
- Fallback — Wenn sich die Zeit im Herbst von 2:59 Uhr auf 2:00 Uhr rückwärts verschiebt, führt der EventBridge Scheduler den Zeitplan nur einmal um 2:30 Uhr aus, bevor die Schicht stattfindet, wiederholt den Zeitplanaufruf jedoch nicht erneut um 2:30 Uhr nach der Zeitverschiebung.

# Verwaltung eines Zeitplans

Ein Zeitplan ist die Hauptressource, die Sie mit Amazon EventBridge Scheduler erstellen, konfigurieren und verwalten.

Jeder Zeitplan hat einen Zeitplanausdruck, der bestimmt, wann und mit welcher Häufigkeit der Zeitplan ausgeführt wird. EventBridge Der Scheduler unterstützt drei Arten von Zeitplänen: Tarif-, Cron-Zeitpläne und Einmalpläne. Weitere Informationen zu den verschiedenen Zeitplantypen finden Sie unter. Arten von Zeitplänen

Wenn Sie einen Zeitplan erstellen, konfigurieren Sie ein Ziel für den Aufruf des Zeitplans. Ein Ziel ist ein API-Vorgang, den EventBridge Scheduler bei jeder Ausführung Ihres Zeitplans in Ihrem Namen aufruft. EventBridge Scheduler unterstützt zwei Arten von Zielen: Ziele mit Vorlagen rufen allgemeine API-Operationen für eine Kerngruppe von Diensten auf, und den Universal Target Parameter (UTP), mit dem Sie mehr als 6.000 Operationen in über 270 Diensten aufrufen können. Weitere Informationen zur Konfiguration von Zielen finden Sie unter. Ziele verwalten

Sie konfigurieren, wie Ihr Zeitplan mit Fehlern umgeht, wenn der EventBridge Scheduler ein Ereignis nicht erfolgreich an ein Ziel übermitteln kann, indem Sie zwei Hauptmechanismen verwenden: eine Wiederholungsrichtlinie und eine Dead-Letter-Queue (DLQ). Eine Wiederholungsrichtlinie legt fest, wie oft der EventBridge Scheduler ein fehlgeschlagenes Ereignis wiederholen muss und wie lange ein unbearbeitetes Ereignis beibehalten werden soll. Ein DLQ ist ein standardmäßiger Amazon SQS EventBridge SQS-Warteschlangenplaner, der fehlgeschlagene Ereignisse zustellt, nachdem die Wiederholungsrichtlinie ausgeschöpft wurde. Sie können eine DLQ verwenden, um Probleme mit Ihrem Zeitplan oder seinem nachgelagerten Ziel zu beheben. Weitere Informationen zu finden Sie unterthe section called “Konfigurieren einer Queue für unzustellbare Nachrichten”.

In diesem Abschnitt finden Sie Beispiele für die Verwaltung Ihrer EventBridge Scheduler-Zeitpläne mit der Konsole, den AWS CLI und den EventBridge Scheduler-SDKs.

Themen

- Den Status des Zeitplans ändern
- Konfiguration flexibler Zeitfenster
- Konfigurieren einer Warteschlange für unzustellNachrichten für einen Zeitplan für unzustellNachrichten Nachrichten Nachrichten
- Löschen eines Zeitplans
- Als nächstes

# Den Status des Zeitplans ändern

Ein EventBridge Scheduler-Zeitplan hat zwei Status: aktiviert und deaktiviert. Im folgenden Beispiel wird `UpdateSchedule` ein Zeitplan deaktiviert, der alle fünf Minuten ausgelöst wird und ein Lambda-Ziel aufruft.

Wenn Sie verwenden`UpdateSchedule`, müssen Sie alle erforderlichen Parameter angeben. EventBridge Der Scheduler ersetzt Ihren Zeitplan durch die von Ihnen bereitgestellten Informationen. Wenn Sie keinen Parameter angeben, den Sie zuvor festgelegt haben, wird standardmäßig der Wert verwendet. `null`

Example AWS CLI

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

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

Im folgenden Beispiel werden das Python-SDK und der `UpdateSchedule` Vorgang verwendet, um einen Zeitplan zu deaktivieren, der auf Amazon SQS abzielt und ein vorgegebenes Ziel verwendet.

Example Python-SDK

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

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

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

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

# Konfiguration flexibler Zeitfenster

Wenn Sie Ihren Zeitplan mit einem flexiblen Zeitfenster konfigurieren, ruft EventBridge Scheduler das Ziel innerhalb des von Ihnen festgelegten Zeitfensters auf. Dies ist in Fällen nützlich, in denen kein genauer geplanter Aufruf von Zielen erforderlich ist. Die Festlegung eines flexiblen Zeitfensters verbessert die Zuverlässigkeit Ihres Zeitplans, da Ihre Zielaufrufe verteilt werden.

Wenn Sie beispielsweise ein flexibles Zeitfenster von 15 Minuten für einen Zeitplan konfigurieren, der jede Stunde ausgeführt wird, wird das Ziel innerhalb von 15 Minuten nach der geplanten Zeit aufgerufen. Im Folgenden AWS CLI und in den Beispielen für das EventBridge Scheduler SDK wird ein flexibles Zeitfenster von 15 Minuten für einen Zeitplan festgelegt, der einmal pro Stunde ausgeführt wird. `UpdateSchedule`

> **Note**
>
> Sie müssen angeben, ob Sie ein flexibles Zeitfenster festlegen möchten oder nicht. Wenn Sie diese Option nicht festlegen möchten, geben Sie an`OFF`. Wenn Sie den Wert auf setzen`FLEXIBLE`, müssen Sie anschließend ein maximales Zeitfenster angeben, in dem Ihr Zeitplan ausgeführt werden soll.

Example AWS CLI

```
$ aws scheduler update-schedule --name lambda-universal --schedule-expression 'rate(1
 hour)' \
--target '{"RoleArn": "ROLE_ARN", "Arn":"arn:aws:scheduler:::aws-sdk:lambda:invoke"
 "Input": "{\"FunctionName\":\"arn:aws:lambda:REGION:123456789012:function:HelloWorld
\",\"InvocationType\":\"Event\",\"Payload\":\"{\\\"message\\\":\\\"testing function\\
\"}\"}" }' \
--flexible-time-window '{ "Mode": "FLEXIBLE", "MaximumWindowInMinutes": 15} \
```

```
{
```

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

Example Python-SDK

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

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

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

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

# Konfigurieren einer Warteschlange für unzustellNachrichten für einen Zeitplan für unzustellNachrichten Nachrichten Nachrichten

Amazon EventBridge Scheduler unterstützt Dead-Letter Queues (DLQ) mithilfe des Amazon Simple Queue Service. Wenn ein Zeitplan sein Ziel nicht aufrufen kann, sendet EventBridge Scheduler eine JSON-Payload, die Aufrufdetails und alle vom Ziel empfangenen Antworten enthält, an eine von Ihnen angegebene Amazon SQS SQS-Standardwarteschlange.

Das folgende Thema bezieht sich auf diesen JSON als ein Dead-Letter-Ereignis. Mit einem Dead-Letter-Event können Sie Probleme mit Ihrem Zeitplan oder Ihren Zielen beheben. Wenn Sie eine Wiederholungsrichtlinie für Ihren Zeitplan konfigurieren, sendet der EventBridge Scheduler das Deadletter-Ereignis aus, das die von Ihnen festgelegte maximale Anzahl von Wiederholungsversuchen erschöpft.

In den folgenden Themen wird beschrieben, wie Sie eine Amazon SQS-Warteschlange als DLQ für Ihren Zeitplan konfigurieren, die Berechtigungen einrichten können, die EventBridge Scheduler für die Übermittlung von Nachrichten an Amazon SQS benötigt, und wie Sie Deadletter-Ereignisse vom DLQ empfangen können.

Themen

- Erstellen einer Amazon-SQS-Warteschlange
- Richten Sie Berechtigungen für Ausführungsrolle ein
- Geben Sie eine Warteschlange für unzustellNachrichten Nachrichten an.
- Ruft das Event für unzustellungshandbuch ab

## Erstellen einer Amazon-SQS-Warteschlange

Bevor Sie einen DLQ für Ihren Zeitplan konfigurieren, müssen Sie eine standardmäßige Amazon SQS SQS-Warteschlange erstellen. Anweisungen zum Erstellen einer Warteschlange mit der Amazon-SQS-Konsole finden Sie unter Erstellen einer Amazon-SQS-Warteschlange für Amazon-Simple-Warteschlangen.

> **Note**
>
> EventBridge Der Scheduler unterstützt nicht die Verwendung einer FIFO-Warteschlange als DLQ Ihres Zeitplans.

Verwenden Sie den folgendenAWS CLI Befehl, um eine Standardwarteschlange zu erstellen.

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

Wenn der Befehl erfolgreich ausgeführt wurde, sehen Sie dasQueueURL in der Ausgabe.

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

Nachdem Sie die Warteschlange erstellt haben, notieren Sie sich den Queue-ARN. Sie benötigen den ARN, wenn Sie einen DLQ für Ihren EventBridge Scheduler-Zeitplan angeben. Sie finden Ihren Queue-ARN in der Amazon SQS SQS-Konsole oder mithilfe des `get-queue-attributes`AWS CLIBefehls.

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

Wenn dies erfolgreich ist, sehen Sie den Queue-ARN in der Ausgabe.

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

Im nächsten Abschnitt fügen Sie Ihrer Rolle zur Ausführung des Zeitplans die erforderlichen Berechtigungen hinzu, damit EventBridge Scheduler Deadlet-Ereignisse an Amazon SQS übermitteln kann.

## Richten Sie Berechtigungen für Ausführungsrolle ein

Damit EventBridge Scheduler Deadlet-Ereignisse an Amazon SQS übermitteln kann, benötigt Ihre Rolle für die Ausführung von Terminplänen die folgende Berechtigungsrichtlinie. Weitere Informationen zum Anhängen einer neuen Berechtigungsrichtlinie an Ihre Rolle für die Ausführung des Zeitplans finden Sie unter Die Ausführungsrolle einrichten.

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

> **Note**
>
> Ihre Rolle zur Ausführung von Zeitplänen verfügt möglicherweise bereits über die erforderlichen Berechtigungen, wenn Sie EventBridge Scheduler verwenden, um ein Amazon SQS SQS-API-Ziel aufzurufen.

Im nächsten Abschnitt verwenden Sie die EventBridge Scheduler-Konsole und geben eine DLQ für Ihren Zeitplan an.

# Geben Sie eine Warteschlange für unzustellNachrichten Nachrichten an.

Um einen DLQ anzugeben, verwenden Sie die EventBridge Scheduler-Konsole oder die,AWS CLI um einen vorhandenen Zeitplan zu aktualisieren oder einen neuen zu erstellen.

