



Benutzerhandbuch

EventBridge Terminplaner



EventBridge Terminplaner: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist EventBridge Scheduler?	1
Die wichtigsten Funktionen von Scheduler EventBridge	1
Zugreifen auf Scheduler EventBridge	2
Einrichtung	3
Melden Sie sich an für AWS	3
Erstellen eines IAM-Benutzers	3
Verwenden Sie verwaltete Richtlinien	5
Einrichten der Ausführungsrolle	5
Richten Sie ein Ziel ein	9
Als nächstes	12
Erste Schritte	13
Voraussetzungen	14
Verwenden der Konsole	14
Mit dem AWS CLI	18
Mit dem SDKs	19
Als nächstes	20
Arten von Zeitplänen	21
Ratenbasierte Zeitpläne	22
Syntax	22
Beispiele	22
Cron-basierte Zeitpläne	23
Syntax	23
Beispiele	24
Einmalige Zeitpläne	25
Syntax	25
Beispiele	25
Zeitzone	26
Sommerzeit	26
Einen Zeitplan verwalten	28
Den Status des Zeitplans ändern	29
Konfiguration flexibler Zeitfenster	30
Konfiguration eines DLQ	31
Erstellen einer Amazon-SQS-Warteschlange	32
Richten Sie Berechtigungen für Ausführungsrollen ein	33

Geben Sie eine Warteschlange für unzustellbare Briefe an	34
Rufen Sie das Dead-Letter-Ereignis ab	35
Löschen eines Zeitplans	38
Löschen nach Abschluss des Zeitplans	38
Manuelles Löschen	39
Als nächstes	40
Verwaltung einer Zeitplangruppe	41
Eine Zeitplangruppe erstellen	42
Erster Schritt: Erstellen Sie eine neue Zeitplangruppe	42
Einen Zeitplan zuordnen	44
Löschen einer Zeitplangruppe	45
Zugehörige Ressourcen	47
Ziele verwalten	48
Verwenden von Zielen mit Vorlagen	49
Amazon SQS SendMessage	50
Lambda Invoke	52
Step Functions StartExecution	54
Verwenden von universellen Zielen	56
Nicht unterstützte Aktionen	56
Beispiele	57
Hinzufügen von Kontextattributen	59
Als nächstes	61
AWS PrivateLink	62
Überlegungen	62
Erstellen eines Schnittstellenendpunkts	62
Erstellen einer Endpunktrichtlinie	63
Sicherheit	65
Zugriffsverwaltung	66
Zielgruppe	66
Authentifizierung mit Identitäten	67
Verwalten des Zugriffs mit Richtlinien	71
Integration mit IAM	74
Verwenden identitätsbasierter Richtlinien	81
Confused-Deputy-Prävention	93
Fehlerbehebung	94
Datenschutz	96

Verschlüsselung im Ruhezustand	97
Verschlüsselung während der Übertragung	106
Compliance-Validierung	106
Ausfallsicherheit	108
Sicherheit der Infrastruktur	108
Überwachung und Metriken	110
Überwachung mit CloudWatch	110
Bedingungen	111
Dimensionen	111
Zugreifen auf -Metriken	112
Liste der Metriken	112
Nutzungsmetriken	119
Überwachung mit Protokollen CloudTrail	121
EventBridge Informationen zum Scheduler in CloudTrail	122
Grundlegendes zu EventBridge Scheduler-Protokolldateieinträgen	123
Kontingente	124
Fehlerbehebung bei Kontingenten	133
ServiceQuotaExceededException	134
Dokumentverlauf	136
.....	cxi

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. Mit dem hochgradig skalierbaren EventBridge Scheduler können Sie Millionen von Aufgaben planen, die mehr als 270 AWS Dienste und über 6.000 API-Operationen aufrufen können. Ohne Infrastruktur bereitstellen und verwalten oder mehrere Dienste integrieren zu müssen, bietet Ihnen EventBridge Scheduler die Möglichkeit, Zeitpläne in großem Umfang bereitzustellen und die Wartungskosten zu senken.

EventBridge Scheduler erledigt Ihre Aufgaben zuverlässig und verfügt über integrierte Mechanismen, die Ihre Zeitpläne an die Verfügbarkeit nachgelagerter 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

- [Die wichtigsten Funktionen von Scheduler EventBridge](#)
- [Zugreifen auf Scheduler EventBridge](#)

Die wichtigsten Funktionen von Scheduler EventBridge

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

- **Vorlagenziele** — EventBridge Scheduler unterstützt vordefinierte Ziele zur Ausführung gängiger API-Operationen mit Amazon SQS, Amazon SNS, Lambda und EventBridge. Mit vordefinierten Zielen können Sie Ihre Zeitpläne schnell mit der EventBridge Scheduler-Konsole, dem Scheduler-SDK oder dem konfigurieren. EventBridge AWS CLI
- **Universelle Ziele** — EventBridge Scheduler bietet einen Universal Target Parameter (UTP), mit dem Sie benutzerdefinierte Trigger erstellen können, die auf mehr als 270 AWS Dienste und über 6.000 API-Operationen nach einem Zeitplan abzielen. Mit UTP können Sie Ihre benutzerdefinierten Trigger mithilfe der EventBridge Scheduler-Konsole, dem Scheduler-SDK oder dem EventBridge konfigurieren. AWS CLI

- **Flexible Zeitfenster** — EventBridge Der Scheduler unterstützt flexible Zeitfenster, sodass Sie Ihre Zeitpläne verteilen und die Zuverlässigkeit Ihrer Trigger für Anwendungsfälle verbessern können, die keinen präzisen geplanten Aufruf von Zielen erfordern.
- **Wiederholungen** — EventBridge Der Scheduler ermöglicht die Übermittlung von at-least-once Ereignissen an Ziele, d. h., dass mindestens eine Übertragung erfolgreich ist und das Ziel darauf reagiert. EventBridge Mit dem Scheduler können Sie die Anzahl der Wiederholungen für Ihren Zeitplan für eine fehlgeschlagene Aufgabe festlegen. EventBridge Der Scheduler wiederholt fehlgeschlagene Aufgaben mit verzögerter Verzögerung, um die Zuverlässigkeit Ihres Zeitplans zu erhöhen und sicherzustellen, dass Ziele verfügbar sind.

