aws

Entwicklerhandbuch

AWS Lambda

AWS Lambda: Entwicklerhandbuch

Table of Contents

Was ist AWS Lambda?

Sie können ihn verwenden AWS Lambda , um Code auszuführen, ohne Server bereitzustellen oder zu verwalten.

Lambda führt Ihren Code auf einer hochverfügbaren Recheninfrastruktur aus und führt die gesamte Verwaltung der Rechenressourcen durch, einschließlich Server- und Betriebssystemwartung, Kapazitätsbereitstellung und automatischer Skalierung sowie Protokollierung. Mit Lambda müssen Sie lediglich Ihren Code in einer der von Lambda unterstützten Laufzeiten bereitstellen.

Sie organisieren Ihren Code in Lambda-Funktionen. Der Lambda-Service führt Ihre Funktion nur bei Bedarf aus und skaliert automatisch. Sie bezahlen nur für die Datenverarbeitungszeit, die Sie wirklich nutzen und es werden keine Gebühren in Rechnung gestellt, wenn Ihr Code nicht ausgeführt wird. Weitere Informationen finden Sie unter AWS Lambda -Preisgestaltung.

> **Tip**
>
> Weitere Informationen zum Erstellen von Serverless-Lösungen finden Sie im Serverless-Benutzerhandbuch.

Verwendung von Lambda

Lambda ist ein idealer Rechenservice für Anwendungsszenarien, die schnell hochskaliert und auf Null herunterskaliert werden müssen, wenn sie nicht benötigt werden. Sie können Lambda beispielsweise für Folgendes verwenden:

- Dateiverarbeitung: Verwenden Sie Amazon Simple Storage Service (Amazon S3), um die Lambda-Datenverarbeitung nach einem Upload in Echtzeit auszulösen.
- Stream-Verarbeitung: Verwenden Sie Lambda und Amazon Kinesis zur Verarbeitung von Echtzeit-Streaming-Daten für Verfolgung von Anwendungsaktivitäten, Verarbeitung von Transaktionsaufträgen, Clickstream-Analyse, Datenbereinigung, Protokollfilterung, Indizierung, Social-Media-Analyse, Internet der Dinge (IoT)-Gerätedatentelemetrie und Messung.
- Webanwendungen: Kombinieren Sie Lambda mit anderen AWS Diensten, um leistungsstarke Webanwendungen zu erstellen, die automatisch hoch- und herunterskaliert werden und in einer hochverfügbaren Konfiguration in mehreren Rechenzentren ausgeführt werden.

- IoT-Backends: Erstellen Sie Serverless-Backends mit Lambda, um Web-, Mobil-, IoT- und Drittanbieter-API-Anfragen zu verarbeiten.
- Mobile Backends: Erstellen Sie Backends mit Lambda und Amazon API Gateway, um API-Anfragen zu authentifizieren und zu verarbeiten. Verwenden Sie AWS Amplify es für die einfache Integration in Ihre iOS-, Android-, Web- und React Native-Frontends.

Wenn Sie Lambda verwenden, sind Sie nur für Ihren Code verantwortlich. Lambda verwaltet die Computing-Flotte, die ein ausgewogenes Verhältnis von Arbeitsspeicher, CPU, Netzwerk und anderen Ressourcen bietet, um Ihren Code auszuführen. Da Lambda diese Ressourcen verwaltet, können Sie sich nicht bei Computing-Instances anmelden oder das Betriebssystem in bereitgestellten Laufzeiten anpassen. Lambda führt in Ihrem Namen operative und administrative Aktivitäten durch, einschließlich der Verwaltung von Kapazität, Überwachung und Protokollierung Ihrer Lambda-Funktionen.

Schlüsselfeatures

Die folgenden Hauptfunktionen helfen Ihnen bei der Entwicklung von Lambda-Anwendungen, die skalierbar, sicher und leicht erweiterbar sind:

Umgebungsvariablen

Verwenden Sie Umgebungsvariablen, um das Verhalten Ihrer Funktion anzupassen, ohne den Code zu aktualisieren.

Versionen

Verwalten Sie die Bereitstellung Ihrer Funktionen mit Versionen, so dass z. B. eine neue Funktion für Beta-Tests verwendet werden kann, ohne dass die Benutzer der stabilen Produktionsversion davon betroffen sind.

Container-Images

Erstellen Sie ein Container-Image für eine Lambda-Funktion, indem Sie ein AWS bereitgestelltes Basis-Image oder ein alternatives Basis-Image verwenden, sodass Sie Ihre vorhandenen Container-Tools wiederverwenden oder größere Workloads bereitstellen können, die auf umfangreichen Abhängigkeiten basieren, wie z. B. maschinelles Lernen.

Ebenen

Verpacken Sie Bibliotheken und andere Abhängigkeiten in Paketen, um die Größe der Bereitstellungsarchive zu reduzieren und die Bereitstellung Ihres Codes zu beschleunigen.

Lambda-Erweiterungen

Ergänzen Sie Ihre Lambda-Funktionen mit Tools für Überwachung, Beobachtbarkeit, Sicherheit und Governance.

Funktions-URLs

Fügen Sie einen dedizierten HTTP(S)-Endpunkt zu Ihrer Lambda-Funktion hinzu.

Antwort-Streaming

Konfigurieren Sie Ihre Lambda-Funktions-URLs, um Antwort-Nutzlasten von Node.js-Funktionen zurück an Clients zu streamen, um die Leistung bis zum ersten Byte (TTFB) zu verbessern oder um größere Nutzlasten zurückzugeben.

Gleichzeitigkeit und Skalierungskontrollen

Sie können die Skalierung und Reaktionsfähigkeit Ihrer Produktionsanwendungen genau steuern.

Codesignatur

Stellen Sie sicher, dass nur zugelassene Entwickler unveränderten, vertrauenswürdigen Code in Ihren Lambda-Funktionen veröffentlichen

Private Vernetzung

Erstellen Sie ein privates Netzwerk für Ressourcen wie Datenbanken, Cache-Instances oder interne Services.

Zugriff auf das Dateisystem

Konfigurieren Sie eine Funktion zum Mounten eines Amazon Elastic File System (Amazon EFS) in ein lokales Verzeichnis, damit Ihr Funktionscode sicher und mit hoher Gleichzeitigkeit auf gemeinsame Ressourcen zugreifen und diese ändern kann.

Lambda SnapStart für Java

Verbessern Sie die Startleistung für Java-Laufzeiten um das bis zu 10-fache, ohne zusätzliche Kosten und in der Regel ohne Änderungen an Ihrem Funktionscode.

Erste Schritte mit Lambda

für Ihre ersten Schritte mit Lambda verwenden Sie die Lambda-Konsole, um eine Funktion zu erstellen. In wenigen Minuten können Sie eine Funktion erstellen und bereitstellen und sie in der Konsole testen.

Bei der Durchführung des Tutorials lernen Sie einige grundlegende Lambda-Konzepte kennen, z. B. wie Sie Argumente an Ihre Funktion mithilfe des Lambda-Ereignisobjekts übergeben. Sie erfahren auch, wie Sie Protokollausgaben von Ihrer Funktion zurückgeben und wie Sie die Aufrufprotokolle Ihrer Funktion in CloudWatch Logs anzeigen können.

Der Einfachheit halber erstellen Sie Ihre Funktion entweder mit der Python- oder Node.js-Laufzeit. Mit diesen interpretierten Sprachen können Sie Funktionscode direkt im integrierten Code-Editor der Konsole bearbeiten. Bei kompilierten Sprachen wie Java und C# müssen Sie ein Bereitstellungspaket auf Ihrem lokalen Build-Rechner erstellen und es in Lambda hochladen. Weitere Informationen zum Bereitstellen von Funktionen in Lambda mithilfe anderer Laufzeiten finden Sie unter den Links im Abschnitt the section called “Zusätzliche Ressourcen und nächste Schritte”.

> **Tip**
>
> Weitere Informationen zum Erstellen von Serverless-Lösungen finden Sie im Serverless-Benutzerhandbuch.

Voraussetzungen

Melde dich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erstellen einer Lambda-Funktion mit der Konsole

In diesem Beispiel besitzt Ihre Funktion ein JSON-Objekt, das zwei ganzzahlige Werte mit der Bezeichnung `"length"` und `"width"` enthält. Die Funktion multipliziert diese Werte, um eine Fläche zu berechnen, und gibt diese als JSON-Zeichenfolge zurück.

Ihre Funktion druckt auch den berechneten Bereich zusammen mit dem Namen der zugehörigen CloudWatch Protokollgruppe. Später im Tutorial werden Sie lernen, CloudWatch Logs zu verwenden, um Aufzeichnungen über den Aufruf Ihrer Funktionen einzusehen.

Um Ihre Funktion zu erstellen, erstellen Sie zunächst mit der Konsole eine grundlegende Hello-World-Funktion. Im folgenden Schritt fügen Sie dann Ihren eigenen Funktionscode hinzu.

So erstellen Sie eine Hello-World-Lambda-Funktion mit der Konsole

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Wählen Sie Verfassen von Grund auf aus.
4. Geben Sie im Bereich Grundlegende Informationen als Funktionsname **`myLambdaFunction`** ein.
5. Wählen Sie als Laufzeit entweder Node.js 20.x oder Python 3.12
6. Belassen Sie die Architektur auf x86_64 und wählen Sie Funktion erstellen.

Lambda erstellt eine Funktion, die die Nachricht `Hello from Lambda!` zurückgibt. Lambda erstellt außerdem eine Ausführungsrolle für Ihre Funktion. Eine Ausführungsrolle ist eine AWS Identity and Access Management (IAM-) Rolle, die einer Lambda-Funktion Zugriff AWS-Services und Ressourcen gewährt. Für Ihre Funktion gewährt die Rolle, die Lambda erstellt, grundlegende Berechtigungen zum Schreiben in CloudWatch Logs.