Console

So geben Sie einen DLQ mithilfe der Konsole an

1. Melden Sie sich bei derAWS Management Console an und wählen Sie dann den folgenden Link, um den EventBridge Scheduler-Bereich der EventBridge Konsole zu öffnen: https://console.aws.amazon.com/scheduler/home
2. Erstellen Sie in der EventBridge Scheduler-Konsole einen neuen Zeitplan, oder wählen Sie einen vorhandenen Zeitplan aus der Liste der zu bearbeitenden Zeitpläne aus.
3. Führen Sie auf der Seite Einstellungen für die Dead-Letter Queue (DLQ) einen der folgenden Schritte aus:
   - Wählen Sie in meinemAWS Konto als DLQ die Option Amazon SQS SQS-Warteschlange auswählen und wählen Sie dann den Warteschleifen-ARN für Ihre DLQ aus der Dropdown-Liste aus.
   - Wählen Sie „Amazon SQS SQS-Warteschlange in anderenAWS Konten als DLQ angeben“ und geben Sie dann den Queue-ARN für Ihre DLQ ein. Wenn Sie eine Warteschlange in einem anderenAWS Konto auswählen, kann die EventBridge Scheduler-Konsole die Warteschlange-ARNs nicht in einer Dropdown-Liste anzeigen.
4. Überprüfen Sie Ihre Auswahl und wählen Sie dann Zeitplan erstellen oder Zeitplan speichern, um die Konfiguration eines DLQ abzuschließen.
5. (Optional) Um die DLQ-Details eines Zeitplans anzuzeigen, wählen Sie den Namen des Zeitplans aus der Liste aus und wählen Sie dann auf der Seite mit den Zeitplandetails den Tab Warteschlange für tote Buchstaben.

AWS CLI

Um einen vorhandenen Zeitplan mit dem zu aktualisierenAWS CLI

- Verwenden Sie den `update-schedule`Befehl, um Ihren Zeitplan zu aktualisieren. Geben Sie die Amazon SQS SQS-Warteschlange, die Sie zuvor erstellt haben, als DLQ an. Geben Sie die IAM-Rolle ARN, der Sie die erforderlichen Amazon SQS SQS-Berechtigungen

zugewiesen haben, als Ausführungsrolle an. Ersetzen Sie alle anderen Platzhalterwerte durch Ihre Informationen.

```
$ 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"}'
```

Um einen neuen Zeitplan mit einem DLQ zu erstellen, verwenden Sie denAWS CLI

- Verwenden Sie den `create-schedule`Befehl, um einen Zeitplan zu erstellen. Ersetzen Sie alle Platzhalterwerte durch Ihre Informationen.

```
$ 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"}'
```

Im nächsten Abschnitt verwenden Sie die, um vom DLQ einAWS CLI unzustellungshandbuch für unzustellungshandbuch für unzustellungshandbuch für unzustellungshandbuch.

## Ruft das Event für unzustellungshandbuch ab

Verwenden Sie den `receive-message`Befehl, wie im Folgenden gezeigt, um ein Dead-Letter-Ereignis aus dem DLQ abzurufen. Mithilfe des`--max-number-of-messages` Attributs können Sie die Anzahl der abzurufenden Nachrichten festlegen.

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

Wenn der Befehl erfolgreich ausgeführt wurde, wird eine Ausgabe ähnlich der Folgenden angezeigt.

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

Beachten Sie die folgenden Attribute im Deadletter-Ereignis, damit Sie mögliche Gründe für das Scheitern der Zielinovation identifizieren und beheben können.

- **ERROR_CODE**— Enthält den Fehlercode, den EventBridge Scheduler von der Service-API des Ziels empfängt. Im vorherigen Beispiel lautet der von Amazon SQS zurückgegebene FehlercodeAWS.SimpleQueueService.NonExistentQueue. Wenn der Zeitplan aufgrund eines Problems mit dem EventBridge Scheduler kein Ziel aufruft, wird stattdessen der folgende Fehlercode angezeigt:AWS.Scheduler.InternalServerError.
- **ERROR_MESSAGE**— Enthält die Fehlermeldung, die EventBridge Scheduler von der Service-API des Ziels erhält. Im vorherigen Beispiel lautet die von Amazon SQS zurückgegebene FehlermeldungThe specified queue does not exist for this wsdl version. Wenn der Zeitplan aufgrund eines Problems mit dem EventBridge Scheduler fehlschlägt, wird stattdessen die folgende Fehlermeldung angezeigt:Unexpected error occurred while processing the request.
- **TARGET_ARN**— Der ARN des Ziels, das Ihr Zeitplan aufruft, im folgenden Service-ARN-Format:arn:aws:scheduler:::aws-sdk:*service*:*apiAction*.
- **EXHAUSTED_RETRY_CONDITION**— Gibt an, warum das Ereignis an den DLQ übermittelt wurde. Dieses Attribut ist vorhanden, wenn es sich bei dem Fehler der Ziel-API um einen wiederholbaren Fehler und nicht um einen permanenten Fehler handelt. Das Attribut kann die Werte enthalten,MaximumRetryAttempts wenn EventBridge Scheduler es an den DLQ gesendet hat, nachdem die maximale Anzahl von Wiederholungsversuchen, die Sie für den Zeitplan konfiguriert haben, überschritten wurdeMaximumEventAgeInSeconds, oder wenn das Ereignis älter als das im Zeitplan konfigurierte Höchstalter ist und immer noch nicht zugestellt werden kann.

Im vorherigen Beispiel können wir anhand des Fehlercodes und der Fehlermeldung feststellen, dass die Zielwarteschlange, die wir für den Zeitplan angegeben haben, nicht existiert.

# Löschen eines Zeitplans

Sie können einen Zeitplan löschen, indem Sie entweder das automatische Löschen konfigurieren oder einen einzelnen Zeitplan manuell löschen. In den folgenden Themen erfahren Sie, wie Sie einen Zeitplan mit beiden Methoden löschen können und warum Sie möglicherweise eine Methode der anderen vorziehen.

Themen



## Löschen nach Abschluss des Zeitplans

Konfigurieren Sie das automatische Löschen nach Abschluss des Zeitplans, wenn Sie vermeiden möchten, dass Sie Ihre Zeitplanressourcen im EventBridge Scheduler einzeln verwalten müssen. In Anwendungen, in denen Sie Tausende von Zeitplänen gleichzeitig erstellen und Flexibilität benötigen, um die Anzahl Ihrer Zeitpläne bei Bedarf zu erhöhen, kann durch automatisches Löschen sichergestellt werden, dass Sie Ihr Kontingent für die Anzahl der Zeitpläne in einer bestimmten Region nicht erreichen.

Wenn Sie das automatische Löschen für einen Zeitplan konfigurieren, löscht EventBridge Scheduler den Zeitplan nach dem letzten Zielaufruf. Bei einmaligen Zeitplänen erfolgt dies, nachdem der Zeitplan sein Ziel einmal aufgerufen hat. Bei wiederkehrenden Zeitplänen, die Sie mit Rate- oder Cron-Ausdrücken einrichten, wird Ihr Zeitplan nach dem letzten Aufruf gelöscht. Der letzte Aufruf eines wiederkehrenden Zeitplans ist der Aufruf, der dem von Ihnen angegebenen am nächsten kommt. `EndDate` Wenn Sie einen Zeitplan mit automatischem Löschen konfigurieren, aber keinen Wert für angeben`EndDate`, löscht EventBridge Scheduler den Zeitplan nicht automatisch.

Sie können das automatische Löschen einrichten, wenn Sie einen Zeitplan zum ersten Mal erstellen, oder die Einstellungen für einen vorhandenen Zeitplan aktualisieren. In den folgenden Schritten wird beschrieben, wie Sie das automatische Löschen für einen vorhandenen Zeitplan konfigurieren.

AWS Management Console

1. Öffnen Sie die EventBridge Scheduler-Konsole unter https://console.aws.amazon.com/scheduler/.
2. Wählen Sie aus der Liste der Zeitpläne den Zeitplan aus, den Sie bearbeiten möchten, und klicken Sie dann auf Bearbeiten.
3. Wählen Sie in der Navigationsliste auf der linken Seite Einstellungen aus.
4. Wählen Sie im Abschnitt Aktion nach Abschluss des Zeitplans in der Dropdownliste die Option LÖSCHEN aus und speichern Sie dann Ihre Änderungen.

AWS CLI

1. Öffnen Sie ein neues Eingabeaufforderungsfenster.
2. Verwenden Sie den AWS CLI Befehl update-schedule, um einen vorhandenen Zeitplan zu aktualisieren, wie im Folgenden gezeigt. Der Befehl setzt den Wert auf `--action-after-completion`. `DELETE` In diesem Beispiel wird davon ausgegangen, dass Sie Ihre Zielkonfiguration lokal in einer JSON-Datei definiert haben. Um einen Zeitplan zu aktualisieren, müssen Sie das Ziel sowie alle anderen Zeitplanparameter angeben, die Sie für Ihren vorhandenen Zeitplan konfigurieren möchten.

   Dies ist ein wiederkehrender Zeitplan mit einer Rate von einem Aufruf pro Stunde. Daher geben Sie bei der Einstellung des `--action-after-completion` Parameters ein Enddatum an.

```
$ 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"}' \
```

## Manuelles Löschen

Wenn Sie einen Zeitplan nicht mehr benötigen, können Sie ihn mithilfe der `DeleteSchedule`Operation löschen.