Zugreifen auf Scheduler EventBridge

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

Amazon EventBridge Scheduler einrichten

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

Themen

- [Melden Sie sich an für AWS](#)
- [Erstellen eines IAM-Benutzers](#)
- [Verwenden Sie verwaltete Richtlinien](#)
- [Einrichten der Ausführungsrolle](#)
- [Richten Sie ein Ziel ein](#)
- [Als nächstes](#)

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/die-Anmeldung>.
2. Folgen Sie den Online-Anweisungen.

Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscode auf der Telefontastatur.

Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

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 (Empfohlen)	<p>Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS.</p> <p>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.</p>	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center - Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff, indem Sie AWS CLI die Konfiguration für die Verwendung AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch vornehmen.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Folgen Sie den Anweisungen unter Erstellen eines IAM-Benutzers für den Notfallzugriff im IAM-Benutzerhandbuch.	Konfigurieren Sie den programmatischen Zugriff unter Zugriffsschlüssel für IAM-Benutzer verwalten im IAM-Benutzerhandbuch .

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 beliebige Ziele mit Vorlagen beschrieben. Informationen zum Hinzufügen von Berechtigungen für andere Ziele finden Sie unter [the section called “Verwenden von Zielen mit Vorlagen”](#).

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 unklaren Stellvertretern zu vermeiden. Weitere Informationen und ein Beispiel für eine Richtlinie finden Sie unter [the 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"
    }
  ]
}
```

- 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": "2022-03-01T19:31:18.620Z",
    "AttachmentCount": 0,
    "IsAttachable": true,
    "PolicyId": "ZXR6A36LTYANPAI7NJ5UV",
    "DefaultVersionId": "v1",
    "Path": "/",
    "Arn": "arn:aws:iam::123456789012:policy/PolicyName",
    "UpdateDate": "2022-03-01T19:31:18.620Z"
  }
}
```

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 EventBridge Scheduler-Zeitplans beschrieben. 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 konfigurieren AWS CLI.

```
$ aws configure
```

```
AWS Access Key ID [None]: AKIAIOSFODNN7EXAMPLE
```

```
AWS Secret Access Key [None]: wJa1rXUtnFEMI/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 Interface Benutzerhandbuch für Version 2.

Themen

- [Voraussetzungen](#)
- [Erstellen Sie mit der EventBridge Scheduler-Konsole einen Zeitplan](#)
- [Erstellen Sie einen Zeitplan mit dem AWS CLI](#)
- [Erstellen Sie mit dem Scheduler einen Zeitplan EventBridge SDKs](#)
- [Als nächstes](#)

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

So erstellen Sie einen neuen Zeitplan mithilfe der Konsole

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

Note

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

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. 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 einen Cron-basierten Zeitplan, um einen Zeitplan mithilfe eines Ausdrucks zu konfigurieren. cron Um einen Preisausdruck 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. 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.
 7. Auf der Seite Ziel auswählen gehen Sie wie folgt vor:
 - a. Wählen Sie Ziele mit Vorlagen und wählen Sie eine Ziel-API aus. Für dieses Beispiel wählen wir das Amazon SQS **SendMessage** SQS-Vorlagenziel.
 - 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 mit dem Schalter 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 unter [the 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, die der EventBridge Scheduler für 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 Dropdown-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 Rollename 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.
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, 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 dem Scheduler einen Zeitplan EventBridge SDKs

Im folgenden Beispiel verwenden Sie den 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 unter [Einen Zeitplan verwalten](#). 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 bedeutet, dass, wenn Sie Ihren Zeitplan so einrichten `1:00`, dass er die Ziel-API zwischen `1:00:00` und `1:00:59` aufruft, vorausgesetzt, dass kein flexibles Zeitfenster festgelegt ist.

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](#)
- [Cron-basierte Zeitpläne](#)
- [Einmalige Zeitpläne](#)
- [EventBridge Zeitzonen im Scheduler](#)
- [EventBridge Sommerzeit im Scheduler](#)

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	, - * /
Day-of-month	1-31	, - * ? / L W
Monat	1-12 oder JAN-DEC	, - * /
Day-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 Day-of-week Feldern als Day-of-month auch 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 Day-of-month Feld könnten Sie 7 eingeben und wenn ein beliebiger Wochentag zulässig ist, könnten Sie eingeben? auf dem Day-of-week Feld.
- Das Platzhalterzeichen L in den Feldern für Day-of-month oder Day-of-week gibt den letzten Tag des Monats oder der Woche an.
- Der W Platzhalter in dem Day-of-month Feld gibt einen Wochentag an. **3W**Gibt in dem Day-of-month Feld den Wochentag an, der dem dritten Tag des Monats am nächsten liegt.
- Der Platzhalter # in dem Day-of-week Feld 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. 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 im EventBridge Scheduler

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 Scheduler unterstützt drei Arten von Zeitplänen: Tarif-, Cron- 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 unter [the section called “Konfiguration eines DLQ”](#).

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

Themen

- [Den Status des Zeitplans im Scheduler ändern EventBridge](#)
- [Konfiguration flexibler Zeitfenster im EventBridge Scheduler](#)
- [Konfiguration der Warteschlange für unzustellbare Briefe eines Zeitplans im Scheduler EventBridge](#)
- [Löschen eines Zeitplans im EventBridge Scheduler](#)
- [Als nächstes](#)

Den Status des Zeitplans im Scheduler ändern EventBridge

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 im EventBridge Scheduler

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 `anOFF`. Wenn Sie den Wert auf `setzenFLEXIBLE`, 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)
```

Konfiguration der Warteschlange für unzustellbare Briefe eines Zeitplans im Scheduler EventBridge

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

Im folgenden Thema wird diese JSON-Datei als Ereignis bezeichnet, bei dem es sich um ein Ereignis handelt, das nicht mehr aktuell ist. Mit einem Ereignis mit unerlaubtem Text können Sie Probleme mit Ihrem Zeitplan oder Ihren Zielen beheben. Wenn Sie eine Wiederholungsrichtlinie für Ihren Zeitplan konfigurieren, übermittelt EventBridge Scheduler das Ereignis, bei dem die von Ihnen festgelegte Höchstzahl an Wiederholungen ausgeschöpft ist.