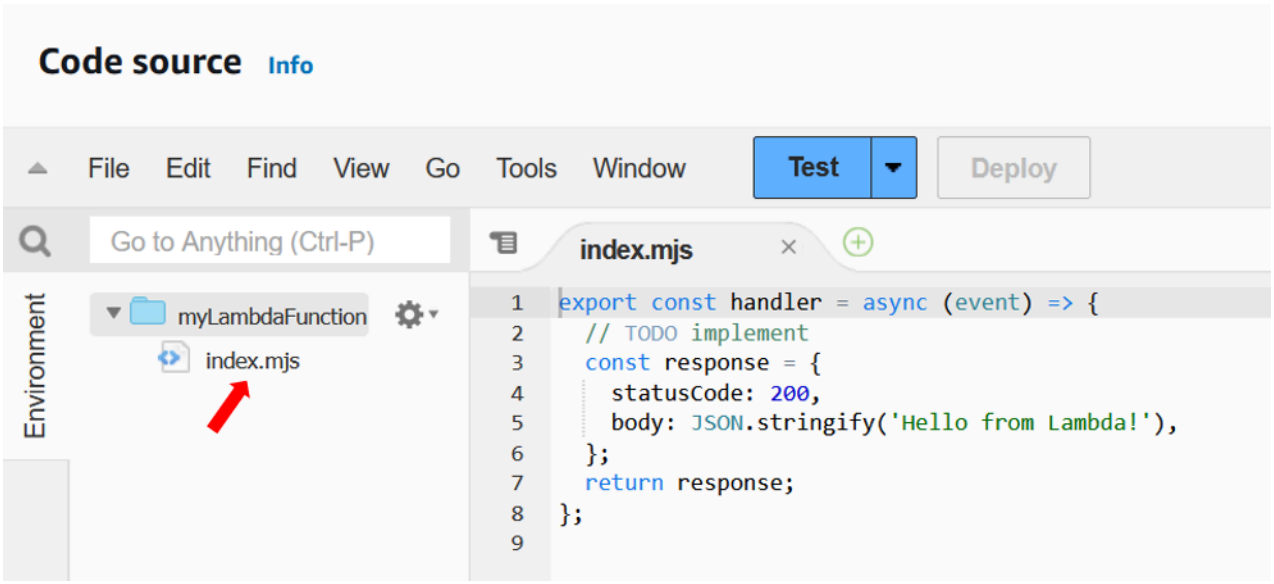
Sie verwenden nun den integrierten Code-Editor der Konsole, um den von Lambda erstellten Hello-World-Code durch Ihren eigenen Funktionscode zu ersetzen.

Node.js

So ändern Sie den Code in der Konsole

1. Wählen Sie die Registerkarte Code.

   Im integrierten Code-Editor der Konsole sollten Sie den von Lambda erstellten Funktionscode sehen. Wenn die Registerkarte index.mjs im Code-Editor nicht angezeigt wird, wählen Sie index.mjs im Datei-Explorer aus, wie im folgenden Diagramm gezeigt.



2. Fügen Sie den folgenden Code in die Registerkarte index.mjs ein und ersetzen Sie den von Lambda erstellten Code.

```
export const handler = async (event, context) => {

  const length = event.length;
  const width = event.width;
  let area = calculateArea(length, width);
  console.log(`The area is ${area}`);

  console.log('CloudWatch log group: ', context.logGroupName);

  let data = {
    "area": area,
  };
    return JSON.stringify(data);

  function calculateArea(length, width) {
    return length * width;
  }
};
```

3. Wählen Sie Bereitstellen aus, um den Code Ihrer Funktion zu aktualisieren. Wenn Lambda die Änderungen bereitgestellt hat, zeigt die Konsole ein Banner an, das Sie über die erfolgreiche Aktualisierung Ihrer Funktion informiert.

Den Funktionscode verstehen

Bevor Sie zum nächsten Schritt übergehen, sollten Sie sich einen Moment Zeit nehmen, um den Funktionscode zu betrachten und einige wichtige Lambda-Konzepte zu verstehen.

- Der Lambda-Handler:

  Ihre Lambda-Funktion enthält eine Node.js-Funktion mit dem Namen `handler`. Eine Lambda-Funktion in Node.js kann mehr als eine Node.js-Funktion enthalten, aber die Handler-Funktion ist immer der Einstiegspunkt in Ihren Code. Wenn Ihre Funktion aufgerufen wird, führt Lambda diese Methode aus.

  Wenn Sie Ihre Hello-World-Funktion über die Konsole erstellt haben, hat Lambda den Namen der Handler-Methode für Ihre Funktion automatisch auf `handler` festgelegt. Achten Sie darauf, den Namen dieser Node.js-Funktion nicht zu bearbeiten. Andernfalls kann Lambda Ihren Code nicht ausführen, wenn Sie Ihre Funktion aufrufen.

  Weitere Informationen zum Lambda-Handler in Node.js finden Sie unter the section called “Handler”.

- Das Lambda-Ereignisobjekt:

  Die Funktion `handler` besitzt zwei Argumente, `event` und `context`. Ein Ereignis in Lambda ist ein JSON-formatiertes Dokument, das Daten enthält, die von Ihrer Funktion verarbeitet werden sollen.

  Wenn Ihre Funktion von einer anderen aufgerufen wird AWS-Service, enthält das Ereignisobjekt Informationen über das Ereignis, das den Aufruf verursacht hat. Wenn beispielsweise ein Amazon Simple Storage Service (Amazon S3)-Bucket beim Hochladen eines Objekts Ihre Funktion aufruft, enthält das Ereignis den Namen des Amazon-S3-Buckets und den Objektschlüssel.

  In diesem Beispiel erstellen Sie ein Ereignis in der Konsole, indem Sie ein JSON-formatiertes Dokument mit zwei Schlüssel-Wert-Paaren eingeben.

- Das Lambda-Kontextobjekt:

  Das zweite Argument, das Ihre Funktion besitzt, ist `context`. Lambda übergibt das Kontextobjekt automatisch an Ihre Funktion. Das Kontextobjekt enthält Informationen über den Aufruf der Funktion und die Ausführungsumgebung.

Mit dem Kontextobjekt können Sie zu Überwachungszwecken Informationen über den Aufruf Ihrer Funktion ausgeben. In diesem Beispiel verwendet Ihre Funktion den `logGroupName` Parameter, um den Namen ihrer CloudWatch Protokollgruppe auszugeben.

Weitere Informationen zum Lambda-Kontextobjekt in Node.js finden Sie unter the section called “Kontext”.

- Protokollierung in Lambda:

  Mit Node.js können Sie Konsolenmethoden wie `console.log` und `console.error` verwenden, um Informationen an das Protokoll Ihrer Funktion zu senden. Der Beispielcode verwendet `console.log` Anweisungen, um die berechnete Fläche und den Namen der CloudWatch Logs-Gruppe der Funktion auszugeben. Sie können auch jede Protokollierungsbibliothek verwenden, die in `stdout` oder `stderr` schreibt.

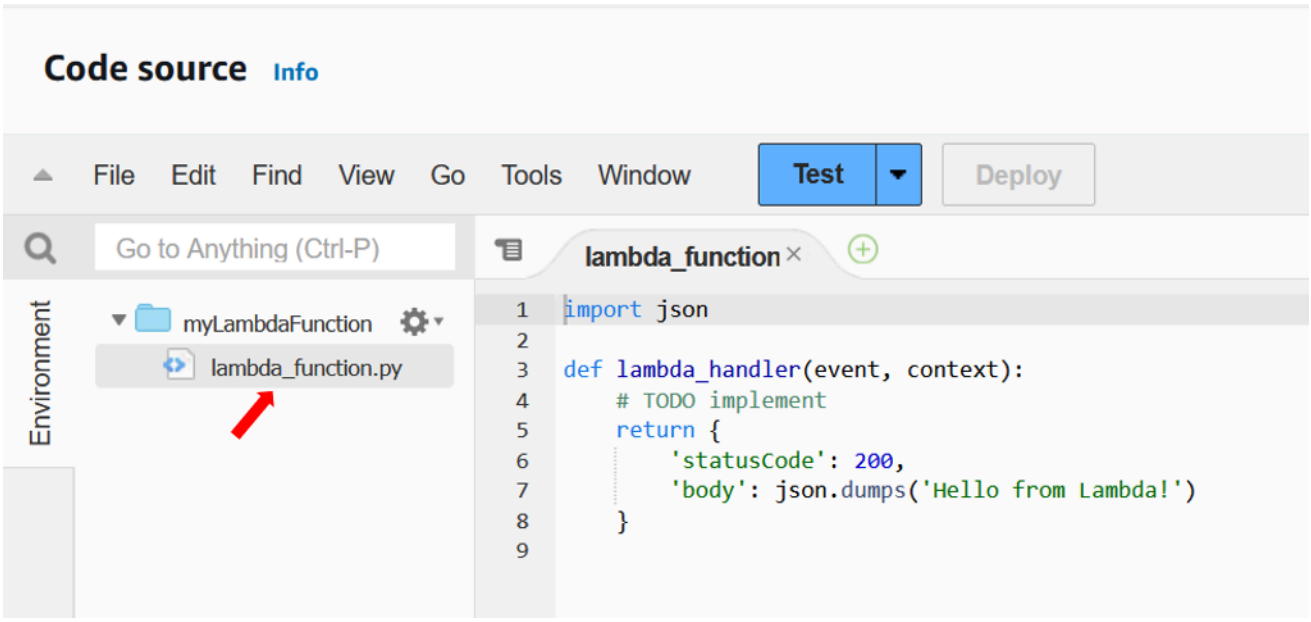
  Weitere Informationen hierzu finden Sie unter the section called “Protokollierung”. Informationen zum Protokollieren in anderen Laufzeiten finden Sie auf den Seiten „Erstellen mit“ für die Laufzeiten, an denen Sie interessiert sind.

Python

So ändern Sie den Code in der Konsole

1. Wählen Sie die Registerkarte Code.

   Im integrierten Code-Editor der Konsole sollten Sie den von Lambda erstellten Funktionscode sehen. Wenn die Registerkarte lambda_function.py im Code-Editor nicht angezeigt wird, wählen Sie lambda_function.py im Datei-Explorer aus, wie im folgenden Diagramm dargestellt.



2. Fügen Sie den folgenden Code in die Registerkarte lambda_function.py ein und ersetzen Sie den von Lambda erstellten Code.

```
import json
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):

    # Get the length and width parameters from the event object. The
    # runtime converts the event object to a Python dictionary
    length = event['length']
    width = event['width']

    area = calculate_area(length, width)
    print(f"The area is {area}")

    logger.info(f"CloudWatch logs group: {context.log_group_name}")

    # return the calculated area as a JSON string
    data = {"area": area}
    return json.dumps(data)

def calculate_area(length, width):
    return length*width
```

3. Wählen Sie Bereitstellen aus, um den Code Ihrer Funktion zu aktualisieren. Wenn Lambda die Änderungen bereitgestellt hat, zeigt die Konsole ein Banner an, das Sie über die erfolgreiche Aktualisierung Ihrer Funktion informiert.