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")
```

## Als nächstes

- Weitere Informationen zur Konfiguration von Zielvorlagen für Lambda- und Step-Funktionen sowie zur Verwendung des Parameters Universal Target finden Sie unter. Ziele verwalten
- Weitere Informationen zu den EventBridge Scheduler-Datentypen und API-Vorgängen finden Sie in der EventBridge Scheduler-API-Referenz.

# Verwaltung einer Zeitplangruppe

Eine Zeitplangruppe ist eine Amazon EventBridge Scheduler-Ressource, mit der Sie Ihre Zeitpläne organisieren.

Ihre AWS-Konto wird mit einer `default` Scheduler-Gruppe geliefert. Sie können der `default` Gruppe oder den von Ihnen erstellten und verwalteten Zeitplangruppen einen neuen Zeitplan zuordnen. Sie können bis zu 500 Zeitplangruppen in Ihrem erstellenAWS-Konto. Mit EventBridge Scheduler können Sie Zeitplangruppen statt einzelner Zeitpläne organisieren, indem Sie Tags anwenden.

Ein Tag ist eine Bezeichnung, die aus einem Schlüssel, bei dem die Groß- und Kleinschreibung beachtet wird, und einem von Ihnen definierten Wert besteht. Sie können Tags erstellen, um Zeitpläne nach Kriterien wie Zweck, Eigentümer oder Umgebung zu kategorisieren. Beispielsweise können Sie die Umgebung, zu der Ihre Zeitpläne gehören, mit dem folgenden Tag identifizieren:`environment:`*`production`*.

> **Important**
>
> Fügen Sie keine personenbezogenen Daten (Personally Identifiable Information, PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele AWS-Dienste zugänglich, einschließlich der Abrechnung. Tags sind nicht für private oder vertrauliche Daten gedacht.

Eine Zeitplangruppe hat zwei mögliche Zustände: AKTIV und LÖSCHEN.

Wenn Sie eine Gruppe zum ersten Mal erstellen, ist dies `ACTIVE` standardmäßig der Fall. Sie können einer `ACTIVE` Gruppe Zeitpläne hinzufügen. Wenn Sie eine Gruppe löschen, ändert sich der Status zu, `DELETING` bis EventBridge Scheduler das Löschen der zugehörigen Zeitpläne abgeschlossen hat. Nachdem EventBridge Scheduler die Zeitpläne in der Gruppe gelöscht hat, ist die Gruppe in Ihrem Konto nicht mehr verfügbar.

Verwenden Sie die folgenden Themen, um eine Zeitplangruppe zu erstellen und ihr ein Tag zuzuweisen. Sie ordnen der Gruppe auch einen Zeitplan zu und löschen schließlich die Gruppe.

Themen

- Eine Zeitplangruppe erstellen
- Löschen einer Zeitplangruppe

- Zugehörige Ressourcen

# Eine Zeitplangruppe erstellen

Verwenden Sie Zeitplangruppen und Tagging, um Zeitpläne zu organisieren, die einen gemeinsamen Zweck verfolgen oder zu derselben Umgebung gehören. In den folgenden Schritten erstellen Sie eine neue Zeitplangruppe und kennzeichnen sie mit einem Tag. Anschließend ordnen Sie dieser Gruppe einen neuen Zeitplan zu.

> **Note**
>
> Sobald Sie eine Gruppe erstellt haben, können Sie keinen Zeitplan aus dieser Gruppe entfernen oder den Zeitplan einer anderen Gruppe zuordnen. Sie können einen Zeitplan einer Gruppe nur zuordnen, wenn Sie den Zeitplan zum ersten Mal erstellen.

## Erster Schritt: Erstellen Sie eine neue Zeitplangruppe

In den folgenden Themen wird beschrieben, wie Sie eine neue Zeitplangruppe erstellen und sie mit dem folgenden Tag kennzeichnen:`environment:development`.

AWS Management Console

Um eine neue Gruppe mit dem zu erstellen AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im linken Navigationsbereich die Option Gruppen planen aus.
3. Wählen Sie auf der Seite Zeitplangruppen die Option Zeitplangruppe erstellen aus.
4. Geben Sie im Abschnitt „Details zur Zeitplangruppe“ unter Name einen Namen für die Gruppe ein. Zum Beispiel **`TestGroup`**.
5. Gehen Sie im Abschnitt Tags wie folgt vor:

   a. Wählen Sie Add new tag (Neues Tag hinzufügen) aus.

   b. Geben Sie unter Schlüssel den Namen ein, den Sie diesem Schlüssel zuweisen möchten. Geben Sie für dieses Tutorial ein, um die Umgebung zu benennen, zu der diese Zeitplangruppe gehört**`environment`**.

c. Geben Sie unter Wert — optional den Wert ein, den Sie diesem Schlüssel zuweisen möchten. Geben Sie für dieses Tutorial den Wert **`development`** für Ihren Umgebungsschlüssel ein.

> **Note**
>
> Sie können Ihrer Gruppe zusätzliche Tags hinzufügen, nachdem Sie sie erstellt haben.

6. Wählen Sie zum Abschluss „Zeitplangruppe erstellen“. Ihre neue Gruppe wird in der Liste der Zeitplangruppen angezeigt.
7. (Optional) Um eine Gruppe zu bearbeiten oder ihre Tags zu verwalten, aktivieren Sie das Kontrollkästchen für die neue Gruppe und wählen Sie Bearbeiten.

> **Note**
>
> Sie können die `default` Zeitplangruppe nicht bearbeiten.

AWS CLI

Um eine neue Gruppe zu erstellen, verwenden Sie AWS CLI

1. Öffnen Sie ein neues Befehlszeilenfenster.
2. Geben Sie über AWS Command Line Interface (AWS CLI) den folgenden `create-schedule-group`Befehl ein, um eine neue Gruppe zu erstellen. Dieser Befehl erstellt eine Gruppe mit einem Tag:`environment:development`. Sie können dieses Tag oder ein ähnliches Tag-System verwenden, um Ihre Zeitplangruppen entsprechend der Umgebung zu kennzeichnen, zu der sie gehören.

   Ersetzen Sie den Namen des Zeitplans und den Tag-Schlüssel und -Wert durch Ihre Informationen.

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

Standardmäßig befindet sich Ihre neue Gruppe im `ACTIVE` Bundesstaat. Sie können der neuen Gruppe, die Sie erstellt haben, jetzt neue Zeitpläne zuordnen.

## Schritt zwei: Einen Zeitplan mit der Gruppe verknüpfen

Gehen Sie wie folgt vor, um der Gruppe, die Sie im vorherigen Schritt erstellt haben, einen neuen Zeitplan zuzuordnen.

AWS Management Console

Um einen Zeitplan mit einer Gruppe zu verknüpfen, verwenden Sie AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im linken Navigationsbereich die Option Zeitpläne aus.
3. Wählen Sie in der Tabelle Zeitpläne die Option Zeitplan erstellen aus, um einen neuen Zeitplan zu erstellen.
4. Wählen Sie auf der Seite Zeitplandetails angeben für Zeitplangruppe den Namen Ihrer neuen Gruppe aus der Dropdownliste aus. Wählen Sie beispielsweise`TestGroup`.
5. Geben Sie ein Zeitplanmuster, ein Ziel und Einstellungen an und überprüfen Sie dann Ihre Auswahl auf der Seite Zeitplan überprüfen und speichern. Weitere Informationen zur Konfiguration eines neuen Zeitplans finden Sie unterErste Schritte.
6. Um den Zeitplan zu beenden und zu speichern, wählen Sie Zeitplan speichern.

AWS CLI

Um einen Zeitplan mit einer Gruppe zu verknüpfen, verwenden Sie AWS CLI

1. Öffnen Sie ein neues Befehlszeilenfenster.
2. Geben Sie über das AWS CLI Symbol AWS Command Line Interface () den folgenden `create-schedule`Befehl ein. Dadurch wird ein Zeitplan erstellt und dieser mit der Gruppe aus dem vorherigen Schritt verknüpft (benannt)`sqs-test-schedule`. Dieser Zeitplan verwendet den vordefinierten Amazon SQS SQS-Zieltyp, um den Vorgang aufzurufen. `SendMessage` Ersetzen Sie den Namen, das Ziel und den Gruppennamen des Zeitplans durch Ihre Informationen.

```
$ 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"}'
```

Ihr neuer Zeitplan ist jetzt der `TestGroup` Zeitplangruppe zugeordnet.

## Löschen einer Zeitplangruppe

Im Folgenden erfahren Sie, wie Sie eine Zeitplangruppe mit dem AWS Management Console und dem AWS Command Line Interface löschen. Wenn Sie eine Gruppe löschen, behält sie den `DELETING` Status, bis der EventBridge Scheduler alle Zeitpläne in der Gruppe löscht. Nachdem EventBridge Scheduler die Zeitpläne in der Gruppe gelöscht hat, ist die Gruppe in Ihrem Konto nicht mehr verfügbar.

> **Note**
>
> Sobald Sie eine Gruppe erstellt haben, können Sie keinen Zeitplan mehr aus dieser Gruppe entfernen oder den Zeitplan einer anderen Gruppe zuordnen. Sie können einen Zeitplan einer Gruppe nur zuordnen, wenn Sie den Zeitplan zum ersten Mal erstellen.

AWS Management Console

Um eine Gruppe mit dem zu löschen AWS Management Console

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im linken Navigationsbereich die Option Gruppen planen aus.
3. Suchen Sie auf der Seite „Gruppen planen“ in der Liste der vorhandenen Gruppen in der aktuellen Version die GruppeAWS-Region, die Sie löschen möchten. Wenn Sie die Gruppe, nach der Sie suchen, nicht sehen, wählen Sie eine andere ausAWS-Region.

> **Note**
>
> Sie können die Standardgruppe nicht löschen oder bearbeiten.

4. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie löschen möchten.
5. Wählen Sie Löschen.
6. Geben Sie im Dialogfeld „Zeitplangruppe löschen“ den Namen der Gruppe ein, um Ihre Auswahl zu bestätigen, und wählen Sie dann Löschen.
7. In der Liste der Zeitplangruppen ändert sich die Spalte Status und gibt an, dass Ihre Gruppe jetzt gelöscht wird. Die Gruppe verbleibt in diesem Status, bis der EventBridge Scheduler alle mit der Gruppe verknüpften Zeitpläne löscht.
8. Um die Liste zu aktualisieren und zu bestätigen, dass die Gruppe gelöscht wurde, wählen Sie das Aktualisierungssymbol.

### AWS CLI

Um eine Gruppe zu löschen, verwenden Sie AWS CLI

1. Öffnen Sie ein neues Befehlszeilenfenster.
2. Geben Sie in AWS Command Line Interface (AWS CLI) den folgenden `delete-schedule-group`Befehl ein, um die Zeitplangruppe zu löschen. Ersetzen Sie den Wert für `--name` durch Ihre Informationen.

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

Bei Erfolg gibt dieser AWS CLI Vorgang keine Antwort zurück.

3. Führen Sie den folgenden `get-schedule-group`Befehl aus, um zu überprüfen, ob sich die Gruppe im `DELETING` Status befindet.

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

Wenn der Vorgang erfolgreich ist, erhalten Sie eine Ausgabe, die der folgenden ähnelt:

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

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

EventBridge Der Scheduler löscht die Gruppe, nachdem er die mit der Gruppe verknüpften Zeitpläne gelöscht hat. Wenn Sie den Vorgang `get-schedule-group` erneut ausführen, erhalten Sie die folgende Antwort: `ResourceNotFoundException`

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

## Zugehörige Ressourcen

Weitere Informationen zu Zeitplangruppen finden Sie in den folgenden Ressourcen:

- CreateScheduleGroupVorgang in der EventBridge Scheduler-API-Referenz.
- DeleteScheduleGroupVorgang in der EventBridge Scheduler-API-Referenz.

# Ziele verwalten

In den folgenden Themen wird beschrieben, wie Sie Templates und universelle Ziele mit EventBridge Scheduler verwenden. Außerdem finden Sie eine Liste der unterstütztenAWS Dienste, die Sie mithilfe des universellen Zielparameters von EventBridge Scheduler konfigurieren können.

Vorlagenziele sind eine Reihe allgemeiner API-Operationen für eine Gruppe vonAWS Kerndiensten wie Amazon SQS, Lambda und Step Functions. Sie können beispielsweise auf den Invoke-API-Vorgang von Lambda abzielen, indem Sie die Funktion ARN angeben, oder den `SendMessage`Vorgang von Amazon SQS mit dem Warteschleifen-ARN des Ziels.

Das universelle Ziel ist ein anpassbarer Satz von Parametern, mit denen Sie eine breitere Palette von API-Vorgängen für vieleAWS Dienste aufrufen können. Sie können beispielsweise den Universal Target Parameter (UTP) von EventBridge Scheduler verwenden, um mithilfe des `CreateQueue`Vorgangs eine neue Amazon SQS SQS-Warteschlange zu erstellen.

Um entweder vordefinierte oder universelle Ziele zu konfigurieren, muss Ihr Zeitplan über die Berechtigung verfügen, den API-Vorgang aufzurufen, den Sie als Ihr Ziel konfiguriert haben. Dazu fügen Sie die erforderlichen Berechtigungen zur Ausführungsrolle Ihres Zeitplans hinzu. Um beispielsweise auf den `SendMessage`Betrieb von Amazon SQS abzuzielen, wird der Ausführungsrolle die Berechtigung erteilt, die`sqs:SendMessage` Aktion auszuführen. In den meisten Fällen können Sie die erforderlichen Berechtigungen hinzufügen, indem Sie die AWSverwalteten Richtlinien verwenden, die der Zieldienst unterstützt. Sie können jedoch auch Ihre eigenen, vom Kunden verwalteten Richtlinien erstellen oder Inline-Berechtigungen zu einer vorhandenen Richtlinie hinzufügen, die der Ausführungsrolle zugeordnet ist. In den folgenden Themen finden Sie Beispiele für das Hinzufügen von Berechtigungen für Zieltypen mit Vorlage und für universelle Zieltypen.

Weitere Informationen zum Einrichten einer Ausführungsrolle für einen Zeitplan finden Sie unterthe section called “Einrichten der Ausführungsrolle”.

Themen

# Verwenden von Vorlagenzielen

Vorlagenziele sind eine Reihe gängiger API-Operationen für eine Gruppe von Core- AWS Services wie Amazon SQS, Lambda und Step Functions. Sie können beispielsweise auf die Lambda-`Invoke`Operation abzielen, indem Sie den Funktions-ARN oder die -Operation von Amazon SQS mithilfe des Warteschlangen-ARN angeben. `SendMessage` Um ein Vorlagenziel zu konfigurieren, müssen Sie der Ausführungsrolle des Zeitplans auch Berechtigungen erteilen, um den Ziel-API-Vorgang auszuführen.

Um ein Vorlagenziel programmgesteuert mit der AWS CLI oder einem der EventBridge Scheduler-SDKs zu konfigurieren, müssen Sie den ARN der Ausführungsrolle, den ARN für die Zielressource, eine optionale Eingabe, die der EventBridge Scheduler an das Ziel liefern soll, und für einige Vorlagenziele einen eindeutigen Satz von Parametern mit zusätzlichen Konfigurationsoptionen für dieses Ziel angeben. Wenn Sie den ARN für eine Vorlagen-Zielressource angeben, geht EventBridge Scheduler automatisch davon aus, dass Sie die unterstützte API-Operation für diesen Service aufrufen möchten. Wenn Sie möchten, dass EventBridge Scheduler auf einen anderen API-Vorgang für den Service abzielt, müssen Sie das Ziel als universelles Ziel konfigurieren.

Im Folgenden finden Sie eine vollständige Liste aller Vorlagenziele, die EventBridge Scheduler unterstützt, und gegebenenfalls die eindeutigen zugehörigen Parameter jedes Ziels. Wählen Sie den Link für jeden Parametersatz aus, um die erforderlichen und optionalen Felder in der EventBridge Scheduler-API-Referenz anzuzeigen.

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

  - Parameter: SageMakerPipelineParameters
- Amazon SNS – Publish
- Amazon SQS – SendMessage
  - Parameter: SqsParameters
- Step Functions – StartExecution

In den folgenden Beispielen erfahren Sie, wie Sie verschiedene Vorlagenziele und die erforderlichen IAM-Berechtigungen für jedes beschriebene Ziel konfigurieren.

## Amazon SQS **SendMessage**

Example Berechtigungsrichtlinie für die Ausführungsrolle

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

Example AWS CLI

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

Example Python-SDK

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

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

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

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

### Example Java-SDK

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

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

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

## Lambda **Invoke**

### Example Berechtigungsrichtlinie für die Ausführungsrolle

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

### Example AWS CLI

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

### Example Python-SDK

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

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

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

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

### Example Java-SDK

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

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

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

## Schrittfunktionen **`StartExecution`**

### Example Berechtigungsrichtlinie für die Ausführungsrolle

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

### Example AWS CLI

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

### Example Python-SDK

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

flex_window = { "Mode": "OFF" }

sfn_templated= {
```