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 Zustellung von Nachrichten an Amazon SQS benötigt, und wie Sie Dead-Letter-Ereignisse von der DLQ empfangen können.

Themen

- [Erstellen einer Amazon-SQS-Warteschlange](#)
- [Richten Sie Berechtigungen für Ausführungsrollen ein](#)
- [Geben Sie eine Warteschlange für unzustellbare Briefe an](#)
- [Rufen Sie das Dead-Letter-Ereignis ab](#)

Erstellen einer Amazon-SQS-Warteschlange

Bevor Sie eine DLQ für Ihren Zeitplan konfigurieren, müssen Sie eine Amazon SQS SQS-Standardwarteschlange erstellen. Anweisungen zum Erstellen einer Warteschlange mit der Amazon SQS SQS-Konsole finden Sie unter [Erstellen einer Amazon SQS SQS-Warteschlange](#) im Amazon Simple Queue Service Developer Guide.

Note

EventBridge Scheduler unterstützt nicht die Verwendung einer FIFO-Warteschlange als DLQ Ihres Zeitplans.

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

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

Wenn dies erfolgreich ist, werden Sie das QueueURL in der Ausgabe sehen.

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

Nachdem Sie die Warteschlange erstellt haben, notieren Sie sich den Warteschlangen-ARN. Sie benötigen den ARN, wenn Sie eine DLQ für Ihren EventBridge Scheduler-Zeitplan angeben. Sie finden Ihren Warteschlangen-ARN in der Amazon SQS SQS-Konsole oder mithilfe des [get-queue-attributes](#) AWS CLI Befehls.

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

Bei Erfolg sehen Sie den Warteschlangen-ARN in der Ausgabe.

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

Im nächsten Abschnitt fügen Sie Ihrer Rolle für die Ausführung von Zeitplänen die erforderlichen Berechtigungen hinzu, damit EventBridge Scheduler unvollständige Ereignisse an Amazon SQS übermitteln kann.

Richten Sie Berechtigungen für Ausführungsrollen ein

Damit EventBridge Scheduler unbemerkte Ereignisse an Amazon SQS übermitteln kann, benötigt Ihre Rolle zur Ausführung von Zeitplänen die folgende Berechtigungsrichtlinie. Weitere Informationen zum Hinzufügen einer neuen Berechtigungsrichtlinie zu Ihrer Rolle für die Ausführung von Zeitplänen finden Sie unter Ausführungsrolle [einrichten](#).

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

Note

Ihrer Rolle für die Ausführung von Zeitplänen sind möglicherweise bereits die erforderlichen Berechtigungen zugewiesen, 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 unzustellbare Briefe 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

Um einen DLQ mit der Konsole anzugeben

1. [Melden Sie sich bei der an und wählen Sie dann den folgenden Link AWS Management Console, um den EventBridge Scheduler-Bereich der EventBridge Konsole zu öffnen: Home https://console.aws.amazon.com/scheduler/](https://console.aws.amazon.com/scheduler/)
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 Warteschlange mit unerlaubtem Schreiben (DLQ) einen der folgenden Schritte aus:
 - Wählen Sie Wählen Sie eine Amazon SQS SQS-Warteschlange in meinem AWS Konto als DLQ aus und wählen Sie dann den Warteschlangen-ARN für Ihre DLQ aus der Drop-down-Liste aus.
 - Wählen Sie Geben Sie eine Amazon SQS SQS-Warteschlange in anderen AWS Konten als DLQ an und geben Sie dann den Warteschlangen-ARN für Ihre DLQ ein. Wenn Sie eine Warteschlange in einem anderen AWS Konto auswählen, kann die EventBridge Scheduler-Konsole die Warteschlange nicht ARNs in einer Dropdownliste anzeigen.
4. Überprüfen Sie Ihre Auswahl und wählen Sie dann Zeitplan erstellen oder Zeitplan speichern, um die Konfiguration einer DLQ abzuschließen.
5. (Optional) Um die DLQ-Details eines Zeitplans anzuzeigen, wählen Sie den Namen des Zeitplans aus der Liste aus und klicken Sie dann auf der Detailseite des Zeitplans auf die Registerkarte Warteschlange mit unbestätigten Nachrichten.

AWS CLI

Um einen vorhandenen Zeitplan mit dem zu aktualisieren AWS 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 den ARN der IAM-Rolle, dem 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 den AWS 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 den, AWS CLI um ein Ereignis mit unerlaubtem Brief vom DLQ zu empfangen.

Rufen Sie das Dead-Letter-Ereignis ab

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

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

Bei Erfolg erhalten Sie eine Ausgabe, die der folgenden ähnelt.

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

```

"ReceiptHandle": "AQEBkNKTD0MrWgHKPoITRBwrPoK3eCSZICzWvqCY0BZ
+FfTcORFpopJbtCqj36VbBTLHreM8+qM/m5jcwqSlAlGmIJ0/hYmMgn/
+dwIty9izE7HnpvRhhEyHxbeTZ5V05RbeasYaBdNyi9WLcnAHviDh6MebLXXNWoFyYNSxdwJuG0f/
w3htX6r3dXPxvVFNpGoQb8ihY37+u0gtsbuIwhLtUSmE8rbldEEwiUfi3IJ1zEZpUS77n/k1GWrMrnYg0Gx/
BuaLz0rFi2F738XI/
Hnh45uv3ca60YwS1ojPQ1LtX2URg1haV5884FYlaRvY8jRlpCZabTkYRTZKSXG5KNGyZnHpmsspii6JNkjitYVFKPo0H91w
"MD5OfBody": "07adc3fc889d6107d8bb8fda42fe0573",
"Body": "{\"MessageBody\": \"Hello, world!\", \"QueueUrl\": \"https://sqs.us-
west-2.amazonaws.com/123456789012/does-not-exist\"}",
"Attributes": {
  "SenderId": "AROAZDZE3W4CTL5ZR7EIN: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"
    }
}
]
}

```

Notieren Sie sich die folgenden Attribute im Dead-Letter-Ereignis, um mögliche Gründe für das Fehlschlagen des Zielaufrufs zu identifizieren und zu beheben.