Den Funktionscode verstehen

Bevor Sie zum nächsten Schritt übergehen, sollten Sie sich einen Moment Zeit nehmen, um den Funktionscode zu betrachten und einige wichtige Lambda-Konzepte zu verstehen.

- Der Lambda-Handler:

  Ihre Lambda-Funktion enthält eine Python-Funktion mit dem Namen `lambda_handler`. Eine Lambda-Funktion in Python kann mehr als eine Python-Funktion enthalten, aber die Handler-Funktion ist immer der Einstiegspunkt in Ihren Code. Wenn Ihre Funktion aufgerufen wird, führt Lambda diese Methode aus.

  Wenn Sie Ihre Hello-World-Funktion über die Konsole erstellt haben, hat Lambda den Namen der Handler-Methode für Ihre Funktion automatisch auf `lambda_handler` festgelegt. Achten Sie darauf, den Namen dieser Python-Funktion nicht zu bearbeiten. Andernfalls kann Lambda Ihren Code nicht ausführen, wenn Sie Ihre Funktion aufrufen.

  Weitere Informationen zum Lambda-Handler in Python finden Sie unter the section called “Handler”.

- Das Lambda-Ereignisobjekt:

  Die Funktion `lambda_handler` besitzt zwei Argumente, `event` und `context`. Ein Ereignis in Lambda ist ein JSON-formatiertes Dokument, das Daten enthält, die von Ihrer Funktion verarbeitet werden sollen.

  Wenn Ihre Funktion von einer anderen aufgerufen wird AWS-Service, enthält das Ereignisobjekt Informationen über das Ereignis, das den Aufruf verursacht hat. Wenn beispielsweise ein Amazon Simple Storage Service (Amazon S3)-Bucket beim Hochladen eines Objekts Ihre Funktion aufruft, enthält das Ereignis den Namen des Amazon-S3-Buckets und den Objektschlüssel.

  In diesem Beispiel erstellen Sie ein Ereignis in der Konsole, indem Sie ein JSON-formatiertes Dokument mit zwei Schlüssel-Wert-Paaren eingeben.

- Das Lambda-Kontextobjekt:

Das zweite Argument, das Ihre Funktion besitzt, ist `context`. Lambda übergibt das Kontextobjekt automatisch an Ihre Funktion. Das Kontextobjekt enthält Informationen über den Aufruf der Funktion und die Ausführungsumgebung.

Mit dem Kontextobjekt können Sie zu Überwachungszwecken Informationen über den Aufruf Ihrer Funktion ausgeben. In diesem Beispiel verwendet Ihre Funktion den `log_group_name` Parameter, um den Namen ihrer CloudWatch Protokollgruppe auszugeben.

Weitere Informationen zum Lambda-Kontextobjekt in Python finden Sie unter the section called “Kontext”.

- Protokollierung in Lambda:

  Mit Python können Sie entweder eine `print`-Anweisung oder eine Python-Protokollbibliothek verwenden, um Informationen an das Protokoll Ihrer Funktion zu senden. Um den Unterschied in der Erfassung zu veranschaulichen, werden im Beispielcode beide Methoden verwendet. In einer Produktionsanwendung empfehlen wir die Verwendung einer Protokollierungsbibliothek.

  Weitere Informationen hierzu finden Sie unter the section called “Protokollierung”. Informationen zum Protokollieren in anderen Laufzeiten finden Sie auf den Seiten „Erstellen mit“ für die Laufzeiten, an denen Sie interessiert sind.

Aufrufen der Lambda-Funktion mithilfe der Konsole

Um Ihre Funktion über die Lambda-Konsole aufzurufen, erstellen Sie zunächst ein Testereignis, das Sie an Ihre Funktion senden. Beim Ereignis handelt es sich um ein JSON-formatiertes Dokument, das zwei Schlüssel-Wert-Paare mit den Schlüsseln `"length"` und `"width"`. enthält.

So erstellen Sie das Testereignis

1. Wählen Sie im Bereich Codequelle die Option Testen aus.
2. Wählen Sie Neues Ereignis erstellen.
3. Geben Sie für Ereignisname **`myTestEvent`** ein.
4. Ersetzen Sie im Bereich JSON-Ereignis die Standardwerte, indem Sie Folgendes einfügen:

```
{
  "length": 6,
  "width": 7
```

```
}
```

5. Wählen Sie Speichern.

Sie testen jetzt Ihre Funktion und verwenden die Lambda-Konsole und CloudWatch Logs, um Aufzeichnungen über den Aufruf Ihrer Funktion einzusehen.

So testen Sie Ihre Funktion und zeigen die Aufrufdatensätze in der Konsole an

- Wählen Sie im Bereich Codequelle die Option Testen aus. Wenn die Ausführung Ihrer Funktion abgeschlossen ist, werden die Antwort- und Funktionsprotokolle auf der Registerkarte Ausführungsergebnisse angezeigt. Sie sollten Ergebnisse ähnlich den folgenden sehen.

  Node.js

  ```
  Test Event Name
  myTestEvent

  Response
  "{\"area\":42}"

  Function Logs
  START RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Version: $LATEST
  2023-08-31T23:39:45.313Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO The area is
   42
  2023-08-31T23:39:45.331Z 5c012b0a-18f7-4805-b2f6-40912935034a INFO CloudWatch
   log group:  /aws/lambda/myLambdaFunction
  END RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a
  REPORT RequestId: 5c012b0a-18f7-4805-b2f6-40912935034a Duration: 20.67 ms Billed
   Duration: 21 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration:
   163.87 ms

  Request ID
  5c012b0a-18f7-4805-b2f6-40912935034a
  ```

  Python

  ```
  Test Event Name
  myTestEvent
  ```

```
Response
"{\"area\": 42}"

Function Logs
START RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Version: $LATEST
The area is 42
[INFO] 2023-08-31T23:43:26.428Z 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b CloudWatch
 logs group: /aws/lambda/myLambdaFunction
END RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
REPORT RequestId: 2d0b1579-46fb-4bf7-a6e1-8e08840eae5b Duration: 1.42 ms Billed
 Duration: 2 ms Memory Size: 128 MB Max Memory Used: 39 MB Init Duration: 123.74
 ms

Request ID
2d0b1579-46fb-4bf7-a6e1-8e08840eae5b
```

In diesem Beispiel haben Sie Ihren Code mithilfe des Test-Features der Konsole aufgerufen. Dies bedeutet, dass Sie die Ausführungsergebnisse Ihrer Funktion direkt in der Konsole anzeigen können. Wenn Ihre Funktion außerhalb der Konsole aufgerufen wird, müssen Sie Logs verwenden. CloudWatch

Um die Aufrufaufzeichnungen Ihrer Funktion in Logs einzusehen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe für Ihre Funktion (`/aws/lambda/myLambdaFunction`) aus. Dies ist der Name der Protokollgruppe, den Ihre Funktion an die Konsole ausgegeben hat.
3. Wählen Sie auf der Registerkarte Protokollstreams den Protokollstream für den Aufruf Ihrer Funktion aus.

   Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

   Node.js

   ```
   INIT_START Runtime Version: nodejs:20.v13    Runtime Version ARN:
    arn:aws:lambda:us-
   west-2::runtime:e3aaabf6b92ef8755eaae2f4bfdcb7eb8c4536a5e044900570a42bdba7b869d9
   START RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20 Version: $LATEST
   2023-08-23T22:04:15.809Z    5c012b0a-18f7-4805-b2f6-40912935034a  INFO The area
    is 42
   ```

```
2023-08-23T22:04:15.810Z    aba6c0fc-cf99-49d7-a77d-26d805dacd20  INFO
 CloudWatch log group:  /aws/lambda/myLambdaFunction
END RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20
REPORT RequestId: aba6c0fc-cf99-49d7-a77d-26d805dacd20    Duration: 17.77 ms
 Billed Duration: 18 ms    Memory Size: 128 MB    Max Memory Used: 67 MB    Init
 Duration: 178.85 ms
```

Python

```
INIT_START Runtime Version: python:3.12.v16    Runtime Version ARN:
 arn:aws:lambda:us-
west-2::runtime:ca202755c87b9ec2b58856efb7374b4f7b655a0ea3deb1d5acc9aee9e297b072
START RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e Version: $LATEST
The area is 42
[INFO] 2023-09-01T00:05:22.464Z 9315ab6b-354a-486e-884a-2fb2972b7d84 CloudWatch
 logs group: /aws/lambda/myLambdaFunction
END RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e
REPORT RequestId: 9d4096ee-acb3-4c25-be10-8a210f0a9d8e    Duration: 1.15 ms
 Billed Duration: 2 ms    Memory Size: 128 MB    Max Memory Used: 40 MB
```

Bereinigen

Wenn Sie mit der Beispielfunktion fertig sind, löschen Sie sie. Sie können auch die Protokollgruppe löschen, in der die Protokolle der Funktion gespeichert sind, sowie die von der Konsole erstellte Ausführungsrolle.

So löschen Sie eine Lambda-Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie im Dialogfenster Delete function (Funktion löschen) den Text löschen ein und wählen Sie anschließend Delete (Löschen) aus.

So löschen Sie die Protokollgruppe

1. Öffnen Sie die Seite Protokollgruppen der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe der Funktion (`/aws/lambda/my-function`).

3. Wählen Sie Actions (Aktionen), Delete log group(s) (Protokollgruppe(n) löschen) aus.
4. Wählen Sie im Dialogfeld Delete log group(s) (Protokollgruppe(n) löschen) die Option Delete (Löschen) aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Rollen der AWS Identity and Access Management (IAM-) Konsole.
2. Wählen Sie die Ausführungsrolle der Funktion aus (zum Beispiel `myLambdaFunction-role-31exxmpl`).
3. Wählen Sie Löschen aus.
4. Geben Sie im Dialogfenster Delete role (Rolle löschen) den Namen der Rolle ein und wählen Sie anschließend Delete (Löschen) aus.

Sie können die Erstellung und Bereinigung von Funktionen, Protokollgruppen und Rollen mit AWS CloudFormation und dem AWS Command Line Interface ()AWS CLI automatisieren.

Zusätzliche Ressourcen und nächste Schritte

Nachdem Sie mit der Konsole eine einfache Lambda-Funktion erstellt und getestet haben, führen Sie die folgenden Schritte aus:

- Erfahren Sie, wie Sie Ihrem Code Abhängigkeiten hinzufügen und diesen mithilfe eines ZIP-Bereitstellungspakets bereitstellen. Wählen Sie unter den folgenden Links die Sprachen aus, die Sie interessieren.