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

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

### Example Java-SDK

```
package com.example;

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


public class MySchedulerApp {

    public static void main(String[] args) {

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

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

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

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

# Verwendung universeller Ziele

Ein universelles Ziel ist ein anpassbarer Satz von Parametern, mit dem Sie einen breiteren Satz von API-Vorgängen für viele AWS Dienste aufrufen können. Sie können beispielsweise einen Universal Target Parameter (UTP) verwenden, um mithilfe des Vorgangs eine neue Amazon SQS SQS-Warteschlange zu erstellen. `CreateQueue`

Um mithilfe des oder eines der AWS CLI EventBridge Scheduler-SDKs ein universelles Ziel für Ihren Zeitplan zu konfigurieren, müssen Sie die folgenden Informationen angeben:

- RoleArn— Der ARN für die Ausführungsrolle, die Sie für das Ziel verwenden möchten. Die von Ihnen angegebene Ausführungsrolle muss über die Berechtigungen zum Aufrufen des API-Vorgangs verfügen, auf den Ihr Zeitplan abzielen soll.
- ARN — Der komplette Service-ARN, einschließlich des API-Vorgangs, auf den Sie abzielen möchten, im folgenden Format:`arn:aws:scheduler:::aws-sdk:`*`service`*`:`*`apiAction`*.

  Für Amazon SQS lautet der von Ihnen angegebene Servicename beispielsweise. `arn:aws:scheduler:::aws-sdk:`**`sqs:sendMessage`**
- Eingabe — Ein wohlgeformtes JSON, das Sie mit den Anforderungsparametern angeben, die EventBridge Scheduler an die Ziel-API sendet. Die Parameter und die Form des JSON, das Sie eingeben, `Input` werden durch die Service-API bestimmt, die Ihr Zeitplan aufruft. Diese Informationen finden Sie in der API-Referenz für den Service, auf den Sie abzielen möchten.

## Nicht unterstützte Aktionen

EventBridge Scheduler unterstützt keine schreibgeschützten API-Aktionen, wie z. B. allgemeine `GET` Operationen, die mit der folgenden Liste von Präfixen beginnen:

```
get
describe
list
poll
```

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

Der Dienst-ARN für die GetQueueUrlAPI-Aktion wäre beispielsweise wie folgt:`arn:aws:scheduler:::aws-sdk:sqs:`**`getQueueURL`**. Da die API-Aktion mit dem `get` Präfix beginnt, unterstützt EventBridge Scheduler dieses Ziel nicht. Ebenso wird die Amazon MQ MQ-Aktion `ListBrokers`nicht als Ziel unterstützt, da der Vorgang mit dem Präfix beginnt. `list`

## Beispiele für die Verwendung des universellen Ziels

Die Parameter, die Sie im `Input` Zeitplanfeld übergeben, hängen von den Anforderungsparametern ab, die die Service-API, die Sie aufrufen möchten, akzeptiert. Um beispielsweise Lambda als Ziel zu verwenden `Invoke`, können Sie die in AWS LambdaAPI-Referenz aufgeführten Parameter festlegen. Dazu gehört die optionale JSON-Nutzlast, die Sie an eine Lambda-Funktion übergeben können.

Informationen zu den Parametern, die Sie für verschiedene APIs festlegen können, finden Sie in der API-Referenz für diesen Dienst. Ähnlich wie bei Lambda `Invoke` akzeptieren einige APIs URI-Parameter sowie eine Payload für den Anforderungstext. In solchen Fällen geben Sie die URI-Pfadparameter sowie die JSON-Nutzlast in Ihrem Zeitplan an. `Input`

Die folgenden Beispiele zeigen, wie Sie das universelle Ziel verwenden, um allgemeine API-Operationen mit Lambda, Amazon SQS und Step Functions aufzurufen.

### 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");
    }
}
```

# Hinzufügen von Kontextattributen

Verwenden Sie die folgenden Schlüsselwörter in der Payload, die Sie an das Ziel übergeben, um Metadaten über den Zeitplan zu sammeln. EventBridge Scheduler ersetzt jedes Schlüsselwort durch seinen jeweiligen Wert, wenn Ihr Zeitplan das Ziel aufruft.

- **<aws.scheduler.schedule-arn>**— Der ARN des Zeitplans.
- **<aws.scheduler.scheduled-time>**— Die Zeit, die Sie für den Zeitplan angegeben haben, um sein Ziel aufzurufen, zum Beispiel. `2022-03-22T18:59:43Z`
- **<aws.scheduler.execution-id>**— Die eindeutige ID, die EventBridge Scheduler jedem versuchten Aufruf eines Ziels zuweist, zum Beispiel. `d32c5kddcf5bb8c3`
- **<aws.scheduler.attempt-number>**— Ein Zähler, der die Nummer des Versuchs für den aktuellen Aufruf identifiziert, zum Beispiel. 1

Dieses Beispiel zeigt die Erstellung eines Zeitplans, der alle fünf Minuten ausgelöst wird und den Amazon SQS `SendMessage` SQS-Vorgang als universelles Ziel aufruft. Der Nachrichtentext enthält den Wert für. `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)
```

## Als nächstes

Weitere Informationen zu den EventBridge Scheduler-Datentypen und API-Operationen finden Sie in der EventBridge Scheduler-API-Referenz.

# Sicherheit in Amazon EventBridge Scheduler

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon EventBridge Scheduler gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von EventBridge Scheduler anwenden können. In den folgenden Themen erfahren Sie, wie Sie EventBridge Scheduler so konfigurieren, dass Sie Ihre Sicherheits- und Compliance-Ziele erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Sie bei der Überwachung und Sicherung Ihrer EventBridge Scheduler-Ressourcen unterstützen.

Themen

# Zugriff auf Amazon EventBridge Scheduler verwalten

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Scheduler-Ressourcen zu verwenden EventBridge . IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen



## Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie im EventBridge Scheduler ausführen.

Dienstbenutzer — Wenn Sie den EventBridge Scheduler-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr EventBridge Scheduler-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie im EventBridge Scheduler nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Fehlerbehebung bei Identität und Zugriff auf Amazon EventBridge Scheduler

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die EventBridge Scheduler-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff EventBridge auf Scheduler. Es ist Ihre Aufgabe, zu bestimmen, auf welche EventBridge Scheduler-Funktionen und -Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um

die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit EventBridge Scheduler verwenden kann, finden Sie unter. So funktioniert EventBridge Scheduler mit IAM

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Scheduler zu verwalten. EventBridge Beispiele für identitätsbasierte EventBridge Scheduler-Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Verwenden identitätsbasierter Richtlinien

## Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -

Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

### AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Der Zugriff erfolgt, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

### Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

### IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen

wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

### Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern,

welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

## Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

## Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

## Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird,

ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

## So funktioniert EventBridge Scheduler mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf EventBridge Scheduler zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für die Verwendung mit Scheduler verfügbar sind. EventBridge

IAM-Funktionen, die Sie mit Amazon EventBridge Scheduler verwenden können

| IAM-Feature | EventBridge Scheduler-Unterstützung |
|---|---|
| Identitätsbasierte Richtlinien | Ja |
| Ressourcenbasierte Richtlinien | Nein |
| Richtlinienaktionen | Ja |
| Richtlinienressourcen | Ja |
| Richtlinienbedingungsschlüssel (services pezifisch) | Ja |
| ACLs | Nein |
| ABAC (Tags in Richtlinien) | Teilweise |
| Temporäre Anmeldeinformationen | Ja |
| Hauptberechtigungen | Ja |
| Servicerollen | Ja |
| Service-verknüpfte Rollen | Nein |

Einen allgemeinen Überblick darüber, wie EventBridge Scheduler und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWS IAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

## Identitätsbasierte Richtlinien für Scheduler EventBridge

| | |
|---|---|
| Unterstützt Richtlinien auf Identitätsbasis. | Ja |

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Scheduler EventBridge

Beispiele für identitätsbasierte Richtlinien von EventBridge Scheduler finden Sie unter. Verwenden identitätsbasierter Richtlinien

## Ressourcenbasierte Richtlinien innerhalb von Scheduler EventBridge

| | |
|---|---|
| Unterstützt ressourcenbasierte Richtlinien | Nein |

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das

Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

## Richtlinienaktionen für Scheduler EventBridge

| | |
|---|---|
| Unterstützt Richtlinienaktionen | Ja |

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der EventBridge Scheduler-Aktionen finden Sie unter Von Amazon EventBridge Scheduler definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen im EventBridge Scheduler verwenden vor der Aktion das folgende Präfix:

```
scheduler
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
```

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

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

## Richtlinienressourcen für Scheduler EventBridge

| | |
|---|---|
| Unterstützt Richtlinienressourcen | Ja |

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der EventBridge Scheduler-Ressourcentypen und ihrer ARNs finden Sie unter Von Amazon EventBridge Scheduler definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon EventBridge Scheduler definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von EventBridge Scheduler finden Sie unter. Verwenden identitätsbasierter Richtlinien

## Bedingungsschlüssel für Richtlinien für Scheduler EventBridge

| | |
|---|---|
| Unterstützt servicespezifische Richtlinienbedingungsschlüssel | Ja |

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der EventBridge Scheduler-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon EventBridge Scheduler in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon EventBridge Scheduler definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von EventBridge Scheduler finden Sie unter. Verwenden identitätsbasierter Richtlinien

## ACLs im Scheduler EventBridge

| | |
|---|---|
| Unterstützt ACLs | Nein |

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

## ABAC mit Scheduler EventBridge

| | |
|---|---|
| Unterstützt ABAC (Tags in Richtlinien) | Teilweise |

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

## Verwenden temporärer Anmeldeinformationen mit Scheduler EventBridge

| | |
|---|---|
| Unterstützt temporäre Anmeldeinformationen | Ja |

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

## Serviceübergreifende Prinzipalberechtigungen für Scheduler EventBridge

| | |
|---|---|
| Unterstützt Forward Access Sessions (FAS) | Ja |

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

## Servicerollen für Scheduler EventBridge

| | |
|---|---|
| Unterstützt Servicerollen | Ja |

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die EventBridge Scheduler-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn der EventBridge Scheduler Sie dazu anleitet.

### Dienstbezogene Rollen für Scheduler EventBridge

| | |
|---|---|
| Unterstützt serviceverknüpfte Rollen | Nein |

Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

## Verwenden identitätsbasierter Richtlinien

Standardmäßig sind Benutzer und Rollen nicht berechtigt, EventBridge Scheduler-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von EventBridge Scheduler definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Scheduler in der Service Authorization Reference.

Themen



## Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand EventBridge Scheduler-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und

Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

## EventBridge Scheduler-Berechtigungen

Damit ein IAM-Prinzipal (Benutzer, Gruppe oder Rolle) Zeitpläne im EventBridge Scheduler erstellen und über die Konsole oder die API auf EventBridge Scheduler-Ressourcen zugreifen kann, müssen für den Prinzipal eine Reihe von Berechtigungen zu seiner Berechtigungsrichtlinie hinzugefügt werden. Sie können diese Berechtigungen je nach Aufgabenbereich des Prinzipals konfigurieren. Beispielsweise benötigt ein Benutzer oder eine Rolle, die die EventBridge Scheduler-Konsole nur zum Anzeigen einer Liste vorhandener Zeitpläne verwendet, nicht über die zum Aufrufen des `CreateSchedule` API-Vorgangs erforderlichen Berechtigungen. Wir empfehlen, Ihre identitätsbasierten Berechtigungen so anzupassen, dass Sie nur den am wenigsten privilegierten Personen Zugriff gewähren.

In der folgenden Liste sind die Ressourcen von EventBridge Scheduler und die entsprechenden unterstützten Aktionen aufgeführt.

- Plan
  - `scheduler:ListSchedules`
  - `scheduler:GetSchedule`
  - `scheduler:CreateSchedule`
  - `scheduler:UpdateSchedule`
  - `scheduler:DeleteSchedule`
- Gruppe planen
  - `scheduler:ListScheduleGroups`
  - `scheduler:GetScheduleGroup`
  - `scheduler:CreateScheduleGroup`
  - `scheduler:DeleteScheduleGroup`
  - `scheduler:ListTagsForResource`
  - `scheduler:TagResource`
  - `scheduler:UntagResource`

Sie können EventBridge Scheduler-Berechtigungen verwenden, um Ihre eigenen, vom Kunden verwalteten Richtlinien zur Verwendung mit EventBridge Scheduler zu erstellen. Sie können auch die im folgenden Abschnitt beschriebenen AWS verwalteten Richtlinien verwenden, um die erforderlichen Berechtigungen für allgemeine Anwendungsfälle zu gewähren, ohne Ihre eigenen Richtlinien verwalten zu müssen.

## AWS verwaltete Richtlinien für EventBridge Scheduler

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die AWS erstellt und verwaltet werden. Verwaltete oder vordefinierte Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch. Die folgenden AWS verwalteten Richtlinien, die Sie Benutzern in Ihrem Konto zuordnen können, sind spezifisch für Scheduler: EventBridge

- the section called “`AmazonEventBridgeSchedulerFullAccess`”— Gewährt vollen Zugriff auf EventBridge Scheduler über die Konsole und die API.

- the section called “AmazonEventBridgeSchedulerReadOnlyAccess”— Gewährt schreibgeschützten Zugriff auf den Scheduler. EventBridge

### AmazonEventBridgeSchedulerFullAccess

Die AmazonEventBridgeSchedulerFullAccess verwaltete Richtlinie gewährt Berechtigungen zur Verwendung aller EventBridge Scheduler-Aktionen für Zeitpläne und Zeitplangruppen.

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

### AmazonEventBridgeSchedulerReadOnlyAccess

Die AmazonEventBridgeSchedulerReadOnlyAccess verwaltete Richtlinie gewährt nur Leseberechtigungen zum Anzeigen von Details zu Ihren Zeitplänen und Zeitplangruppen.

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

```
                "scheduler:GetSchedule",
                "scheduler:GetScheduleGroup",
                "scheduler:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

## Vom Kunden verwaltete Richtlinien für Scheduler EventBridge

Verwenden Sie die folgenden Beispiele, um Ihre eigenen kundenverwalteten Richtlinien für EventBridge Scheduler zu erstellen. Durch vom Kunden verwaltete Richtlinien können Sie nur Berechtigungen für die Aktionen und Ressourcen gewähren, die für Anwendungen und Benutzer in Ihrem Team entsprechend der Aufgabenstellung eines Prinzipals erforderlich sind.

Themen

- Beispiel: CreateSchedule
- Beispiel: GetSchedule
- Beispiel: UpdateSchedule
- Beispiel: DeleteScheduleGroup

### Beispiel: **`CreateSchedule`**

Wenn Sie einen neuen Zeitplan erstellen, wählen Sie aus, ob Sie Ihre Daten im EventBridge Scheduler mit einem oder einem AWS-eigener Schlüsselvom Kunden verwalteten Schlüssel verschlüsseln möchten.

Die folgende Richtlinie ermöglicht es einem Prinzipal, einen Zeitplan zu erstellen und die Verschlüsselung mithilfe eines anzuwenden. AWS-eigener Schlüssel Mit einem AWS-eigener Schlüssel werden Ressourcen auf AWS Key Management Service (AWS KMS) für Sie AWS verwaltet, sodass Sie für die Interaktion keine zusätzlichen Berechtigungen benötigen AWS KMS.

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

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

Verwenden Sie die folgende Richtlinie, um es einem Prinzipal zu ermöglichen, einen Zeitplan zu erstellen und einen vom AWS KMS Kunden verwalteten Schlüssel für die Verschlüsselung zu verwenden. Um einen vom Kunden verwalteten Schlüssel verwenden zu können, muss ein Principal berechtigt sein, auf die AWS KMS Ressourcen in Ihrem Konto zuzugreifen. Diese Richtlinie gewährt Zugriff auf einen einzelnen angegebenen KMS-Schlüssel, der zum Verschlüsseln von Daten auf EventBridge Scheduler verwendet werden kann. Alternativ können Sie ein Platzhalterzeichen (*) verwenden, um Zugriff auf alle Schlüssel in einem Konto oder auf eine Teilmenge zu gewähren, die einem bestimmten Namensmuster entspricht.

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

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

### Beispiel: **`GetSchedule`**

Verwenden Sie die folgende Richtlinie, um es einem Prinzipal zu ermöglichen, Informationen über einen Zeitplan abzurufen.

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

Beispiel: **`UpdateSchedule`**

Verwenden Sie die folgenden Richtlinien, um es einem Prinzipal zu ermöglichen, einen Zeitplan zu aktualisieren, indem er die `scheduler:UpdateSchedule` Aktion aufruft. Ähnlich wie hängt die Richtlinie davon ab`CreateSchedule`, ob der Zeitplan einen AWS KMS AWS-eigener Schlüssel oder einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwendet. Verwenden Sie für einen Zeitplan, der mit einem konfiguriert wurde AWS-eigener Schlüssel, die folgende Richtlinie:

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

Verwenden Sie für einen Zeitplan, der mit einem vom Kunden verwalteten Schlüssel konfiguriert wurde, die folgende Richtlinie. Diese Richtlinie beinhaltet zusätzliche Berechtigungen, die es einem Prinzipal ermöglichen, auf AWS KMS Ressourcen in Ihrem Konto zuzugreifen:

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

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

Beispiel: **`DeleteScheduleGroup`**

Verwenden Sie die folgende Richtlinie, um einem Prinzipal das Löschen einer Zeitplangruppe zu ermöglichen. Wenn Sie eine Gruppe löschen, löschen Sie auch die mit dieser Gruppe verknüpften Zeitpläne. Der Hauptbenutzer, der die Gruppe löscht, muss berechtigt sein, auch die mit dieser Gruppe verknüpften Zeitpläne zu löschen. Diese Richtlinie gewährt einem Prinzipal die Berechtigung, die `scheduler:DeleteScheduleGroup` Aktion für die angegebenen Zeitplangruppen sowie für alle Zeitpläne in der Gruppe aufzurufen:

> **Note**
>
> EventBridge Scheduler unterstützt nicht die Angabe von Berechtigungen auf Ressourcenebene für einzelne Zeitpläne. Die folgende Aussage ist beispielsweise ungültig und sollte nicht in Ihrer Richtlinie enthalten sein: `"Resource": "arn:aws:scheduler:us-west-2:123456789012:schedule/my-group/my-schedule-name"`

```
{
```

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

## AWS verwaltete Richtlinienaktualisierungen

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| the section called “AmazonEventBridgeSchedulerFullAccess”— Neue verwaltete Richtlinie | EventBridge Scheduler bietet Unterstützung für eine neue verwaltete Richtlinie, die Benutzern vollen Zugriff auf alle Ressourcen, einschließlich Zeitpläne und Zeitplangruppen, gewährt. | 10. November 2022 |
| the section called “AmazonEventBridgeSchedulerReadOnlyAc | EventBridge Scheduler bietet Unterstützung für eine neue verwaltete Richtlinie, die Benutzern schreibgeschützten | 10. November 2022 |

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| cess "— Neue verwaltete Richtlinie | Zugriff auf alle Ressourcen, einschließlich Zeitpläne und Zeitplangruppen, gewährt. | |
| EventBridge Scheduler hat mit der Nachverfolgung von Änderungen begonnen | EventBridge Scheduler hat damit begonnen, Änderunge n für seine AWS verwalteten Richtlinien zu verfolgen. | 10. November 2022 |

## Confused-Deputy-Prävention

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiertere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ihrer Rolle für die Ausführung von Zeitplänen zu verwenden, um die Berechtigungen einzuschränken, die EventBridge Scheduler einem anderen Dienst für den Zugriff auf die Ressource erteilt. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Die folgende Bedingung ist auf eine einzelne Zeitplangruppe beschränkt: `arn:aws:scheduler:*:`*`123456789012`*`:schedule-group/`*`your-schedule-group`*

Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel

`aws:SourceArn` mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Zum Beispiel: `arn:aws:scheduler:*:123456789012:schedule-group/*`.

Der Wert von `aws:SourceArn` muss Ihr EventBridge Scheduler-Zeitplangruppen-ARN sein, auf den Sie diese Bedingung eingrenzen möchten.

> **Important**
>
> Beschränken Sie die `aws:SourceArn` Anweisung nicht auf einen bestimmten Zeitplan oder ein Zeitplannamenpräfix. Der von Ihnen angegebene ARN muss eine Zeitplangruppe sein.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in Ihrer Vertrauensrichtlinie für die Ausführungsrolle verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern:

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

## Fehlerbehebung bei Identität und Zugriff auf Amazon EventBridge Scheduler

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit EventBridge Scheduler und IAM auftreten können.