- **ERROR_CODE**— Enthält den Fehlercode, den EventBridge Scheduler von der Service-API des Ziels erhält. Im vorherigen Beispiel lautet `AWS.SimpleQueueService.NonExistentQueue` der von Amazon SQS zurückgegebene Fehlercode. Wenn der Zeitplan ein Ziel aufgrund eines Problems mit dem EventBridge Scheduler nicht aufrufen kann, 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 `The specified queue does not exist for this wsd1 version` die von Amazon SQS zurückgegebene Fehlermeldung. 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 Dienst-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 Fehler handelt, der wiederholt werden kann, und nicht um einen dauerhaften Fehler. Das Attribut kann die Werte `MaximumRetryAttempts` wenn der EventBridge Scheduler es an die DLQ gesendet hat, nachdem es die maximale Anzahl an Wiederholungsversuchen überschritten hat, die Sie für den Zeitplan konfiguriert haben `MaximumEventAgeInSeconds`, oder wenn das Ereignis älter als das im Zeitplan festgelegte 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 im EventBridge Scheduler

Sie können einen Zeitplan löschen, indem Sie entweder das automatische Löschen konfigurieren oder indem Sie 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](#)
- [Manuelles Löschen](#)

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 `endDate` angeben, 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 im EventBridge Scheduler

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 erstellen AWS-Konto. Mit EventBridge Scheduler organisieren Sie Zeitplangruppen anstelle einzelner Zeitpläne, 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, auch für die 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 werden der Gruppe auch einen Zeitplan zuordnen. Schließlich löschen Sie die Gruppe.

Themen

- [Eine Zeitplangruppe im EventBridge Scheduler erstellen](#)
- [Löschen einer Zeitplangruppe im EventBridge Scheduler](#)

- [Zugehörige Ressourcen](#)

Eine Zeitplangruppe im EventBridge Scheduler 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. Beispiel, **TestGroup**.
5. Gehen Sie im Abschnitt Tags wie folgt vor:
 - a. Wählen Sie 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 unter [Erste 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) `aws-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 EventBridge Scheduler

Im Folgenden erfahren Sie, wie Sie eine Zeitplangruppe mit dem AWS Management Console und dem löschen AWS Command Line Interface. 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 Gruppe AWS-Region, die Sie löschen möchten. Wenn Sie die Gruppe, nach der Sie suchen, nicht sehen, wählen Sie eine andere aus AWS-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 bleibt 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:

- [CreateScheduleGroup](#) Vorgang in der EventBridge Scheduler-API-Referenz.
- [DeleteScheduleGroup](#) Vorgang in der EventBridge Scheduler-API-Referenz.

Ziele im EventBridge Scheduler verwalten

In den folgenden Themen wird beschrieben, wie Vorlagen und universelle Ziele mit EventBridge Scheduler verwendet werden. Außerdem finden Sie eine Liste der unterstützten AWS Dienste, die Sie mit dem universellen Zielparameter von EventBridge Scheduler konfigurieren können.

Bei Zielvorlagen handelt es sich um eine Reihe gängiger API-Operationen für eine Gruppe von AWS Kerndiensten wie Amazon SQS, Lambda und Step Functions. Sie können beispielsweise den API-Vorgang „[Invoke](#) API“ von Lambda als Ziel festlegen, indem Sie die Funktion ARN angeben, oder den [SendMessage](#)Vorgang von Amazon SQS mit dem Warteschlangen-ARN des Ziels.

Das universelle Ziel ist ein anpassbarer Satz von Parametern, mit dem Sie für viele Dienste einen breiteren Satz von API-Vorgängen aufrufen können. AWS Sie können beispielsweise den Universal Target Parameter (UTP) von EventBridge Scheduler verwenden, um mithilfe des Vorgangs eine neue Amazon SQS SQS-Warteschlange zu erstellen. [CreateQueue](#)

Um entweder vordefinierte oder universelle Ziele zu konfigurieren, muss Ihr Zeitplan über die Berechtigung verfügen, den API-Vorgang aufzurufen, den Sie als Ziel konfigurieren. Dazu fügen Sie der Ausführungsrolle Ihres Zeitplans die erforderlichen Berechtigungen hinzu. Um beispielsweise auf den [SendMessage](#)Betrieb von Amazon SQS abzielen, wird der Ausführungsrolle die Erlaubnis erteilt, die `sqs:SendMessage` Aktion auszuführen. In den meisten Fällen können Sie die erforderlichen Berechtigungen mithilfe der [AWS verwalteten Richtlinien](#) hinzufügen, die der Zielservice 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. Die folgenden Themen zeigen Beispiele für das Hinzufügen von Berechtigungen sowohl für vordefinierte als auch für universelle Zieltypen.

Weitere Informationen zum Einrichten einer Ausführungsrolle für einen Zeitplan finden Sie unter [the section called “Einrichten der Ausführungsrolle”](#).

Themen

- [Verwenden von Zielvorlagen im Scheduler EventBridge](#)
- [Verwenden von universellen Zielen im EventBridge Scheduler](#)
- [Hinzufügen von Kontextattributen im EventBridge Scheduler](#)
- [Als nächstes](#)

Verwenden von Zielvorlagen im Scheduler EventBridge

Bei Zielvorlagen handelt es sich um eine Reihe gängiger API-Operationen für eine Gruppe von AWS Kerndiensten wie Amazon SQS, Lambda und Step Functions. Sie können beispielsweise den [Invoke](#) Betrieb von Lambda als Ziel festlegen, indem Sie die Funktion ARN bereitstellen, oder den [SendMessage](#) Vorgang von Amazon SQS mithilfe des Warteschlangen-ARN. Um ein Ziel mit einer Vorlage zu konfigurieren, müssen Sie außerdem der Ausführungsrolle des Zeitplans Berechtigungen für die Ausführung des geplanten API-Vorgangs erteilen.