  Node.js

  Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

  Typescript

  Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

  Python

  Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

  Ruby

  Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

Java

Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

Go

Siehe the section called “Bereitstellen von ZIP-Dateiarchiven”

C#

Siehe the section called “Bereitstellungspaket”

- Führen Sie das Tutorial Verwenden eines Amazon-S3-Auslösers zum Aufrufen einer Lambda-Funktion durch, um zu erfahren, wie Sie eine Lambda-Funktion so konfigurieren, dass sie von einem anderen AWS-Service aufgerufen wird.
- Wählen Sie eines der folgenden Tutorials für ein komplexeres Beispiel für die Verwendung von Lambda mit anderen AWS-Services.
  - Verwenden von Lambda mit API Gateway: Erstellen Sie eine REST-API für Amazon API Gateway, die eine Lambda-Funktion aufruft.
  - Verwenden einer Lambda-Funktion für den Zugriff auf eine Amazon-RDS-Datenbank: Verwenden Sie eine Lambda-Funktion, um Daten über den RDS-Proxy in eine Datenbank des Amazon Relational Database Service (Amazon RDS) zu schreiben.
  - Verwenden eines Amazon-S3-Auslösers zum Erstellen von Miniaturbildern: Verwenden Sie eine Lambda-Funktion, um bei jedem Hochladen einer Image-Datei in einen Amazon-S3-Bucket ein Miniaturbild zu erstellen.

AWS Lambda Grundlagen

Die Lambda-Funktion ist die Prinzipalressource des Lambda-Services.

Sie können Ihre Funktionen mithilfe der Lambda-Konsole, der Lambda-API AWS CloudFormation oder konfigurieren AWS SAM. Sie erstellen Code für die Funktion und laden den Code mithilfe eines Bereitstellungspakets hoch. Lambda ruft die Funktion auf, wenn ein Ereignis eintritt. Lambda führt mehrere Instances Ihrer Funktion parallel aus, abhängig von Parallelitäts- und Skalierungsgrenzen.

Themen

Lambda-Konzepte

Lambda führt Instances Ihrer Funktion aus, um Ereignisse zu verarbeiten. Sie können Ihre Funktion direkt über die Lambda-API aufrufen oder Sie können einen AWS Dienst oder eine Ressource so konfigurieren, dass Ihre Funktion aufgerufen wird.

Konzepte

- Funktion
- Auslöser
- Ereignis
- Ausführungsumgebung
- Befehlssatz-Architektur
- Bereitstellungspaket
- Laufzeit
- Ebene
- Erweiterung
- Nebenläufigkeit
- Qualifier
- Bestimmungsort

Funktion

Eine Funktion ist eine Ressource, die Sie aufrufen können, um Ihren Code in Lambda auszuführen. Eine Funktion verfügt über Code zur Verarbeitung der Ereignisse, die Sie an die Funktion übergeben oder die andere AWS-Services an die Funktion senden.

Auslöser

Ein Auslöser ist eine Ressource oder Konfiguration, die eine Lambda-Funktion aufruft. Auslöser umfassen AWS-Services, die Sie zum Aufrufen einer Funktion und Ereignisquellen-Mappings konfigurieren können. Ein Ereignisquellen-Mapping ist eine Ressource in Lambda die Elemente aus einem Stream oder einer Warteschlange liest und eine Funktion aufruft. Weitere Informationen erhalten Sie unter Grundlegendes zu Methoden zum Aufrufen von Lambda-Funktionen und Lambda mit Ereignissen aus anderen Diensten aufrufen AWS.

Ereignis

Ein Ereignis ist ein JSON-formatiertes Dokument, das Daten für eine Lambda-Funktion enthält, die verarbeitet werden soll. Die Laufzeit konvertiert die Funktion zu einem Objekt und übergibt es an Ihren Funktionscode. Wenn Sie eine Funktion aufrufen, bestimmen Sie die Struktur und den Inhalt des Ereignisses.

Example Benutzerdefiniertes Ereignis – Wetterdaten

```
{
  "TemperatureK": 281,
  "WindKmh": -3,
  "HumidityPct": 0.55,
  "PressureHPa": 1020
}
```

Wenn ein AWS-Service Ihre Funktion aufruft, definiert der Service die Ereignisform.

Example Ein Serviceereignis – Amazon-SNS-Benachrichtigung

```
{
  "Records": [
    {
      "Sns": {
        "Timestamp": "2019-01-02T12:45:07.000Z",
        "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi+tE/1+82j...65r==",
        "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
        "Message": "Hello from SNS!",
        ...
```

Weitere Informationen zu Ereignissen aus AWS-Services finden Sie unter Lambda mit Ereignissen aus anderen Diensten aufrufen AWS.

Ausführungsumgebung

Eine Ausführungsumgebung bietet eine sichere und isolierte Laufzeitumgebung für Ihre Lambda-Funktion. Eine Ausführungsumgebung verwaltet die Prozesse und Ressourcen, die zum Ausführen der Funktion erforderlich sind. Die Ausführungsumgebung bietet Lebenszyklusunterstützung für die Funktion und für alle Erweiterungen, die mit Ihrer Funktion verknüpft sind.

Weitere Informationen finden Sie unter Lambda-Ausführungsumgebung.

Befehlssatz-Architektur

Die-Befehlssatz-Architekturbestimmt den Typ des Computerprozessors, den Lambda zum Ausführen der Funktion verwendet. Lambda bietet eine Auswahl an Befehlssatz-Architekturen:

- arm64 — 64-Bit-ARM-Architektur, für die AWS Graviton2-Prozessor.
- x86_64 — 64-Bit-x86-Architektur für x86-basierte Prozessoren.

Weitere Informationen finden Sie unter Konfiguration der Befehlssatzarchitektur für eine Lambda-Funktion.

Bereitstellungspaket

Sie stellen Ihren Lambda-Funktionscode mithilfe eines Bereitstellungspakets bereit. Lambda unterstützt zwei Arten von Bereitstellungspaketen:

- Ein ZIP-Dateiarchiv, das Ihren Funktionscode und seine Abhängigkeiten enthält. Lambda stellt das Betriebssystem und die Laufzeit für Ihre Funktion bereit.
- Ein Container-Image, das mit der Open Container Initiative (OCI)-Spezifikation kompatibel ist. Sie fügen dem Image Ihren Funktionscode und Ihre Abhängigkeiten hinzu. Sie müssen auch das Betriebssystem und eine Lambda-Laufzeit angeben.

Weitere Informationen finden Sie unter Lambda-Bereitstellungspakete.

Laufzeit

Die Laufzeit stellt eine sprachspezifische Umgebung bereit, die in der Ausführungsumgebung ausgeführt wird. Die Laufzeit leitet Aufrufereignisse, Kontextinformationen und Antworten zwischen Lambda und der Funktion weiter. Sie können von Lambda bereitgestellte Laufzeiten verwenden oder Ihre eigenen erstellen. Wenn Sie Ihren Code als ZIP-Dateiarchiv verpacken, müssen Sie Ihre Funktion so konfigurieren, dass eine Laufzeitumgebung verwendet wird, die Ihrer Programmiersprache entspricht. Bei einem Container-Image schließen Sie die Laufzeit beim Erstellen des Images ein.

Weitere Informationen finden Sie unter Lambda-Laufzeiten.

Ebene

Eine Lambda-Ebene ist ein ZIP-Dateiarchiv, das zusätzlichen Code oder Daten enthalten kann. Eine Ebene kann Bibliotheken, eine benutzerdefinierte Laufzeit, Daten oder Konfigurationsdateien enthalten.

Mit Ebenen lassen sich auf einfache Weise Bibliotheken und andere Abhängigkeiten verpacken, die Sie mit Ihren Lambda-Funktionen benutzen können. Die Verwendung von Ebenen verringert die Größe hochgeladener Bereitstellungsarchive und ermöglicht eine schnellere Bereitstellung Ihres Codes. Ebenen fördern außerdem die gemeinsame Nutzung von Code und die Trennung von Verantwortlichkeiten, damit Sie beim Schreiben von Geschäftslogik schneller iterieren können.

Sie können pro Funktion bis zu fünf Ebenen einschließen. Ebenen zählen zu den standardmäßigen Größenkontingenten für die Lambda-Bereitstellung. Wenn Sie eine Ebene in eine Funktion einschließen, wird der Inhalt in das `/opt`-Verzeichnis der Ausführungsumgebung entpackt.

Standardmäßig sind von Ihnen erstellte Ebenen privat für Ihr AWS-Konto. Sie können eine Ebene wahlweise auch mit anderen Konten teilen oder sie öffentlich machen. Falls Ihre Funktionen eine Ebene verwendet, die ein anderes Konto veröffentlicht hat, können Ihre Funktionen die Ebenenversion auch weiterverwenden, nachdem diese gelöscht wurde oder Ihre Zugangsberechtigung zur Ebene widerrufen wurde. Sie können jedoch keine neue Funktion erstellen oder Funktionen mit einer gelöschten Ebenen-Version aktualisieren.

Funktionen, die als Container-Image bereitgestellt werden, verwenden keine Ebenen. Stattdessen packen Sie Ihre bevorzugte Laufzeitumgebung, Bibliotheken und andere Abhängigkeiten beim Erstellen des Images in das Container-Image.

Weitere Informationen finden Sie unter Lambda-Ebenen.

Erweiterung

Lambda-Erweiterungen ermöglichen Ihnen, Ihre Funktionen zu erweitern. Sie können beispielsweise Erweiterungen verwenden, um Ihre Funktionen in Ihre bevorzugten Überwachungs-, Beobachtbarkeits-, Sicherheits- und Governance-Tools zu integrieren. Sie können aus einer Vielzahl von Tools wählen, die von AWS Lambda-Partnern bereitgestellt werden, oder Sie können Ihre eigenen Lambda-Erweiterungen erstellen.

Eine interne Erweiterung wird im Laufzeitprozess ausgeführt und hat denselben Lebenszyklus wie die Laufzeitumgebung. Eine externe Erweiterung wird als separater Prozess in der

Ausführungsumgebung ausgeführt. Die externe Erweiterung wird initialisiert, bevor die Funktion aufgerufen wird, wird parallel zur Laufzeit der Funktion und weiterhin ausgeführt, nachdem der Funktionsaufruf abgeschlossen ist.

Weitere Informationen finden Sie unter Erweitern Sie Lambda-Funktionen mithilfe von Lambda-Erweiterungen.