Themen



## Ich bin nicht autorisiert, eine Aktion im Scheduler auszuführen EventBridge

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `scheduler:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Mateo-Richtlinie aktualisiert werden, damit er mit der `scheduler:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht autorisiert sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an EventBridge Scheduler übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion im EventBridge Scheduler auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

## Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine EventBridge Scheduler-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob EventBridge Scheduler diese Funktionen unterstützt, finden Sie unter. So funktioniert EventBridge Scheduler mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie im IAM-Benutzerhandbuch unter Kontenübergreifender Ressourcenzugriff in IAM.

# Datenschutz in Amazon EventBridge Scheduler

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon EventBridge Scheduler. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit EventBridge Scheduler oder anderen Geräten arbeiten und die Konsole, die AWS-Services API oder SDKs verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen



## Verschlüsselung im Ruhezustand

In diesem Abschnitt wird beschrieben, wie Amazon EventBridge Scheduler Ihre Daten im Ruhezustand ver- und entschlüsselt. Daten im Ruhezustand sind Daten, die im EventBridge Scheduler und den dem Service zugrunde liegenden Komponenten gespeichert sind. EventBridge Scheduler ist in AWS Key Management Service (AWS KMS) integriert, um Ihre Daten mit einem zu verschlüsseln und zu entschlüsseln. AWS KMS key EventBridge Scheduler unterstützt zwei Arten von KMS-Schlüsseln: und vom Kunden AWS-eigene Schlüsselverwaltete Schlüssel.

> **Note**
>
> EventBridge Scheduler unterstützt nur die Verwendung von KMS-Schlüsseln mit symmetrischer Verschlüsselung.

AWS-eigene Schlüsselsind KMS-Schlüssel, die ein AWS Dienst besitzt und verwaltet, sodass sie in mehreren AWS Konten verwendet werden können. Die vom AWS-eigene Schlüssel EventBridge Scheduler verwendeten Daten werden zwar nicht in Ihrem AWS Konto gespeichert, EventBridge Scheduler verwendet sie jedoch, um Ihre Daten und Ressourcen zu schützen. Standardmäßig verschlüsselt und entschlüsselt der EventBridge Scheduler all Ihre Daten mit einem eigenen Schlüssel. AWS Sie müssen Ihre AWS-eigener Schlüssel oder ihre Zugriffsrichtlinien nicht verwalten. Es fallen keine Gebühren an, wenn EventBridge Scheduler Ihre Daten schützt, und deren Nutzung wird nicht als Teil Ihrer AWS KMS Kontingente in Ihrem Konto gezählt. AWS-eigene Schlüssel

Von Kunden verwaltete Schlüssel sind KMS-Schlüssel, die in Ihrem AWS Konto gespeichert sind und die Sie erstellen, besitzen und verwalten. Wenn Ihr spezieller Anwendungsfall erfordert, dass Sie die Verschlüsselungsschlüssel, die Ihre Daten schützen, auf EventBridge Scheduler kontrollieren und prüfen, können Sie einen vom Kunden verwalteten Schlüssel verwenden. Wenn Sie sich für einen vom Kunden verwalteten Schlüssel entscheiden, müssen Sie Ihre Schlüsselrichtlinie verwalten. Für kundenverwaltete Schlüssel fällt eine monatliche Gebühr sowie eine Gebühr für die über das

kostenlose Kontingent hinausgehende Nutzung an. Die Verwendung eines vom Kunden verwalteten Schlüssels zählt ebenfalls zu Ihrem AWS KMS Kontingent. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service Preisgestaltung.

Themen



## Verschlüsselungsartefakte

In der folgenden Tabelle werden die verschiedenen Datentypen beschrieben, die EventBridge Scheduler im Ruhezustand verschlüsselt, und welche Art von KMS-Schlüssel er für jede Kategorie unterstützt.

| Datentyp | Beschreibung | AWS-eigener Schlüssel | vom Kunden verwalteter Schlüssel |
|---|---|---|---|
| Nutzlast (bis zu 256 KB) | Die Daten, die Sie im `TargetInput` Parameter des Zeitplans angeben, wenn Sie den Zeitplan so konfigurieren, dass er an das Ziel gesendet wird. | Unterstützt | Unterstützt |
| Bezeichner und Status | Der eindeutige Name und der Status (aktiviert, deaktiviert) des Zeitplans. | Unterstützt | Nicht unterstützt |
| Konfiguration des Zeitplans | Der Planungsausdruck, z. B. der Rate- oder Cron-Ausdruck für wiederkehrende Zeitpläne, | Unterstützt | Nicht unterstützt |

| Datentyp | Beschreibung | AWS-eigener Schlüssel | vom Kunden verwalteter Schlüssel |
|---|---|---|---|
| | der Zeitstempel für einmalige Aufrufe sowie das Startdatum, das Enddatum und die Zeitzone des Zeitplans. | | |
| Zielkonfiguration | Der Amazon-Ressourcenname (ARN) des Ziels und andere zielbezogene Konfigurationsdetails. | Unterstützt | Nicht unterstützt |
| Konfiguration des Aufrufs- und Fehlerverhaltens | Flexible Zeitfenster konfiguration, die Wiederholungsrichtlinie des Zeitplans und die Informationen zur Warteschlange mit unerlaubten Nachrichten, die für fehlgeschlagene Lieferungen verwendet werden. | Unterstützt | Nicht unterstützt |

EventBridge Scheduler verwendet Ihre vom Kunden verwalteten Schlüssel nur beim Verschlüsseln und Entschlüsseln der Ziel-Payload, wie in der vorherigen Tabelle beschrieben. Wenn Sie sich dafür entscheiden, einen vom Kunden verwalteten Schlüssel zu verwenden, verschlüsselt und entschlüsselt EventBridge Scheduler die Payload zweimal: einmal mit dem Standard und ein anderes Mal mit dem von Ihnen angegebenen AWS-eigener Schlüssel, vom Kunden verwalteten Schlüssel. Für alle anderen Datentypen verwendet EventBridge Scheduler nur den Standard, um Ihre Daten im Ruhezustand AWS-eigener Schlüssel zu schützen.

Im folgenden the section called “KMS-Schlüssel verwalten” Abschnitt erfahren Sie, wie Sie Ihre IAM-Ressourcen und wichtigen Richtlinien verwalten müssen, um einen vom Kunden verwalteten Schlüssel mit EventBridge Scheduler verwenden zu können.

## KMS-Schlüssel verwalten

Sie können optional einen vom Kunden verwalteten Schlüssel zur Ver- und Entschlüsselung der Payload bereitstellen, die Ihr Zeitplan an das Ziel übermittelt. EventBridge Scheduler verschlüsselt und entschlüsselt Ihre Nutzdaten mit bis zu 256 KB an Daten. Für die Verwendung eines vom Kunden verwalteten Schlüssels fallen eine monatliche Gebühr und eine Gebühr an, die über das kostenlose Kontingent hinausgeht. Die Verwendung eines vom Kunden verwalteten Schlüssels zählt zu Ihrem AWS KMS Kontingent. Weitere Informationen zur Preisgestaltung finden Sie unter AWS Key Management Service Preisgestaltung

EventBridge Scheduler verwendet IAM-Berechtigungen, die dem Prinzipal zugeordnet sind, der einen Zeitplan erstellt, um Ihre Daten zu verschlüsseln. Das bedeutet, dass Sie dem Benutzer oder der Rolle, die die Scheduler-API aufruft, die erforderlichen AWS KMS zugehörigen Berechtigungen zuweisen müssen. EventBridge Darüber hinaus verwendet EventBridge Scheduler ressourcenbasierte Richtlinien, um Ihre Daten zu entschlüsseln. Das bedeutet, dass die mit Ihrem Zeitplan verknüpfte Ausführungsrolle auch über die erforderlichen Berechtigungen verfügen muss, um die AWS KMS API beim AWS KMS Entschlüsseln von Daten aufrufen zu können.

> **Note**
>
> EventBridge Scheduler unterstützt nicht die Verwendung von Zuschüssen für temporäre Berechtigungen.

Im folgenden Abschnitt erfahren Sie, wie Sie Ihre AWS KMS Schlüsselrichtlinie und die erforderlichen IAM-Berechtigungen für die Verwendung eines vom Kunden verwalteten Schlüssels auf EventBridge Scheduler verwalten können.

Themen

- Fügen Sie IAM-Berechtigungen hinzu
- Verwalten Sie die Schlüsselrichtlinie

Fügen Sie IAM-Berechtigungen hinzu

Um einen vom Kunden verwalteten Schlüssel zu verwenden, müssen Sie dem identitätsbasierten IAM-Prinzipal, der einen Zeitplan erstellt, sowie der Ausführungsrolle, die Sie dem Zeitplan zuordnen, die folgenden Berechtigungen hinzufügen.

Identitätsbasierte Berechtigungen für vom Kunden verwaltete Schlüssel

Sie müssen der Berechtigungsrichtlinie, die jedem Prinzipal (Benutzer, Gruppen oder Rollen) zugeordnet ist, der bei der Erstellung eines EventBridge Zeitplans die Scheduler-API aufruft, die folgenden AWS KMS Aktionen hinzufügen.

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

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

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

- **`kms:DescribeKey`**— Erforderlich, um zu überprüfen, ob es sich bei dem von Ihnen angegebenen Schlüssel um einen KMS-Schlüssel mit symmetrischer Verschlüsselung handelt.
- **`kms:GenerateDataKey`**— Erforderlich, um den Datenschlüssel zu generieren, den EventBridge Scheduler für die clientseitige Verschlüsselung verwendet.
- **`kms:Decrypt`**— Erforderlich, um den verschlüsselten Datenschlüssel zu entschlüsseln, den EventBridge Scheduler zusammen mit Ihren verschlüsselten Daten speichert.

Berechtigungen zur Ausführung von Rollen für vom Kunden verwaltete Schlüssel

Sie müssen die folgende Aktion zur Berechtigungsrichtlinie für Ausführungsrollen Ihres Zeitplans hinzufügen, um Zugriff auf den EventBridge Scheduler zu gewähren, mit dem die AWS KMS API beim Entschlüsseln Ihrer Daten aufgerufen werden kann.

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

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

- **`kms:Decrypt`**— Erforderlich: Entschlüsseln Sie den verschlüsselten Datenschlüssel, den EventBridge Scheduler zusammen mit Ihren verschlüsselten Daten speichert.

Wenn Sie beim Erstellen eines neuen EventBridge Zeitplans die Scheduler-Konsole verwenden, um eine neue Ausführungsrolle zu erstellen, ordnet EventBridge Scheduler Ihrer Ausführungsrolle automatisch die erforderlichen Berechtigungen zu. Wenn Sie jedoch eine vorhandene Ausführungsrolle auswählen, müssen Sie der Rolle die erforderlichen Berechtigungen hinzufügen, um Ihre vom Kunden verwalteten Schlüssel verwenden zu können.

Verwalten Sie die Schlüsselrichtlinie

Wenn Sie einen vom Kunden verwalteten Schlüssel erstellen AWS KMS, verfügt Ihr Schlüssel standardmäßig über die folgende Schlüsselrichtlinie, um Zugriff auf die Ausführungsrollen Ihrer Zeitpläne zu gewähren.

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

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

Optional können Sie den Geltungsbereich Ihrer Schlüsselrichtlinie so einschränken, dass nur Zugriff auf die Ausführungsrolle gewährt wird. Sie können dies tun, wenn Sie Ihren vom Kunden verwalteten Schlüssel nur mit Ihren EventBridge Scheduler-Ressourcen verwenden möchten. Verwenden Sie das folgende Beispiel für eine wichtige Richtlinie, um einzuschränken, welche EventBridge Scheduler-Ressourcen Ihren Schlüssel verwenden können.