Um ein vorgegebenes Ziel programmatisch mit dem AWS CLI oder einem der EventBridge Scheduler zu konfigurieren SDKs, müssen Sie den ARN der Ausführungsrolle, den ARN für die Zielressource, eine optionale Eingabe, die EventBridge Scheduler an das Ziel liefern soll, und für einige vorlagenbasierte Ziele einen eindeutigen Satz von Parametern mit zusätzlichen Konfigurationsoptionen für dieses Ziel angeben. Wenn Sie den ARN für eine Zielressource mit Vorlagen angeben, geht EventBridge Scheduler automatisch davon aus, dass Sie den unterstützten API-Vorgang für diesen Dienst aufrufen möchten. [Wenn Sie möchten, dass EventBridge Scheduler auf einen anderen API-Vorgang für den Dienst abzielt, müssen Sie das Ziel als universelles Ziel konfigurieren.](#)

Im Folgenden finden Sie eine vollständige Liste aller von EventBridge Scheduler unterstützten Vorlagenziele und, falls zutreffend, der eindeutigen zugehörigen Parameter für jedes Ziel. Wählen Sie den Link für jeden Parametersatz, um die erforderlichen und optionalen Felder in der EventBridge Scheduler-API-Referenz zu sehen.

- 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 KI — [StartPipelineExecution](#)
 - Parameter: [SageMakerPipelineParameters](#)
- Amazon SNS — [Publish](#)
- Amazon SQS – [SendMessage](#)
 - Parameter: [SqsParameters](#)
- Step Functions — [StartExecution](#)

Anhand der folgenden Beispiele erfahren Sie, wie Sie verschiedene Ziele mit Vorlagen konfigurieren und welche IAM-Berechtigungen für jedes der beschriebenen Ziele erforderlich sind.

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");
    }
}

```

Step Functions **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");
    }
}
```

Verwenden von universellen Zielen im EventBridge Scheduler

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

Um mit dem oder einem der AWS CLI EventBridge Scheduler ein universelles Ziel für Ihren Zeitplan zu konfigurieren SDKs, 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
invokeModel
```

Der Dienst-ARN für die [GetQueueUrl](#) API-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 `list` beginnt.

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 Lambda API-Referenz](#) aufgeführten Parameter festlegen. Dazu gehört die optionale [JSON-Nutzlast](#), die Sie an eine Lambda-Funktion übergeben können.

Informationen zur Bestimmung der Parameter, die Sie für verschiedene festlegen können APIs, finden Sie in der API-Referenz für diesen Dienst. Ähnlich wie bei Lambda `Invoke` APIs akzeptieren einige URI-Parameter sowie eine Nutzlast des Anforderungstexts. 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 im EventBridge Scheduler

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-Vorgängen finden Sie unter [EventBridge Scheduler-API-Referenz](#).

Greifen Sie über einen Schnittstellenendpunkt auf Amazon EventBridge Scheduler zu ()AWS PrivateLink

Sie können AWS PrivateLink verwenden, um eine private Verbindung zwischen Ihrer VPC und Amazon EventBridge Scheduler herzustellen. Sie können auf EventBridge Scheduler zugreifen, als wäre er in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf EventBridge Scheduler zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für den Scheduler bestimmt ist. EventBridge

Weitere Informationen finden Sie im Handbuch unter [Access AWS-Services through AWS PrivateLink](#).AWS PrivateLink

Überlegungen zum EventBridge Scheduler

Bevor Sie einen Schnittstellenendpunkt für EventBridge Scheduler einrichten, lesen Sie die [Überlegungen](#) im AWS PrivateLink Handbuch durch.

EventBridge Scheduler unterstützt Aufrufe all seiner API-Aktionen über den Schnittstellenendpunkt.

Erstellen Sie einen Schnittstellenendpunkt für Scheduler EventBridge

Sie können einen Schnittstellenendpunkt für EventBridge Scheduler entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter [Erstellen eines Schnittstellenendpunkts](#) im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für EventBridge Scheduler mit dem folgenden Servicenamen:

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

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an EventBridge Scheduler stellen, indem Sie dessen standardmäßigen regionalen DNS-Namen verwenden. Beispiel, `scheduler.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff auf EventBridge Scheduler über den Schnittstellenendpunkt. Um den Zugriff auf EventBridge Scheduler von Ihrer VPC aus zu steuern, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Services mit Endpunktrichtlinien](#) im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für EventBridge Scheduler-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten EventBridge Scheduler-Aktionen.

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