Nebenläufigkeit

Gleichzeitigkeit bezeichnet die Anzahl der Anforderungen, die Ihre Funktion zu einem bestimmten Zeitpunkt verarbeitet. Wenn Ihre Funktion aufgerufen wird, stellt Lambda eine Instance bereit, um das Ereignis zu verarbeiten. Wenn der Funktionscode die Ausführung abgeschlossen hat, kann er eine andere Anforderung verarbeiten. Wenn die Funktion erneut aufgerufen wird, während noch eine Anforderung verarbeitet wird, erfolgt die Bereitstellung einer weiteren Instance, wodurch die Gleichzeitigkeit der Funktion erhöht wird.

Die Gleichzeitigkeit unterliegt Kontingenten auf AWS-Regionenebene. Sie können auch einzelne Funktionen konfigurieren, um ihre Gleichzeitigkeit zu begrenzen oder sicherzustellen, dass sie eine bestimmte Gleichzeitigkeitsstufe erreichen können. Weitere Informationen finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.

Qualifier

Wenn Sie eine Funktion aufrufen oder anzeigen, können Sie einen Qualifikator angeben, um eine Version oder einen Alias festzulegen. Eine Version ist ein unveränderlicher Snapshot des Codes und der Konfiguration einer Funktion, die einen numerischen Qualifikator hat. Beispiel, `my-function:1`. Ein Alias ist ein Zeiger auf eine Version, der aktualisiert werden kann, um ihn einer anderen Version zuzuordnen oder den Datenverkehr zwischen zwei Versionen aufzuteilen. Beispiel, `my-function:BLUE`. Sie können Versionen und Aliase zusammen verwenden, um eine stabile Schnittstelle für Clients bereitzustellen, über die diese Ihre Funktion aufrufen können.

Weitere Informationen finden Sie unter Versionen der Lambda-Funktion.

Bestimmungsort

Ein Ziel ist eine AWS-Ressource, an die Lambda Ereignisse von einem asynchronen Aufruf senden kann. Sie können ein Ziel für Ereignisse konfigurieren, deren Verarbeitung fehlschlägt. Einige Services unterstützen auch ein Ziel für Ereignisse, die erfolgreich verarbeitet wurden.

Weitere Informationen finden Sie unter Konfigurieren von Zielen für den asynchronen Aufruf.

Lambda-Programmiermodell

Lambda stellt ein Programmiermodell bereit, das allen Laufzeitumgebungen gemeinsam ist. Das Programmiermodell definiert die Schnittstelle zwischen Ihrem Code und dem Lambda-System. Sie teilen Lambda den Einstiegspunkt für Ihre Funktion mit, indem Sie einen Handler in der Funktionskonfiguration definieren. Die Laufzeit übergibt Objekte an den Handler, die das Aufrufereignis und den Kontext, wie z. B. den Funktionsnamen und die Anforderungs-ID, enthalten.

Wenn der Handler die Verarbeitung des ersten Ereignisses beendet hat, sendet die Laufzeit ihm ein anderes. Die Klasse der Funktion bleibt im Speicher, sodass Clients und Variablen, die außerhalb der Handler-Methode in Initialisierungscodedeklariert sind, wiederverwendet werden können. Um die Verarbeitungszeit bei nachfolgenden Ereignissen zu verkürzen, erstellen Sie während der Initialisierung wiederverwendbare Ressourcen wie AWS SDK-Clients. Nach der Initialisierung kann jede Instance Ihrer Funktion Tausende von Anfragen verarbeiten.

Ihre Funktion hat auch Zugriff auf den lokalen Speicher im `/tmp`-Verzeichnis. Der Inhalt des Verzeichnisses bleibt bestehen, wenn die Ausführungsumgebung eingefroren ist, und bietet einen temporären Zwischenspeicher, der für mehrere Aufrufe verwendet werden kann. Weitere Informationen finden Sie unter Lambda-Ausführungsumgebung.

Wenn die AWS X-Ray-Ablaufverfolgung aktiviert ist, zeichnet die Laufzeitumgebung separate Untersegmente für die Initialisierung und Ausführung auf.

Die Laufzeit erfasst die Protokollierungsausgabe Ihrer Funktion und sendet sie an Amazon CloudWatch Logs. Neben der Protokollierung der Ausgabe Ihrer Funktion protokolliert die Laufzeitumgebung auch Einträge, wenn der Funktionsaufruf gestartet und beendet wird. Dazu gehört ein Berichtsprotokoll mit der Anforderungskennung, der fakturierten Dauer, der Initialisierungsdauer und weiteren Details. Wenn Ihre Funktion einen Fehler ausgibt, gibt die Laufzeit diesen Fehler an den Aufrufer zurück.

> **Note**
>
> Die Protokollierung unterliegt den CloudWatch Logs-Kontingenten . Protokolldaten können durch Ablehnung verloren gehen, oder, in einigen Fällen, wenn eine Instance Ihrer Funktion gestoppt wird.

Lambda skaliert Ihre Funktion, indem zusätzliche Instances davon ausgeführt werden, wenn der Bedarf steigt und indem Instances beendet werden, wenn der Bedarf sinkt. Dieses Modell führt zu Variationen in der Anwendungsarchitektur, wie zum Beispiel:

- Sofern nicht anders angegeben, werden eingehende Anforderungen nicht in der richtigen Reihenfolge oder gleichzeitig verarbeitet.
- Verlassen Sie sich nicht darauf, dass die Instances Ihrer Funktion langlebig sind, sondern speichern Sie den Zustand Ihrer Anwendung an anderer Stelle.
- Verwenden Sie lokale Speicher und Objekte auf Klassenebene, um die Leistung zu steigern, aber halten Sie die Größe Ihres Bereitstellungspakets und die Datenmenge, die Sie in die Ausführungsumgebung übertragen, möglichst gering.

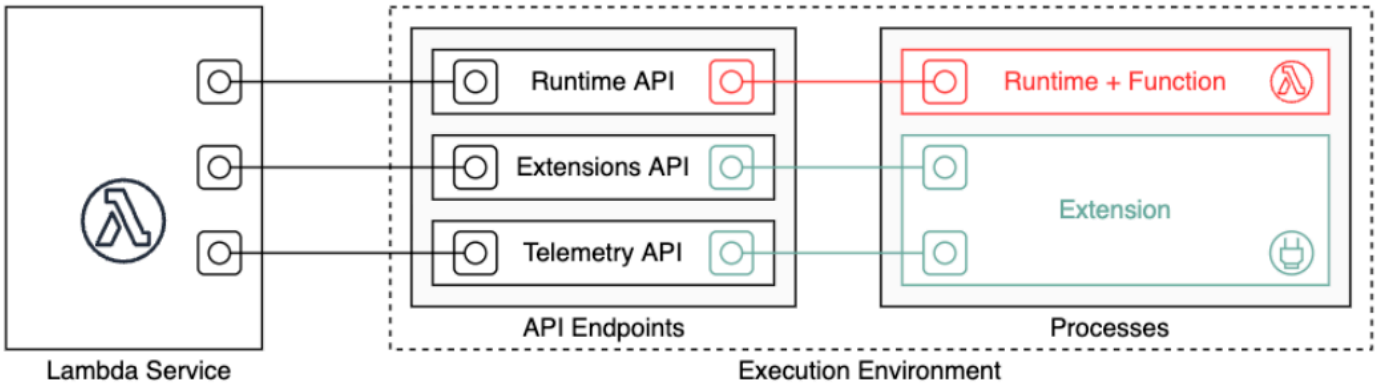
In den folgenden Kapiteln finden Sie eine praktische Einführung in das Programmiermodell in Ihrer bevorzugten Programmiersprache.

- Erstellen von Lambda-Funktionen mit Node.js
- Erstellen von Lambda-Funktionen mit Python
- Erstellen von Lambda-Funktionen mit Ruby
- Erstellen von Lambda-Funktionen mit Java
- Erstellen von Lambda-Funktionen mit Go
- Erstellen von Lambda-Funktionen mit C#
- Aufbau von Lambda-Funktionen mit PowerShell

Lambda-Ausführungsumgebung

Lambda ruft Ihre Funktion in einer Ausführungsumgebung auf, die eine sichere und isolierte Laufzeitumgebung bereitstellt. Die Ausführungsumgebung verwaltet die Ressourcen, die zum Ausführen Ihrer Funktion erforderlich sind. Die Ausführungsumgebung bietet auch Lebenszyklusunterstützung für die Laufzeit der Funktion und alle externen Erweiterungen die mit Ihrer Funktion verknüpft sind.

Die Laufzeitumgebung der Funktion kommuniziert Lambda mit der Laufzeit-API. Erweiterungen kommunizieren mit Lambda über die Erweiterungs-API. Erweiterungen können mithilfe der Telemetrie-API auch Protokollnachrichten und andere Telemetriedaten von der Funktion empfangen.



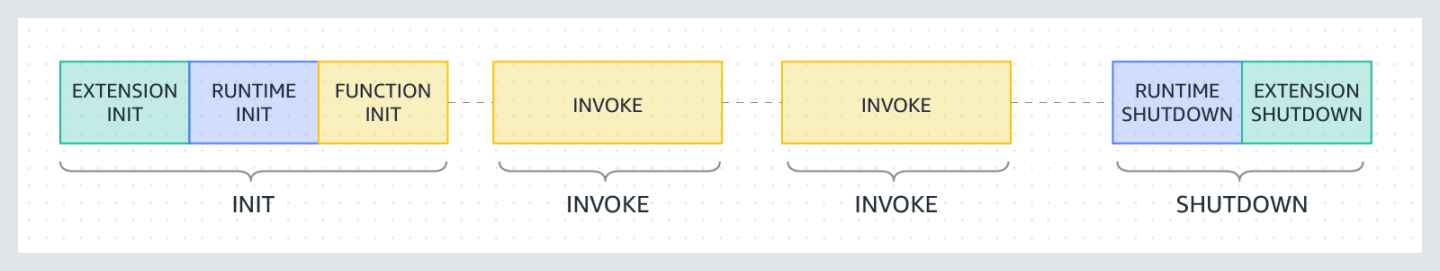
Wenn Sie Ihre Lambda-Funktion erstellen, geben Sie Konfigurationsinformationen an, z. B. den verfügbaren Arbeitsspeicher und die maximal zulässige Ausführungszeit für Ihre Funktion. Lambda verwendet diese Informationen, um die Ausführungsumgebung einzurichten.

Die Laufzeit der Funktion und jede externe Erweiterung sind Prozesse, die innerhalb der Ausführungsumgebung ausgeführt werden. Berechtigungen, Ressourcen, Anmeldeinformationen und Umgebungsvariablen werden von der Funktion und den Erweiterungen gemeinsam genutzt.