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

```
}
```

## CloudTrail Beispiel für ein Ereignis

AWS CloudTrail erfasst alle API-Aufruf-Ereignisse. Dies schließt API-Aufrufe ein, wenn EventBridge Scheduler Ihren vom Kunden verwalteten Schlüssel verwendet, um Ihre Daten zu entschlüsseln. Das folgende Beispiel zeigt einen CloudTrail Ereigniseintrag, der zeigt, dass EventBridge Scheduler die `kms:Decrypt` Aktion mithilfe eines vom Kunden verwalteten Schlüssels verwendet.

```
{
  "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"
  }
}
```

## Verschlüsselung während der Übertragung

EventBridge Scheduler verschlüsselt Ihre Daten bei der Übertragung durch das Netzwerk. Transport Layer Security (TLS) verschlüsselt Ihre Daten, wenn Sie EventBridge Scheduler-API-Operationen aufrufen, sowie wenn Scheduler beim Aufrufen Ihres EventBridge Zeitplans Ziel-APIs aufruft. Standardmäßig verwendet EventBridge Scheduler TLS 1.2 bei der Verschlüsselung Ihrer Daten während der Übertragung. Sie müssen die Verschlüsselung bei der Übertragung nicht konfigurieren, und Sie können keine andere TLS-Version wählen, wenn Sie Scheduler verwenden EventBridge .

Verwenden der EventBridge Scheduler-API — Wenn Sie beispielsweise eine API-Operation ausführen, verschlüsselt EventBridge Scheduler die gesamte HTTP-Anfrage`CreateSchedule`,

einschließlich des Hauptteils der Anfrage und der Header. EventBridge Scheduler verschlüsselt auch das gesamte Antwortobjekt, das Sie von unseren APIs erhalten.

Ziel-APIs verwenden — Wenn EventBridge Scheduler Ihren Zeitplan aufruft, ruft er die Ziel-API auf, die Sie bei der Erstellung des Zeitplans angegeben haben. Bei der Übermittlung eines Ereignisses an ein Ziel verschlüsselt EventBridge Scheduler die gesamte Anfrage, einschließlich des Anfragetexts und aller Header sowie der Antwort, die sie vom Ziel erhält.

# Konformitätsvalidierung für Amazon EventBridge Scheduler

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.

- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS-Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

## Resilienz in Amazon EventBridge Scheduler

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet EventBridge Scheduler mehrere Funktionen zur Unterstützung Ihrer Datenausfallsicherheit und Backup-Anforderungen.

# Infrastruktursicherheit in Amazon EventBridge Scheduler

Als verwalteter Service ist Amazon EventBridge Scheduler durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf EventBridge Scheduler zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

# Überwachung und Metriken für Amazon EventBridge Scheduler

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon EventBridge Scheduler und Ihrer anderenAWS -Lösungen aufrechtzuerhalten. AWSstellt die folgenden Überwachungstools bereit, um die EventBridge Scheduler zu überwachen, zu melden, wenn etwas nicht stimmt, und um gegebenenfalls automatische Aktionen durchzuführen:

- Amazon CloudWatch überwacht IhreAWS -Ressourcen und dieAWS in ausgeführten Anwendungen in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Weitere Informationen finden Sie im CloudWatch Benutzerhandbuch für Amazon.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.

Themen



# Überwachung von Amazon EventBridge Scheduler mit Amazon CloudWatch

Sie können Amazon EventBridge Scheduler mithilfe von Amazon Scheduler überwachen CloudWatch, der Rohdaten sammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. EventBridge Scheduler gibt einen Satz von Metriken für alle Zeitpläne und einen zusätzlichen Satz von Metriken für Zeitpläne aus, denen eine Dead-Letter-Warteschlange (DLQ) zugeordnet ist. Wenn Sie eine DLQ für Ihren Zeitplan konfigurieren, veröffentlicht EventBridge Scheduler zusätzliche Metriken, wenn Ihr Zeitplan die Wiederholungsrichtlinie erschöpft hat.

Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und einen besseren Überblick darüber erhalten, warum ein Zeitplan fehlschlägt, und die zugrunde liegenden Probleme beheben können. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Themen



## Bedingungen

Namespace

Ein Namespace ist ein Container für die CloudWatch Metriken eines AWS Dienstes. Für EventBridge Scheduler ist der Namespace. `AWS/Scheduler`

CloudWatch Metriken

Eine CloudWatch Metrik stellt einen nach der Zeit geordneten Satz von Datenpunkten dar, die spezifisch für sind. CloudWatch

Dimension

Eine Dimension ist ein Name-Wert-Paar, das zur Identifizierung einer Metrik beiträgt.

Einheit

Eine Statistik hat eine Maßeinheit. Bei EventBridge Scheduler beinhalten die Einheiten die Anzahl.

## Dimensionen

In diesem Abschnitt werden die CloudWatch Dimensionen beschrieben, in denen EventBridge Scheduler-Metriken gruppiert werden. CloudWatch

| Dimension | Beschreibung |
| --- | --- |
| ScheduleGroup | Die Gruppe von Zeitplänen, für die Sie Metriken anzeigen möchten. CloudWatch Wenn Sie noch keine Gruppen erstellt haben, ordnet EventBridge Scheduler Ihre Zeitpläne der `default` Gruppe zu. |

## Zugreifen auf -Metriken

In diesem Abschnitt wird beschrieben, wie Sie in CloudWatch einem bestimmten EventBridge Scheduler-Zeitplan auf Leistungskennzahlen zugreifen können.

So zeigen Sie Leistungsmetriken für eine Dimension an

1. Öffnen Sie die Seite „Metriken“ in der CloudWatch Konsole.
2. Verwenden Sie die AWS Regionsauswahl, um die Region für Ihren Zeitplan auszuwählen
3. Wählen Sie den Scheduler-Namespace.
4. Wählen Sie auf der Registerkarte Alle Metriken eine Dimension aus, zum Beispiel Schedule Group Metrics. Um Kennzahlen für alle Zeitpläne anzuzeigen, die Sie in der ausgewählten Region erstellt haben, wählen Sie Account Metrics aus.
5. Wählen Sie eine CloudWatch Metrik für eine Dimension aus. Wählen Sie zum Beispiel InvocationAttemptCount oder InvocationDroppedCount und wählen Sie dann Graphsuche aus.
6. Wählen Sie die Registerkarte Graphische Metriken, um Leistungsstatistiken für EventBridge Scheduler-Metriken anzuzeigen.

## Liste der Metriken

In den folgenden Tabellen sind die Metriken für alle EventBridge Scheduler-Zeitpläne sowie zusätzliche Metriken für Zeitpläne aufgeführt, für die Sie einen DLQ konfiguriert haben.

## Metriken für alle Zeitpläne

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| AWS/Scheduler | InvocationAttemptCount | Anzahl | Wird bei jedem Aufrufversuch ausgegeben. Verwenden Sie diese Metrik, um zu überprüfen, ob EventBridge Scheduler versucht, Ihre Zeitpläne aufzurufen, und um zu sehen, wann Aufrufe Ihre Kontokontingente erreichen. |
| AWS/Scheduler | TargetErrorCount | Anzahl | Wird ausgegeben, wenn das Ziel eine Ausnahme zurückgibt, nachdem EventBridge Scheduler die Ziel-API aufgerufen hat. Verwenden Sie diese Option, um zu überprüfen, ob die Lieferung an ein Ziel fehlschlägt. |
| AWS/Scheduler | TargetErrorThrottledCount | Anzahl | Wird ausgegeben, wenn der Zielaufruf aufgrund einer API-Drosselung durch das Ziel fehlschlägt. Verwenden Sie dies, um Zustellungsfehler |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| | | | zu diagnostizieren, wenn der Grund dafür die Drosselung von Aufrufen der Ziel-API durch Scheduler ist EventBridge |
| AWS/Scheduler | InvocationThrottleCount | Anzahl | Wird ausgelöst, wenn EventBridge Scheduler einen Zielaufruf drosselt, weil er Ihre von Scheduler festgelegten Dienstkontingente überschreitet. EventBridge Verwenden Sie dies, um festzustellen, wann Sie Ihre Scheduler-Kontingente überschritten haben. EventBridge Weitere Informationen zu Servicekontingenten finden Sie unterKontingente. |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| AWS/Scheduler | InvocationDroppedCount | Anzahl | Wird ausgelöst, wenn der EventBridge Scheduler den Versuch beendet, das Ziel aufzurufen, nachdem die Wiederholungsrichtlinie eines Zeitplans erschöpft ist. Weitere Informationen zu Wiederholungsrichtlinien finden Sie RetryPolicy in der Scheduler-API-Referenz. EventBridge |

## Metriken für Zeitpläne mit einem DLQ

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| AWS/Scheduler | InvocationsSentToDeadLetterCount | Anzahl | Wird für jede erfolgreiche Lieferung gemäß dem DLQ eines Zeitplans ausgegeben. Verwenden Sie diese Option, um festzustellen, wann Ereignisse an einen DLQ |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| | | | gesendet werden, und überprüfen Sie dann, ob das Ereignis an den DLQ des Zeitplans gesendet wurde, um weitere Informationen zu erhalten, anhand derer Sie die Ursache des Fehlers ermitteln können. |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| AWS/Scheduler | InvocationsFailedToBeSentToDeadLetterCount | Anzahl | Wird ausgegeben, wenn der EventBridge Scheduler ein Ereignis nicht an den DLQ übermitteln kann. Verwenden Sie diese beiden Metriken, um den Grund zu ermitteln, warum EventBridge Scheduler kein Ereignis an den DLQ senden kann, und ändern Sie Ihre DLQ-Konfiguration, um das Problem zu beheben.<br><br>Das Folgende ist ein Beispiel für die InvocationsFailedToBeSentTo |
| AWS/Scheduler | InvocationsFailedToBeSentToDeadLetterCount_<error_code> | Anzahl | |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| | | | `DeadLetterCount_<error_code>` Metrik, wenn die Amazon SQS SQS-Warteschlange, die Sie als DLQ angeben, nicht existiert: `InvocationsFailedToBeSentToDeadLetterCount_` **`AWS.SimpleQueueService.NonExistentQueue`** |

| Namespace | Metrik | Einheit | Beschreibung |
| --- | --- | --- | --- |
| AWS/Scheduler | InvocationsSentToDeadLetterCount_Truncated_MessageSizeExceeded | Anzahl | Wird ausgelöst, wenn die Nutzlast des an den DLQ gesendeten Ereignisses die von Amazon SQS zulässige Maximalgröße überschreitet und EventBridge Scheduler die von Ihnen im Attribut eines Zeitplans angegebene Nutzlast kürzt. Input |

## EventBridge Scheduler Nutzungsmetriken

CloudWatch sammelt Metriken, die die Nutzung einiger AWS Ressourcen verfolgen. Diese Metriken entsprechen AWS Servicekontingenten. Die Verfolgung dieser Metriken kann Ihnen dabei helfen, Ihre Kontingente proaktiv zu verwalten. Ermitteln Sie anhand der folgenden Messwerte, wann Sie Ihre EventBridge Scheduler-Kontingente überschritten haben. Weitere Informationen zu Servicekontingenten finden Sie unterKontingente.

Diese Messwerte sind nicht im AWS/Usage Namespace enthaltenAWS/Scheduler, sondern werden jede Minute erfasst.