```
}  
  ]  
}
```

Sicherheit in Amazon EventBridge Scheduler

Cloud-Sicherheit AWS hat 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](#)
- [Datenschutz in Amazon EventBridge Scheduler](#)
- [Konformitätsprüfung für Amazon EventBridge Scheduler](#)
- [Resilienz in Amazon EventBridge Scheduler](#)
- [Infrastruktursicherheit in Amazon EventBridge Scheduler](#)

Zugriff auf Amazon EventBridge Scheduler verwalten

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. 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](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert EventBridge Scheduler mit IAM](#)
- [Verwenden von identitätsbasierten Richtlinien im Scheduler EventBridge](#)
- [Verhinderung verwirrter Stellvertreter im Scheduler EventBridge](#)
- [Fehlerbehebung bei Identität und Zugriff auf Amazon EventBridge Scheduler](#)

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 Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern 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. Anschließend müssen Sie Anforderungen an Ihren IAM-

Administrator senden, um die Berechtigungen der Servicebenutzer 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 von identitätsbasierten Richtlinien im Scheduler EventBridge](#)

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 Zugangsportale 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 für die Selbstsignierung von Anforderungen finden Sie unter [AWS Signature Version 4 für API-Anforderungen](#) im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. 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 [AWS Multi-Faktor-Authentifizierung \(MFA\) in IAM](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, 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. Sie können darauf zugreifen, 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. Verwenden Sie diese nur, 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 eine Gruppe benennen IAMAdmins und dieser Gruppe Berechtigungen zur Verwaltung 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 [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb von Ihrem AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie [von einer Benutzer- zu einer IAM-Rolle \(Konsole\) 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 [Methoden für die Übernahme einer Rolle](#) 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 \(Verbund\)](#) 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 zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von

Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt](#) werden.

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. Die Berechtigungen in den Richtlinien legen fest, ob eine 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 auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 Inline-Richtlinie wählen, finden Sie unter [Auswählen 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.

Zugriffskontrolllisten (ACLs)

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

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.
- **Dienststeuerungsrichtlinien (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 alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter [Richtlinien zur Servicesteuerung](#) im AWS Organizations Benutzerhandbuch.
- **Ressourcenkontrollrichtlinien (RCPs)** — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter [Resource Control Policies \(RCPs\)](#) 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 mit Scheduler verwendet werden können. 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 (servicespezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Prinzipalberechtigungen	Ja
Servicerollen	Ja

IAM-Feature	EventBridge Scheduler-Unterstützung
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 [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 von identitätsbasierten Richtlinien im Scheduler EventBridge](#)

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 Prinzipalentsität (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 [Kontoübergreifender 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 Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Eigenschaften 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 von identitätsbasierten Richtlinien im Scheduler EventBridge](#)

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 von identitätsbasierten Richtlinien im Scheduler EventBridge](#)

ACLs EventBridge im Scheduler

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten 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 Bedingungelement 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 [Definieren von Berechtigungen mit ABAC-Autorisierung](#) 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 von einer Benutzerrolle zu einer IAM-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: Ja

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 von identitätsbasierten Richtlinien im Scheduler EventBridge

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Scheduler-Ressourcen zu erstellen oder zu ändern. EventBridge 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 \(Konsole\)](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von EventBridge Scheduler definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EventBridge Scheduler](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)
- [EventBridge Scheduler-Berechtigungen](#)
- [AWS verwaltete Richtlinien für EventBridge Scheduler](#)
- [Vom Kunden verwaltete Richtlinien für Scheduler EventBridge](#)
- [AWS verwaltete Richtlinienaktualisierungen](#)

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 AWS-Konto verursachen. 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 AWS-Konto verfügbar. 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 [Richtlinienvvalidierung mit 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 [Sicherer API-Zugriff mit MFA](#) 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 Schlüssel](#) vom [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 “AmazonEventBridgeSchedulerReadOnlyAccess” — Neue verwaltete Richtlinie	EventBridge Scheduler bietet Unterstützung für eine neue verwaltete Richtlinie, die Benutzern schreibgeschützten Zugriff auf alle Ressourcen, einschließlich Zeitpläne und Zeitplangruppen, gewährt.	10. November 2022
EventBridge Scheduler hat mit der Nachverfolgung von Änderungen begonnen	EventBridge Scheduler hat damit begonnen, Änderungen für seine AWS verwalteten Richtlinien zu verfolgen.	10. November 2022

Verhinderung verwirrter Stellvertreter im Scheduler EventBridge

Das Problem des verwirrten Stellvertreters ist ein Sicherheitsproblem, bei dem eine Entität, die keine Berechtigung zur Durchführung einer Aktion hat, eine privilegiere Entität zur Durchführung der Aktion zwingen kann. In AWS kann ein dienstübergreifendes Identitätswechsels zu einem Problem mit verwirrtem Stellvertreter 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 unbekannt Teile des ARN. 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

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

Themen

- [Ich bin nicht berechtigt, eine Aktion im Scheduler auszuführen EventBridge](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine EventBridge Scheduler-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, 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 auszuführen: 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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, 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 unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