Themen

- Lebenszyklus der Lambda-Ausführungsumgebung
- Implementierung von Staatenlosigkeit in Funktionen

Lebenszyklus der Lambda-Ausführungsumgebung



Jede Phase beginnt mit einem Ereignis, das Lambda an die Laufzeit und an alle registrierten Erweiterungen sendet. Die Laufzeit und jede Erweiterung zeigen den Abschluss durch Senden einer `Next`-API-Anfrage an. Lambda friert die Ausführungsumgebung ein, wenn die Laufzeit und jede Erweiterung abgeschlossen sind und keine ausstehenden Ereignisse vorhanden sind.

Themen

Init-Phase

Lambda führt in der `Init`-Phase drei Aufgaben aus:

- Alle Erweiterungen starten (`Extension init`)
- Laufzeit-Bootstrap (`Runtime init`)
- Ausführen des statischen Codes der Funktion (`Function init`)
- Alle `beforeCheckpoint` Runtime-Hooks ausführen (SnapStart nur Lambda)

Die `Init`-Phase endet, wenn die Laufzeit und alle Erweiterungen signalisieren, dass sie bereit sind, indem sie eine `Next`-API-Anforderung senden. Die `Init`-Phase ist auf 10 Sekunden begrenzt. Wenn alle drei Aufgaben nicht innerhalb von 10 Sekunden abgeschlossen werden, versucht Lambda die `Init`-Phase zum Zeitpunkt des ersten Funktionsaufrufs mit dem konfigurierten Funktionstimeout erneut.

Wenn Lambda SnapStart aktiviert ist, findet die `Init`-Phase statt, wenn Sie eine Funktionsversion veröffentlichen. Lambda speichert einen Snapshot des Arbeitsspeichers und des Festplattenzustands der initialisierten Ausführungsumgebung, speichert den verschlüsselten Snapshot und speichert ihn im Cache für den Zugriff mit geringer Latenz. Wenn Sie über einen `beforeCheckpoint`-Laufzeit-Hook verfügen, wird der Code am Ende der `Init`-Phase ausgeführt.

> **Note**
>
> Das 10-Sekunden-Timeout gilt nicht für Funktionen, die bereitgestellte Parallelität verwenden oder. SnapStart Bei bereitgestellter Parallelität und SnapStart Funktionen kann Ihr Initialisierungscode bis zu 15 Minuten lang ausgeführt werden. Das Zeitlimit beträgt 130 Sekunden oder das konfigurierte Funktions-Timeout (maximal 900 Sekunden), je nachdem, welcher Wert höher ist.

Wenn Sie die bereitgestellte Gleichzeitigkeit verwenden, initialisiert Lambda die Ausführungsumgebung, wenn Sie die PC-Einstellungen für eine Funktion konfigurieren. Lambda stellt außerdem sicher, dass initialisierte Ausführungsumgebungen vor Aufrufen immer verfügbar sind. Möglicherweise treten Lücken zwischen den Aufruf- und Initialisierungsphasen Ihrer Funktion auf. Abhängig von der Laufzeit- und Speicherkonfiguration Ihrer Funktion können beim ersten Aufruf in einer initialisierten Ausführungsumgebung auch variable Latenzzeiten auftreten.

Bei Funktionen, die On-Demand-Gleichzeitigkeit nutzen, initialisiert Lambda gelegentlich Ausführungsumgebungen vor Aufrufanfragen. In diesem Fall stellen Sie möglicherweise auch eine Zeitlücke zwischen der Initialisierungs- und der Aufrufphase Ihrer Funktion fest. Wir empfehlen Ihnen, sich nicht von diesem Verhalten abhängig zu machen.

Fehler in der Initialisierungsphase

Wenn eine Funktion in der `Init`-Phase abstürzt oder ein Timeout auftritt, gibt Lambda Fehlerinformationen im `INIT_REPORT`-Protokoll aus.

Example – INIT_REPORT-Protokoll für Timeout

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: timeout
```

Example – INIT_REPORT-Protokoll für den Erweiterungsfehler

```
INIT_REPORT Init Duration: 1236.04 ms Phase: init Status: error Error Type:
 Extension.Crash
```

Wenn die `Init` Phase erfolgreich ist, gibt Lambda das Protokoll nicht aus `INIT_REPORT` — es sei denn, es SnapStartist aktiviert. SnapStart Funktionen senden immer aus. `INIT_REPORT` Weitere Informationen finden Sie unter Überwachung für Lambda SnapStart.

Wiederherstellungsphase (SnapStart nur Lambda)

Wenn Sie eine SnapStartFunktion zum ersten Mal aufrufen und die Funktion skaliert wird, nimmt Lambda neue Ausführungsumgebungen aus dem persistenten Snapshot wieder auf, anstatt die Funktion von Grund auf neu zu initialisieren. Wenn Sie über einen `afterRestore()`-Laufzeit-Hook verfügen, wird der Code am Ende der `Restore`-Phase ausgeführt. Die Dauer von `afterRestore()`-Laufzeit-Hooks wird Ihnen in Rechnung gestellt. Die Laufzeit (JVM) muss geladen werden und `afterRestore()`-Laufzeit-Hooks müssen innerhalb des Timeout-Limits(10 Sekunden) abgeschlossen werden. Andernfalls erhalten Sie eine. SnapStartTimeoutException Wenn die `Restore`-Phase abgeschlossen ist, ruft Lambda den Funktionshandler (Invoke-Phase) auf.

Fehler in der Wiederherstellphase

Wenn die `Restore`-Phase fehlschlägt, gibt Lambda Fehlerinformationen im `RESTORE_REPORT`-Protokoll aus.

Example – RESTORE_REPORT-Protokoll für Timeout

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: timeout
```

Example – RESTORE_REPORT-Protokoll für einen Laufzeit-Hook-Fehler

```
RESTORE_REPORT Restore Duration: 1236.04 ms Status: error Error Type: Runtime.ExitError
```

Weitere Informationen zum `RESTORE_REPORT`-Protokoll finden Sie unter Überwachung für Lambda SnapStart.

Invoke-Phase

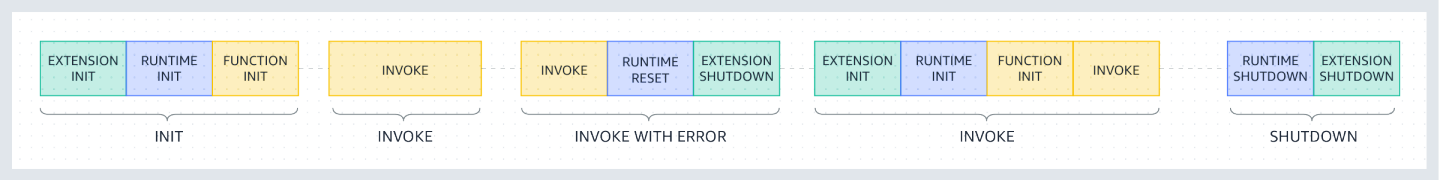
Wenn eine Lambda-Funktion als Antwort auf eine `Next`-API-Anforderung aufgerufen wird, sendet Lambda ein `Invoke`-Ereignis an die Laufzeit und an jede Erweiterung.

Die Timeout-Einstellung der Funktion begrenzt die Dauer der gesamten `Invoke`-Phase. Wenn Sie beispielsweise die Zeitüberschreitung für die Funktion auf 360 Sekunden festlegen, müssen die Funktion und alle Erweiterungen innerhalb von 360 Sekunden abgeschlossen werden. Beachten Sie, dass es keine unabhängige Post-Invoke-Phase gibt. Die Dauer ist die Summe der gesamten Aufrufzeit (Laufzeit + Erweiterungen) und wird erst berechnet, wenn die Funktion und alle Erweiterungen vollständig ausgeführt wurden.

Die Invoke-Phase endet nach der Laufzeit und alle Erweiterungen signalisieren durch Senden einer `Next`-API-Anforderung dass sie abgeschlossen sind.

Fehler während der Aufrufphase

Wenn die Lambda-Funktion während der `Invoke`-Phase abstürzt oder das Zeitlimit überschreitet, setzt Lambda die Ausführungsumgebung zurück. Das folgende Diagramm veranschaulicht das Verhalten der Lambda-Ausführungsumgebung bei einem Aufruffehler:



In folgendem Diagramm:

- Ist die erste Phase die INIT-Phase, die ohne Fehler läuft.
- Ist die zweite Phase die INVOKE-Phase, die ohne Fehler läuft.
- Angenommen, Ihre Funktion tritt zu einem Aufruffehler auf (z. B. ein Funktionstimeout oder einen Laufzeitfehler). Die dritte Phase mit der Bezeichnung INVOKE MIT FEHLER veranschaulicht dieses Szenario. Wenn dies geschieht, führt der Lambda-Service einen Neustart durch. Der Reset verhält sich wie ein `Shutdown`-Ereignis. Zuerst beendet Lambda die Laufzeit und sendet dann ein `Shutdown`-Ereignis an jede registrierte externe Erweiterung. Das Ereignis enthält den Grund für das Abschalten. Wenn diese Umgebung für einen neuen Aufruf verwendet wird, initialisiert Lambda die Erweiterung und die Laufzeit als Teil des nächsten Aufrufers erneut.

> **Note**
>
> Der Lambda-Reset löscht den`/tmp`Verzeichnisinhalt vor der nächsten Init-Phase. Dieses Verhalten stimmt mit der regulären Shutdown-Phase überein.

- Die vierte Phase stellt die INVOKE-Phase unmittelbar nach einem Aufruffehler dar. Hier initialisiert Lambda die Umgebung erneut, indem es die INIT-Phase erneut ausführt. Dies wird als unterdrückte Initialisierung bezeichnet. Wenn unterdrückte Inits auftreten, meldet Lambda nicht explizit eine zusätzliche INIT-Phase in Logs. CloudWatch Stattdessen stellen Sie möglicherweise fest, dass die Dauer in der REPORT-Zeile eine zusätzliche INIT-Dauer plus die INVOKE-Dauer enthält. Nehmen wir zum Beispiel an, Sie sehen die folgenden Protokolle in: CloudWatch

  ```
  2022-12-20T01:00:00.000-08:00 START RequestId: XXX Version: $LATEST
  2022-12-20T01:00:02.500-08:00 END RequestId: XXX
  2022-12-20T01:00:02.500-08:00 REPORT RequestId: XXX Duration: 3022.91 ms
  Billed Duration: 3000 ms Memory Size: 512 MB Max Memory Used: 157 MB
  ```

  In diesem Beispiel beträgt der Unterschied zwischen den Zeitstempeln BERICHT und START 2,5 Sekunden. Dies entspricht nicht der angegebenen Dauer von 3 022,91 Millsekunden, da es die zusätzliche INIT (unterdrückte Initialisierung), die Lambda ausgeführt hat, nicht berücksichtigt. In diesem Beispiel können Sie ableiten, dass die tatsächliche INVOKE-Phase 2,5 Sekunden gedauert hat.