Derzeit ist der einzige Metrikname in diesem Namespace, der CloudWatch veröffentlicht wird,. `CallCount` Diese Metrik wird mit den Dimensionen `Resource`, `Service`, und `Type` veröffentlicht. Die `Resource`-Dimension gibt den Namen der nachverfolgten API-Operation an.

Die `CallCount` Metrik mit den folgenden Dimensionen gibt beispielsweise an, wie oft der EventBridge Scheduler `CreateSchedule` API-Vorgang in Ihrem Konto aufgerufen wurde:

- „Service“: „Scheduler“
- „Typ“: „API“
- „Ressource“: "CreateSchedule“

Die `CallCount`-Metrik hat keine angegebene Einheit. Die nützlichste Statistik für die Metrik ist `SUM`, die die Gesamtanzahl der Operationen für den 1-Minuten-Zeitraum darstellt.

## Metriken

| Metrik | Beschreibung | | |
|---|---|---|---|
| `CallCount` | Die Anzahl der angegebenen Operationen, die in Ihrem Konto ausgeführt werden. | | |

## Dimensionen

| Dimension | Beschreibung | | |
|---|---|---|---|
| `Service` | Der Name des AWS Dienstes, der die Ressource enthält.<br><br>Für EventBridge Scheduler Nutzungsmetriken lautet der Wert für diese Dimension`Scheduler` . | | |
| `Class` | Die Klasse der nachverfolgten Ressource. | | |

| Dimension | Beschreibung | | |
|---|---|---|---|
| | EventBridge Scheduler API-Nutzungsmetriken verwenden diese Dimension mit einem Wert von `None`. | | |
| `Type` | Der Typ der nachverfolgten Ressource.<br><br>Wenn die `Service`-Dimension `Scheduler` ist, ist `API` der derzeit einzige gültige Wert für `Type`. | | |
| `Resource` | Der Name der API-Operation. Gültige Werte sind unter anderem:<br><br>• `CreateSchedule`<br>• `CreateScheduleGroup`<br>• `DeleteSchedule`<br>• `DeleteScheduleGroup`<br>• `GetSchedule`<br>• `GetScheduleGroup`<br>• `ListScheduleGroups`<br>• `ListSchedulesCallCount`<br>• `ListTagsForResource`<br>• `TagResource`<br>• `UntagResource`<br>• `UpdateSchedule` | | |

# Protokollieren von Amazon EventBridge Scheduler-API-Aufrufen mitAWS CloudTrail

Amazon EventBridge Scheduler ist in integriertAWS CloudTrail, einen Service integriert, der die Aktionen eines Benutzers, einer Rolle oder einesAWS -Services in EventBridge Scheduler

protokolliert. CloudTrail erfasst alle APIAufrufe für EventBridge Scheduler als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der EventBridge Scheduler-Konsole und Code-Aufrufe der EventBridge Scheduler-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignissen für EventBridge Scheduler, aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail Konsole trotzdem in Ereignisverlauf anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an EventBridge Scheduler gestellte Anfrage, die IP-Adresse, von der die Anforderung gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

## EventBridge Informationen zum Terminplaner in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität in EventBridge Scheduler auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen Ereignissen desAWS -Service in Ereignisverlauf protokolliert. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit CloudTrail Ereignisverlauf.

Erstellen Sie einen Trail zur laufenden Aufzeichnung der Ereignisse in IhremAWS-Konto -Konto, einschließlich Ereignissen für EventBridge Scheduler, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3 S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andereAWS -Services konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von von von von von von von von SNBenachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Konten und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle EventBridge Scheduler-Aktionen werden von der Amazon EventBridge Scheduler API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren

Aufrufe von`UpdateSchedule` und`DeleteSchedule` Aktionen Einträge in den CloudTrail Protokolldateien.`CreateSchedule`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

## Grundlagen zu EventBridge SchScheduler-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolldateien sind kein geordnetes Stack-Trace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

# Kontingente für Amazon EventBridge Scheduler

Ihr AWS Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jeden AWS Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen, andere können nicht erhöht werden.

Um die Kontingente für EventBridge Scheduler anzuzeigen, öffnen Sie die Service Quotas-Konsole . Wählen Sie im Navigationsbereich AWS Services und dann EventBridge Scheduler aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

> **Note**
>
> Die Kontingente für `CreateSchedule`, `UpdateScheduleGetSchedule`, und `DeleteSchedule` Transaktionen pro Sekunde (TPS) für EventBridge Scheduler sind auf bis zu Tausende von TPS anpassbar. Das Drosselungskontingent für Aufrufe ist auf Zehntausende von TPS anpassbar.

Ihr AWS Konto verfügt über die folgenden Kontingente im Zusammenhang mit EventBridge Scheduler.

| Name | Standard | Anpas | Beschreibung |
|---|---|---|---|
| CreateSchedule Anforderungsrate | Jede unterstützte Region: 50 | Ja | Maximale CreateSch edule Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBrid ge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| CreateScheduleGroup Anforderungsrate | Jede unterstützte Region: 10 | Yes (Ja) | Maximale CreateSch eduleGroup Anforderu |

| Name | Standard | Anpas | Beschreibung |
| --- | --- | --- | --- |
| | | | ngen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| DeleteSchedule Anforderungsrate | Jede unterstützte Region: 50 | Ja | Maximale DeleteSchedule Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| DeleteScheduleGroup Anforderungsrate | Jede unterstützte Region: 10 | Yes (Ja) | Maximale DeleteScheduleGroup Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |

| Name | Standard | Anpas | Beschreibung |
| --- | --- | --- | --- |
| GetSchedule Anforderungsrate | Jede unterstützte Region: 50 | Ja | Maximale GetSchedule Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| GetScheduleGroup Anforderungsrate | Jede unterstützte Region: 10 | Yes (Ja) | Maximale GetScheduleGroup Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| Drossel-Limit für Aufrufe in Transaktionen pro Sekunde | Jede unterstützte Region: 500 | Ja | Ein Aufruf ist eine geplante Nutzlast, die an das definierte Ziel übermittelt wird. Nachdem die Grenze erreicht ist, werden die Aufrufe gedrosselt, d. h. sie erfolgen weiterhin, aber verzögert. |

| Name | Standard | Anpas | Beschreibung |
| --- | --- | --- | --- |
| ListScheduleGroups Anforderungsrate | Jede unterstützte Region: 10 | Yes (Ja) | Maximale ListScheduleGroups Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| ListSchedules Anforderungsrate | Jede unterstützte Region: 50 | Ja | Maximale ListSchedules Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |
| ListTagsForResource Anforderungsrate | Jede unterstützte Region: 10 | Yes (Ja) | Listet die Tags auf, die der Planer-Ressource zugeordnet sind. |
| Anzahl der Zeitplangruppen | Jede unterstützte Region: 500 | Ja | Maximale Anzahl von Zeitplangruppen pro Region. |

| Name | Standard | Anpas | Beschreibung |
| --- | --- | --- | --- |
| Anzahl der Zeitpläne | Jede unterstützte Region: 1 000 000 | Ja | Die maximale Anzahl von Zeitplänen pro Region. Dieses Kontingent beinhaltet einmalige Zeitpläne, deren Ausführung abgeschlossen ist. Wir empfehlen, Ihre einmaligen Zeitpläne zu löschen, nachdem sie ausgeführt und ein Ziel aufgerufen haben. |
| TagResource Anforderungsrate | Jede unterstützte Region: 1 | Ja | Weist der angegebenen Planer-Ressource ein oder mehrere Tags (Schlüssel-Wert-Paare) zu. |
| UntagResource Anforderungsrate | Jede unterstützte Region: 1 | Ja | Entfernt ein oder mehrere Tags aus der angegebenen Planer-Ressource. |
| UpdateSchedule Anforderungsrate | Jede unterstützte Region: 50 | Ja | Maximale UpdateSchedule Anforderungen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. |

Weitere Informationen zu Kontingenten und Service-Endpunkten für EventBridge Scheduler finden Sie unter Amazon- EventBridge Scheduler-Endpunkte und -Kontingente im AWS Allgemeinen Referenzhandbuch.

# Dokumentation für diese Version von EventBridge Dokumentation für diese Version von Scheduler

Die folgende Tabelle beschreibt die Dokumentation für diese Version von EventBridge Scheduler.

| Änderung | Beschreibung | Datum |
| --- | --- | --- |
| Änderungen in der Exekutionsrolle und Verhinderung verwirrter Stellvertreter | In diesem Update werden Änderungen an der Art und Weise beschrieben, wie die Ausführungsrolle auf eine Zeitplangruppenressource angewendet wird, wenn Sie in der Berechtigungsrichtlinie der Rolle die Verhinderung verwirrter Stellvertreter implementieren.<br>• the section called “Confused-Deputy-Prävention” | 07. September 2023 |
| Automatisches Löschen von Zeitplänen nach Abschluss | EventBridge Der Scheduler unterstützt das automatische Löschen. Wenn Sie das automatische Löschen konfigurieren, EventBridge Der Scheduler löscht Ihren Zeitplan nach dem letzten geplanten Aufruf.<br>• the section called “Löschen nach Abschluss des Zeitplans” | 02. August 2023 |
| Das Thema zur Verwendung universeller Ziele wurde aktualisiert | Die Liste der unterstützten Dienste wurde aktualisiert, die EventBridge Scheduler | 17. März 2023 |

| | | |
|---|---|---|
| | kann gezielt eingesetzt und integriert werden. Das Update beschreibt die nicht von dieser Version von`GET`API-Operationen und beinhalte t Verbesserungen an den Universal Target-Beispielen sowie weitere kleinere Verbesserungen im gesamten Handbuch.<br>• the section called “Verwendung universeller Ziele” | |
| Die Informationen zu tarifbasi erten Flugplänen ohne Startdatum wurden aktualisiert | Die Dokumentation beschreib t das EventBridge Scheduler verarbeitet tarifbasierte Zeitpläne, wenn Sie keinen angeben`StartDate` .<br>• the section called “Ratenbas ierte Zeitpläne” | 17. März 2023 |

| | | |
|---|---|---|
| Neues Thema zur Verwaltung von Scheduler-Gruppen | Es wurde ein neues Kapitel zum Erstellen von Scheduler -Gruppen hinzugefügt mit EventBridge Scheduler. In diesem Kapitel erfahren Sie, wie Sie eine Gruppe erstellen, der Gruppe Zeitpläne hinzufügen und Tags anwenden, um Ihre Gruppe einfacher zu verwalten und zu überwachen EventBridge Scheduler-Ressourcen und schließlich das Löschen einer Gruppe.<br>• Verwaltung einer Zeitplang ruppe | 17. März 2023 |
| Neue Themen zur Sommerzeit und zu Zeitzonen | Es wurden neue Abschnitte hinzugefügt, die beschreib en, wie EventBridge Der Scheduler verwaltet die Sommerzeit und zeigt, wie Sie Zeitpläne in verschiedenen Zeitzonen erstellen können.<br>• the section called “Sommerzeit”<br>• the section called “Zeitzone n” | 17. November 2022 |

| | | |
|---|---|---|
| Neues Thema zu Metriken | Es wurde ein neues Thema hinzugefügt, das die Metriken beschreibt, die EventBridge Der Scheduler beschreibt für diese Version von CloudWatch. Mithilfe dieser Messwerte können Sie Fehlschläge bei Aufrufen überwachen und herausfinden, wie Sie Probleme mit Ihren Zeitplänen beheben können.<br>• the section called “Überwachung mit CloudWatch” | 15. November 2022 |
| Erstversion | Die erste Version von EventBridge Das Dokumentation für diese Version von Scheduler | 10. November 2022 |

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.