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 die AWS Cloud gesamte Infrastruktur läuft. 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 zu schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS, um mit AWS-Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit einem AWS CloudTrail. Informationen zur Verwendung von CloudTrail-Pfaden zur Erfassung von AWS-Aktivitäten finden Sie unter [Arbeiten mit CloudTrail-Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- 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 auf AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

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 verwenden. AWS CLI AWS SDKs 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.

Verschlüsselung im Ruhezustand im Scheduler EventBridge

In diesem Abschnitt wird beschrieben, wie Amazon EventBridge Scheduler Ihre Daten im Ruhezustand verschlüsselt 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 für die Verwendung in mehreren AWS Konten verwaltet. 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 gezahlt. 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](#)
- [KMS-Schlüssel verwalten](#)
- [CloudTrail Beispiel für ein Ereignis](#)

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 verwaltet er Schlüssel
Nutzlast (bis zu 256 KB)	Die Daten, die Sie im <code>TargetInput</code> 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 Planungs Ausdruck, z. B. der Rate- oder Cron-Ausdruck für wiederkehrende Zeitpläne, der Zeitstempel für einmalige Aufrufe sowie das Startdatum, das Enddatum und die Zeitzone des Zeitplans.	Unterstützt	Nicht unterstützt
Zielkonfiguration	Der Amazon-Ressourcenname (ARN) des Ziels und	Unterstützt	Nicht unterstützt

Datentyp	Beschreibung	AWS-eigener Schlüssel	vom Kunden verwalteter Schlüssel
	andere zielbezogene Konfigurationsdetails.		
Konfiguration des Aufrufs- und Fehlerverhaltens	Flexible Zeitfensterkonfiguration, die Wiederholungsrichtung 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": "ABCDEFGH11JKLMNOP2Q3",
"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 bei der Übertragung im Scheduler EventBridge

EventBridge Scheduler verschlüsselt Ihre Daten während 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 ein 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 unserem erhalten. APIs

Target verwenden APIs — 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.

Konformitätsprüfung 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 heruntergeladenen AWS Artifact. Weitere Informationen finden Sie unter [Berichte heruntergeladen 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:

- [Compliance und Governance im Bereich Sicherheit](#) – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- [Referenz für berechnete HIPAA-Services](#) – Listet berechnete HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- [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](#) — Auf diese AWS-Service Weise erhalten Sie 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. Die Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerreferenz](#).
- [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 auf AWS-Regionen 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

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von Amazon EventBridge Scheduler und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um EventBridge Scheduler zu überwachen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen 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 Amazon-Benutzerhandbuch](#).
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im [AWS CloudTrail -Benutzerhandbuch](#).

Themen

- [Überwachung von Amazon EventBridge Scheduler mit Amazon CloudWatch](#)
- [Protokollieren von Amazon EventBridge Scheduler-API-Aufrufen mit AWS CloudTrail](#)

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](#)
- [Dimensionen](#)
- [Zugreifen auf -Metriken](#)
- [Liste der Metriken](#)
- [EventBridge Metriken zur Nutzung von Scheduler](#)

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. Beispiel: InvocationAttemptCountoder 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 Ihr Limit für die Drosselung von Aufrufen überschritten haben. Weitere Informationen zu Servicekontingente n finden Sie unter. Kontingente

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.
AWS/Scheduler	InvocationsFailedToBeSentToDeadLetterCount_<error_code>	Anzahl	Das Folgende ist ein Beispiel für die <code>InvocationsFailedToBeSentTo</code>

Namespace	Metrik	Einheit	Beschreibung
			<p>DeadLetter rCount_<e rror_code > Metrik, wenn die Amazon SQS SQS-Warte schlange, die Sie als DLQ angeben, nicht existiert : Invocatio nsFailedT oBeSentTo DeadLette rCount_ AWS.Simp eQueueSer vice.NonE xistentQu eue</p>

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

EventBridge Metriken zur Nutzung von Scheduler

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 unter [Kontingente](#).

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

Derzeit ist der einzige Metrikname in diesem Namespace, der CloudWatch veröffentlicht, `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		
<code>CallCount</code>	Die Anzahl der angegebenen Operationen, die in Ihrem Konto ausgeführt werden.		

Dimensionen

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

Dimension	Beschreibung		
	EventBridge Scheduler API-Nutzungsmetriken verwenden diese Dimension mit einem Wert von None.		
Type	<p>Der Typ der nachverfolgten Ressource.</p> <p>Wenn die Service-Dimension Scheduler ist, ist API der derzeit einzige gültige Wert für Type.</p>		
Resource	<p>Der Name der API-Operation. Gültige Werte sind unter anderem:</p> <ul style="list-style-type: none"> • CreateSchedule • CreateScheduleGroup • DeleteSchedule • DeleteScheduleGroup • GetSchedule • GetScheduleGroup • ListScheduleGroups • ListSchedules • ListTagsForResource • TagResource • UntagResource • UpdateSchedule 		

Protokollieren von Amazon EventBridge Scheduler-API-Aufrufen mit AWS CloudTrail

Amazon EventBridge Scheduler ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in

EventBridge Scheduler ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für EventBridge Scheduler als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der EventBridge Scheduler-Konsole und Codeaufrufen für die EventBridge Scheduler-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für EventBridge Scheduler. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an den EventBridge Scheduler, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

EventBridge Informationen zum Scheduler in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn im EventBridge Scheduler Aktivitäten auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter [Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für den EventBridge Terminplaner, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle EventBridge Scheduler-API-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. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Grundlegendes zu EventBridge Scheduler-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Kontingente für Amazon EventBridge Scheduler

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

Um die Kontingente für EventBridge Scheduler anzuzeigen, öffnen Sie die [Service Quotas Quotas-Konsole](#). Wählen Sie im Navigationsbereich AWS Dienste und anschließend 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](#).

Ihr AWS Konto hat die folgenden Kontingente für EventBridge Scheduler.

Name	Standard	Anpas	Beschreibung
CreateSchedule Rate anfragen	us-east-1: 1 000 us-east-2: 1 000 us-west-2: 1 000 ap-northeast-1: 1 000 ap-south-1:1.000 ap-southeast-1:1.0 00 ap-southeast-2: 1 000 eu-central-1: 1 000 eu-west-1: 1,000	Ja	Maximale Anzahl von CreateSchedule Anfragen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. Dies ist auf Tausende von Anfragen pro Sekunde einstellbar.

Name	Standard	Anpas	Beschreibung