  Für mehr Einblick in dieses Verhalten können Sie die Lambda-Telemetrie-API verwenden. Die Telemetrie-API gibt `INIT_START`, `INIT_RUNTIME_DONE` und `INIT_REPORT`-Ereignisse mit `phase=invoke` immer dann aus, wenn unterdrückte Initialisierungen zwischen den Aufrufphasen auftreten.
- Die fünfte Phase stellt die SHUTDOWN-Phase dar, die fehlerfrei abläuft.

Shutdown-Phase

Wenn Lambda dabei ist, die Laufzeit herunterzufahren, sendet es ein `Shutdown`-Ereignis an jede registrierte externe Erweiterung. Erweiterungen können diese Zeit für abschließende Bereinigungsaufgaben verwenden. Das `Shutdown`-Ereignis ist eine Antwort auf eine `Next`-API-Anforderung.

Duration (Dauer): Die gesamte `Shutdown`-Phase ist auf 2 Sekunden begrenzt. Wenn die Laufzeit oder eine Erweiterung nicht reagiert, beendet Lambda sie über ein Signal (`SIGKILL`).

Nachdem die Funktion und alle Erweiterungen abgeschlossen sind, behält Lambda die Ausführungsumgebung für einige Zeit im Vorgriff auf einen anderen Funktionsaufruf bei. Lambda beendet die Ausführungsumgebungen jedoch alle paar Stunden, um Laufzeitaktualisierungen und Wartungsarbeiten zu ermöglichen — auch für Funktionen, die kontinuierlich aufgerufen werden. Sie

sollten nicht davon ausgehen, dass die Ausführungsumgebung auf unbestimmte Zeit bestehen bleibt. Weitere Informationen finden Sie unter Implementierung von Staatenlosigkeit in Funktionen.

Wenn die Funktion erneut aufgerufen wird, aktiviert Lambda die Umgebung zur wieder zur weiteren Verwendung. Die Wiederverwendung der Ausführungsumgebung hat folgende Auswirkungen:

- Objekte, die außerhalb der Handler-Methode der Funktion deklariert sind, bleiben initialisiert und bieten eine zusätzliche Optimierung, wenn die Funktion erneut aufgerufen wird. Beispiel: Falls Ihre Lambda-Funktion eine Datenbankverbindung herstellt, statt die Verbindung neu herzustellen, wird die ursprüngliche Verbindung bei nachfolgenden Aufrufen verwendet. Wir empfehlen, dass Sie Ihrem Code eine Logik hinzufügen, um zu prüfen, ob eine Verbindung besteht, bevor Sie eine neue erstellen.
- Jede Ausführungsumgebung stellt Speicherplatz von 512 MB bis 10 240 MB, in 1-MB-Schritten, im Verzeichnis `/tmp` zur Verfügung. Der Inhalt des Verzeichnisses bleibt bestehen, wenn die Ausführungsumgebung eingefroren ist, und bietet einen temporären Zwischenspeicher, der für mehrere Aufrufe verwendet werden kann. Sie können zusätzlichen Code hinzufügen, um zu prüfen, ob der Cache die gespeicherten Daten enthält. Weitere Informationen zu Beschränkungen der Bereitstellungsgröße finden Sie unter Lambda-Kontingente.
- Hintergrundprozesse oder Callbacks, die von Ihrer Lambda-Funktion initiiert wurden und nicht abgeschlossen wurden, wenn die Funktion beendet wurde, werden wieder aufgenommen, wenn Lambda die Ausführungsumgebung wiederverwendet. Sie sollten sicherstellen, dass alle Hintergrundprozesse oder Callbacks in Ihrem Code abgeschlossen sind, bevor der Code beendet wird.

Implementierung von Staatenlosigkeit in Funktionen

Wenn Sie Ihren Lambda-Funktionscode schreiben, behandeln Sie die Ausführungsumgebung als zustandslos und gehen Sie davon aus, dass sie nur für einen einzigen Aufruf existiert. Lambda beendet Ausführungsumgebungen alle paar Stunden, um Laufzeitaktualisierungen und Wartungsarbeiten zu ermöglichen — auch für Funktionen, die kontinuierlich aufgerufen werden. Initialisieren Sie jeden erforderlichen Status (z. B. das Abrufen eines Einkaufswagens aus einer Amazon DynamoDB-Tabelle), wenn Ihre Funktion gestartet wird. Übernehmen Sie vor dem Beenden permanente Datenänderungen in dauerhafte Speicher wie Amazon Simple Storage Service (Amazon S3), DynamoDB oder Amazon Simple Queue Service (Amazon SQS). Verlassen Sie sich nicht auf bestehende Datenstrukturen, temporäre Dateien oder Zustände, die sich über mehrere Aufrufe erstrecken, wie Zähler oder Aggregate. Dadurch wird sichergestellt, dass Ihre Funktion jeden Aufruf unabhängig verarbeitet.

Lambda-Bereitstellungspakete

Der Code Ihrer AWS Lambda Funktion besteht aus Skripten oder kompilierten Programmen und deren Abhängigkeiten. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Lambda unterstützt zwei Arten von Bereitstellungspaketen: Container-Images und ZIP-Dateiarchiven.

Themen

Container-Images

Ein Container-Image enthält das Basisbetriebssystem, die Laufzeit, Lambda-Erweiterungen, Ihren Anwendungscode und seine Abhängigkeiten. Sie können dem Image auch statische Daten wie Modelle für Machine Learning hinzufügen.

Lambda bietet eine Reihe von Open-Source-Basis-Images, mit denen Sie Ihr Container-Image erstellen können. Um Container-Images zu erstellen und zu testen, können Sie die Befehlszeilenschnittstelle AWS Serverless Application Model (AWS SAM CLI) () oder native Container-Tools wie die Docker-CLI verwenden.

Laden Sie Ihre Container-Images in Amazon Elastic Container Registry (Amazon ECR) hoch, einen verwalteten AWS Container-Image-Registry-Service. Um das Image für Ihre Funktion bereitzustellen, geben Sie die Amazon ECR-Image-URL mithilfe der Lambda-Konsole, der Lambda-API, der Befehlszeilentools oder der SDKs an. AWS

Weitere Informationen zu Lambda-Container-Images finden Sie im Abschnitt Erstellen Sie eine Lambda-Funktion mit einem Container-Image.

ZIP-Dateiarchive

Ein ZIP-Dateiarchiv enthält Ihren Anwendungscode und seine Abhängigkeiten. Wenn Sie Funktionen mit der Lambda-Konsole oder einem Toolkit erstellen, erstellt Lambda automatisch ein ZIP-Dateiarchiv Ihres Codes.

Wenn Sie Funktionen mit der Lambda-API, Befehlszeilentools oder den AWS SDKs erstellen, müssen Sie ein Bereitstellungspaket erstellen. Sie müssen auch ein Bereitstellungspaket erstellen, wenn Ihre Funktion eine kompilierte Sprache verwendet, oder um Ihrer Funktion Abhängigkeiten hinzuzufügen. Um den Code Ihrer Funktion bereitzustellen, laden Sie das Bereitstellungspaket von Amazon Simple Storage Service (Amazon S3) oder Ihrem lokalen Computer hoch.

Sie können mit der Lambda-Konsole AWS Command Line Interface (AWS CLI) eine ZIP-Datei als Bereitstellungspaket oder in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochladen.

Verwenden von Lambda-Konsole

Die folgenden Schritte veranschaulichen, wie Sie eine ZIP-Datei mithilfe der Lambda-Konsole als Bereitstellungspaket hochladen.

So laden Sie eine ZIP-Datei auf die Lambda-Konsole hoch

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie im Bereich Quellcode die Option Upload von und dann ZIP-Datei aus.
4. Wählen Sie Upload (Hochladen) aus, um Ihre lokale ZIP-Datei auszuwählen.
5. Wählen Sie Save aus.

Mit dem AWS CLI

Mithilfe von AWS Command Line Interface (AWS CLI) können Sie eine ZIP-Datei als Bereitstellungspaket hochladen. Sprachenspezifische Anweisungen finden Sie in den folgenden Themen:

Node.js

- Bereitstellen von Node.js Lambda-Funktionen mit ZIP-Dateiarchiven

Python

- Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen

Ruby

- Arbeiten mit ZIP-Dateiarchiven für Ruby-Lambda-Funktionen

Java

Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven

Go

Bereitstellen von Lambda-Go-Funktionen mit ZIP-Dateiarchiven

C#

Erstellen und Bereitstellen von C#-Lambda-Funktionen mit ZIP-Dateiarchiven

PowerShell

Bereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven

Verwenden von Amazon S3

Sie können mit Amazon Simple Storage Service (Amazon S3) eine ZIP-Datei als Bereitstellungspaket hochladen. Weitere Informationen finden Sie unter .

Ebenen

Wenn Sie Ihren Funktionscode mit einem ZIP-Dateiarchiv bereitstellen, können Sie Lambda-Ebenen als Verteilungsmechanismus für Bibliotheken, benutzerdefinierte Laufzeiten und andere Funktionsabhängigkeiten verwenden. Mit Ebenen können Sie Ihren in der Entwicklung befindlichen Funktionscode unabhängig von dem unveränderlichen Code sowie den Ressourcen, die er verwendet, verwalten. Sie können Ihre Funktion so konfigurieren, dass von Ihnen erstellte Ebenen, bereitgestellte Ebenen oder Ebenen von anderen AWS Kunden verwendet werden. AWS

Sie können Ebenen nicht mit Container-Bildern verwenden. Verpacken Sie stattdessen Ihre bevorzugte Laufzeit, Bibliotheken und andere Abhängigkeiten in das Container-Image, wenn Sie das Image erstellen.

(Weitere Informationen über Ebenen finden Sie unter Lambda-Ebenen.

Verwenden Sie andere AWS Dienste, um ein Bereitstellungspaket zu erstellen

Im folgenden Abschnitt werden andere AWS Dienste beschrieben, die Sie verwenden können, um Abhängigkeiten für Ihre Lambda-Funktion zu verpacken.