	eu-west-2:1.000 sa-east-1:1.000 Jede der anderen unterstützten Regionen: 250		
CreateScheduleGroup Anforderungsrate	Jede unterstützte Region: 10	Yes (Ja)	Maximale Anzahl CreateScheduleGroup Anfragen pro Sekunde. Wenn Sie dieses Kontingent erreichen , lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab.

Name	Standard	Anpas	Beschreibung
DeleteSchedule Anforderungsrate	us-east-1: 1 000 us-east-2: 1 000 us-west-2: 1 000 ap-northeast-1: 1 000 ap-south-1:1.000 ap-southeast-1:1.0 00 ap-southeast-2: 1 000 eu-central-1: 1 000 eu-west-1: 1,000 eu-west-2:1.000 sa-east-1:1.000 Jede der anderen unterstützten Regionen: 250	Ja	Maximale Anzahl von DeleteSchedule Anfragen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. Dies ist auf Tausende von Anfragen pro Sekunde einstellbar.

Name	Standard	Anpas	Beschreibung
DeleteScheduleGroup Anforderungsrate	Jede unterstützte Region: 10	Yes (Ja)	Maximale Anzahl DeleteScheduleGroup Anfragen 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	us-east-1: 1 000 us-east-2: 1 000 us-west-2: 1 000 ap-northeast-1: 1 000 ap-south-1:1.000 ap-southeast-1:1.0 00 ap-southeast-2: 1 000 eu-central-1: 1 000 eu-west-1: 1,000 eu-west-2:1.000 sa-east-1:1.000 Jede der anderen unterstützten Regionen: 250	Ja	Maximale Anzahl von GetSchedule Anfragen pro Sekunde. Wenn Sie dieses Kontingent erreichen, lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. Dies ist auf Tausende von Anfragen pro Sekunde einstellbar.

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

Name	Standard	Anpas	Beschreibung
Drossel-Limit für Aufrufe in Transaktionen pro Sekunde	us-east-1: 1 000 us-east-2: 1 000 us-west-2: 1 000 ap-northeast-1: 1 000 ap-south-1:1.000 ap-southeast-1:1.000 ap-southeast-2: 1 000 eu-central-1: 1 000 eu-west-1: 1,000 eu-west-2:1.000 sa-east-1:1.000 Jede der anderen unterstützten Regionen: 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. Dies ist auf Zehntausende von Transaktionen pro Sekunde einstellbar.

Name	Standard	Anpas	Beschreibung
ListScheduleGroups Rate anfragen	Jede unterstützte Region: 10	Yes (Ja)	Maximale Anzahl ListScheduleGroups Anfragen 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 Anzahl ListSchedules Anfragen 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: 10 000 000	Ja	Die maximale Anzahl von Zeitplänen pro Region. Dieses Kontingent beinhaltet einmalige Zeitpläne, deren Ausführung abgeschlossen ist. Wir empfehlen, Ihre Zeitpläne mithilfe der ActionAfterCompletion Funktion so zu konfigurieren, dass sie nach Abschluss automatisch gelöscht werden. Dies ist an Milliarden von Zeitplänen anpassbar.
TagResource Rate anfragen	Jede unterstützte Region: 1	Ja	Weist der angegebenen Planer-Ressource ein oder mehrere Tags (Schlüssel-Wert-Paare) zu.
UntagResource Rate anfragen	Jede unterstützte Region: 1	Ja	Entfernt ein oder mehrere Tags aus der angegebenen Planer-Ressource.

Name	Standard	Anpas	Beschreibung
UpdateSchedule Rate anfragen	us-east-1: 1 000 us-east-2: 1 000 us-west-2: 1 000 ap-northeast-1: 1 000 ap-south-1:1.000 ap-southeast-1:1.000 ap-southeast-2: 1 000 eu-central-1: 1 000 eu-west-1: 1,000 eu-west-2:1.000 sa-east-1:1.000 Jede der anderen unterstützten Regionen: 250	<u>Ja</u>	Maximale Anzahl von UpdateSchedule Anfragen pro Sekunde. Wenn Sie dieses Kontingent erreichen , lehnt EventBridge Scheduler Anfragen für diesen Vorgang für den Rest des Intervalls ab. Dies ist auf Tausende von Anfragen pro Sekunde einstellbar.

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

Problembehandlung bei Kontingenten im EventBridge Scheduler

Mithilfe der folgenden Informationen können Sie häufig auftretende Probleme im Zusammenhang mit EventBridge Scheduler-Kontingenten diagnostizieren und beheben.

ServiceQuotaExceededException

Ich erhalte Drosselungsfehler bei `CreateSchedule`, `DeleteSchedule`, `GetSchedule` oder der `UpdateSchedule` Anforderungsrate, obwohl ich unter dem Standardratenlimit liege.

Häufige Ursache

Am 7. September 2023 begann EventBridge Scheduler, den ScheduleGroup ARN (Amazon Resource Name) anstelle des Schedule ARN in den Vertrauensrichtlinien für Ausführungsrollen zu unterstützen. Kunden, die Schedule weiterhin ARNs in ihrer Vertrauensrichtlinie verwenden dürfen, können Grenzwerte von 50 TPS anstelle der Standardgrenzwerte von 250 bis 1000 TPS (abhängig von der Region) festlegen.

Auflösung

Wenden Sie sich an den [Support](#), um ein höheres Höchstlimit anzufordern.

Vorbeugung

Ändern Sie Ihre bestehenden Vertrauensrichtlinien auf eine der folgenden Arten:

- Der gesamte Geltungsbereich wird aus der Rolle entfernt.
- Festlegung des Geltungsbereichs der Rolle, sodass sie mithilfe des Schedule ARN oder des ScheduleGroup ARN übernommen werden kann.

Nehmen wir zum Beispiel an, Sie hätten die folgende bestehende Vertrauensrichtlinie:

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

Sie könnten die Vertrauensrichtlinie wie folgt aktualisieren:

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

Dokumentenverlauf für das EventBridge Scheduler- Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für EventBridge Scheduler beschrieben.

Änderung	Beschreibung	Datum
Änderungen an der Ausführungsrolle und Vermeidung verwirrter Stellvertreter	<p>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.</p> <ul style="list-style-type: none">• the section called “Confused-Deputy-Prävention”	07. September 2023
Automatisches Löschen von Zeitplänen nach Abschluss	<p>EventBridge Der Scheduler unterstützt das automatische Löschen. Wenn Sie das automatische Löschen konfigurieren, löscht EventBridge Scheduler Ihren Zeitplan nach dem letzten geplanten Aufruf.</p> <ul style="list-style-type: none">• the section called “Löschen nach Abschluss des Zeitplans”	02. August 2023

[Das Thema zur Verwendung universeller Ziele wurde aktualisiert](#)

Die Liste der unterstützten Dienste, auf die EventBridge Scheduler abzielen und in die sie integrieren kann, wurde aktualisiert. Dieses Update enthält auch eine Liste der nicht unterstützten GET API-Operationen und enthält Verbesserungen an den Universal Target-Beispielen sowie weitere kleinere Verbesserungen im gesamten Handbuch.

17. März 2023

- [the section called “Verwenden von universalen Zielen”](#)

[Die Informationen zu tarifbasierten Flugplänen ohne Startdatum wurden aktualisiert](#)

Es wurden Informationen darüber hinzugefügt, wie EventBridge Scheduler mit tarifbasierten Zeitplänen umgeht, wenn Sie kein angeben. [StartDate](#)

17. März 2023

- [the section called “Ratenbasierte Zeitpläne”](#)

[Neues Thema zur Verwaltung von Scheduler-Gruppen](#)

Neues Kapitel zum Erstellen von Scheduler-Gruppen mit EventBridge Scheduler hinzugefügt. In diesem Kapitel erfahren Sie, wie Sie eine Gruppe erstellen, der Gruppe Zeitpläne hinzufügen, Tags anwenden, um Ihre EventBridge Scheduler-Ressourcen einfacher zu verwalten und zu überwachen, und schließlich eine Gruppe löschen.

17. März 2023

- [Verwaltung einer Zeitplangruppe](#)

[Neue Themen zur Sommerzeit und zu Zeitzonen](#)

Es wurden neue Abschnitte hinzugefügt, in denen beschrieben wird, wie der EventBridge Scheduler mit der Sommerzeit umgeht und wie Sie Zeitpläne für verschiedene Zeitzonen erstellen können.

17. November 2022

- [the section called “Sommerzeit”](#)
- [the section called “Zeitzone n”](#)

Neues Thema zu Metriken

Es wurde ein neues Thema hinzugefügt, das die Metriken beschreibt, für die EventBridge Scheduler veröffentlicht. CloudWatch Sie können diese Metriken verwenden, um Fehlschläge bei Aufrufen zu überwachen und zu verstehen, wie Sie Probleme mit Ihren Zeitplänen lösen können.

15. November 2022

- [the section called “Überwachung mit CloudWatch”](#)

Erstversion

Erste Version des EventBridge Scheduler-Benutzerhandbuchs

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.