Bereitstellungspakete mit C- oder C++-Bibliotheken

Wenn Ihr Bereitstellungspaket systemeigene Bibliotheken enthält, können Sie das Bereitstellungspaket mit AWS Serverless Application Model (AWS SAM) erstellen. Sie können den AWS SAM `sam build` CLI-Befehl mit dem verwenden`--use-container`, um Ihr Bereitstellungspaket zu erstellen. Diese Option erstellt ein Bereitstellungspaket in einem Docker-Image, das mit der Lambda-Ausführungsumgebung kompatibel ist.

Weitere Informationen finden Sie unter SAM-Entwicklung im AWS Serverless Application Model - Entwicklerhandbuch.

Bereitstellungspakete über 50 MB

Wenn Ihr Bereitstellungspaket größer als 50 MB ist, laden Sie Ihren Funktionscode und Ihre Abhängigkeiten in einen Amazon-S3-Bucket hoch.

Sie können ein Bereitstellungspaket erstellen und die ZIP-Datei in Ihren Amazon S3 S3-Bucket in der AWS Region hochladen, in der Sie eine Lambda-Funktion erstellen möchten. Geben Sie beim Erstellen Ihrer Lambda-Funktion den S3-Bucket-Namen und den Objektschlüsselnamen in der Lambda-Konsole an oder verwenden Sie die AWS CLI.

Informationen zum Erstellen eines Buckets mit der Amazon S3 S3-Konsole finden Sie unter Bucket erstellen im Amazon Simple Storage Service-Benutzerhandbuch.

Verwenden von Lambda mit Infrastructure as Code (IaC)

Lambda bietet verschiedene Möglichkeiten, Ihren Code bereitzustellen und Funktionen zu erstellen. Sie können beispielsweise die Lambda-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden, um Lambda-Funktionen manuell zu erstellen oder zu aktualisieren. Zusätzlich zu diesen manuellen Optionen bietet AWS eine Reihe von Lösungen für die Bereitstellung von Lambda-Funktionen und Serverless-Anwendungen mithilfe von Infrastructure as Code (IaC). Mit IaC können Sie Lambda-Funktionen und andere AWS-Ressourcen mithilfe von Code bereitstellen und verwalten, anstatt manuelle Prozesse und Einstellungen zu verwenden.

In den meisten Fällen werden Lambda-Funktionen nicht isoliert ausgeführt. Stattdessen sind sie Teil einer Serverless-Anwendung, zu der auch andere Ressourcen wie Datenbanken, Warteschlangen und Speicher gehören. Mit IaC können Sie Ihre Bereitstellungsprozesse automatisieren, um ganze Serverless-Anwendungen mit vielen separaten AWS-Ressourcen schnell und wiederholbar bereitzustellen und zu aktualisieren. Dieser Ansatz beschleunigt Ihren Entwicklungszyklus, erleichtert die Konfigurationsverwaltung und stellt sicher, dass Ihre Ressourcen jedes Mal auf die gleiche Weise bereitgestellt werden.

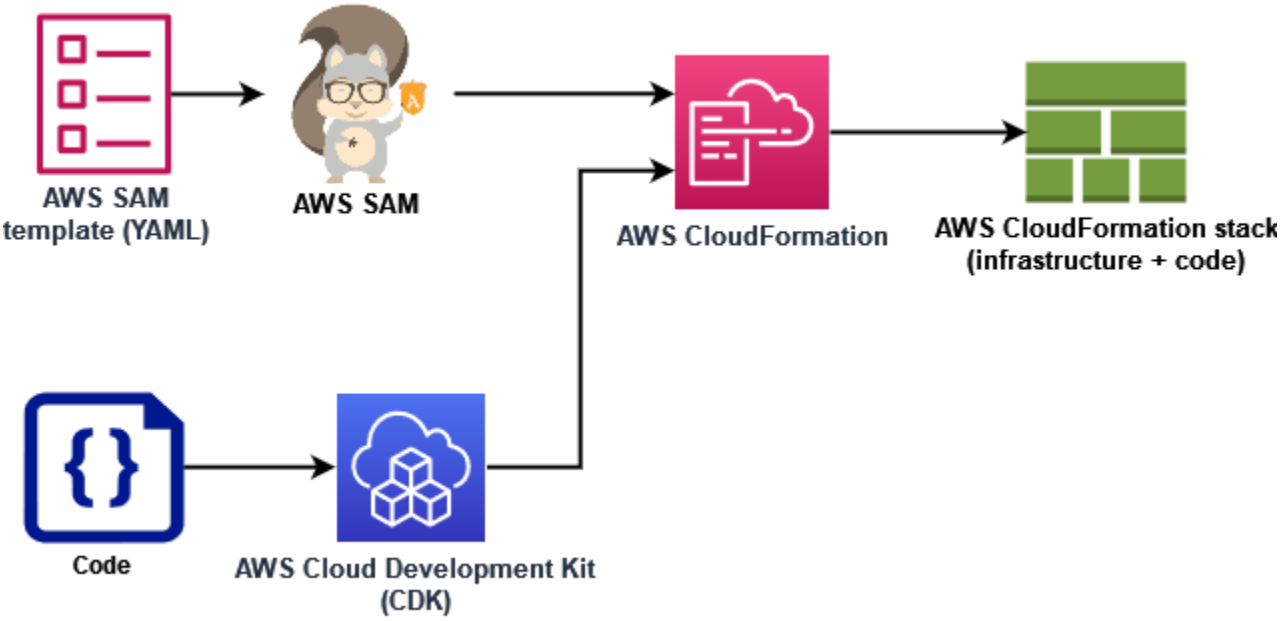
Themen

IaC-Tools für Lambda

Um Lambda-Funktionen und Serverless-Anwendungen mithilfe von IaC bereitzustellen, bietet AWS eine Reihe verschiedener Tools und Services.

AWS CloudFormation war der erste Service, der von AWS zur Erstellung und Konfiguration von Cloud-Ressourcen angeboten wurde. Mit AWS CloudFormation erstellen Sie Textvorlagen zur Definition von Infrastruktur und Code. Als in AWS immer mehr neue Services eingeführt wurden und die Erstellung von AWS CloudFormation-Vorlagen immer komplexer wurde, wurden zwei weitere Tools veröffentlicht. AWS SAM ist ein weiteres auf Vorlagen basierendes Framework zur Definition von Serverless-Anwendungen. Bei AWS Cloud Development Kit (AWS CDK) handelt es sich um einen Ansatz, bei dem der Code an erster Stelle steht, um Infrastruktur mithilfe von Code-Konstrukten in vielen gängigen Programmiersprachen zu definieren und bereitzustellen.

Mit sowohl AWS SAM als auch AWS CDK arbeitet AWS CloudFormation im Hintergrund, um Ihre Infrastruktur aufzubauen und bereitzustellen. Die folgende Abbildung veranschaulicht die Beziehung zwischen diesen Tools und in den Absätzen nach dem Diagramm werden ihre wichtigsten Funktionen erläutert.



- AWS CloudFormation – Wenn CloudFormation Sie Ihre AWS Ressourcen mithilfe einer YAML- oder JSON-Vorlage modellieren und einrichten, die Ihre Ressourcen und deren Eigenschaften beschreibt. CloudFormation stellt Ihre Ressourcen auf sichere, wiederholbare Weise bereit, sodass Sie Ihre Infrastruktur und Anwendungen häufig ohne manuelle Schritte erstellen können. Wenn Sie die Konfiguration ändern, CloudFormation bestimmt die richtigen Operationen, die zum Aktualisieren Ihres Stacks ausgeführt werden sollen. CloudFormation kann Änderungen sogar rückgängig machen.
- AWS Serverless Application Model (AWS SAM) – AWS SAM ist ein Open-Source-Framework für die Definition von Serverless-Anwendungen. In den AWS SAM-Vorlagen wird eine Kurzsyntax verwendet, um Funktionen, APIs, Datenbanken und Zuordnungen von Ereignisquellen mit nur wenigen Textzeilen (YAML) pro Ressource zu definieren. Während der Bereitstellung transformiert und erweitert AWS SAM die AWS SAM-Syntax in eine AWS CloudFormation-Syntax. Aus diesem Grund kann jede CloudFormation Syntax zu AWS SAM Vorlagen hinzugefügt werden. Dies bietet die AWS SAM volle Leistung von CloudFormation, jedoch mit weniger Konfigurationszeilen.
- AWS Cloud Development Kit (AWS CDK) – Mit der definieren AWS CDKSie Ihre Infrastruktur mithilfe von Codekonstrukten und stellen sie über bereitAWS CloudFormation. AWS CDK ermöglicht es Ihnen, die Anwendungsinfrastruktur mit TypeScript, Python, Java, .NET und Go

(in der Entwicklervorschau) mithilfe Ihrer vorhandenen IDE, Testtools und Workflow-Muster zu modellieren. Sie erhalten alle Vorteile von AWS CloudFormation, einschließlich wiederholbarer Bereitstellung, einfachem Rollback und Erkennung von Abweichungen.

AWS bietet außerdem einen Service namens AWS Application Composer zur Entwicklung von IaC-Vorlagen mithilfe einer einfachen grafischen Oberfläche. Mit Application Composer entwerfen Sie eine Anwendungsarchitektur, indem Sie AWS-Services auf einer visuellen Zeichenfläche ziehen, gruppieren und verbinden. Application Composer erstellt dann eine AWS SAM-Vorlage oder eine AWS CloudFormation-Vorlage aus Ihrem Entwurf, die Sie zur Bereitstellung Ihrer Anwendung verwenden können.

Im folgenden Abschnitt the section called “Erste Schritte mit IaC für Lambda” verwenden Sie Application Composer, um eine Vorlage für eine Serverless-Anwendung zu entwickeln, die auf einer vorhandenen Lambda-Funktion basiert.

Erste Schritte mit IaC für Lambda

In diesem Tutorial können Sie mit der Verwendung von IaC mit Lambda beginnen, indem Sie eine AWS SAM-Vorlage aus einer vorhandenen Lambda-Funktion erstellen und dann eine Serverless-Anwendung in Application Composer erstellen, indem Sie weitere AWS-Ressourcen hinzufügen.

Wenn Sie lieber mit einem AWS SAM- oder AWS CloudFormation-Tutorial beginnen möchten, um zu lernen, wie Sie mit Vorlagen arbeiten können, ohne Application Composer zu verwenden, finden Sie im Abschnitt the section called “Nächste Schritte” am Ende dieser Seite Links zu anderen Ressourcen.

Während Sie dieses Tutorial durchführen, lernen Sie einige grundlegende Konzepte kennen, z. B. wie AWS-Ressourcen in AWS SAM angegeben werden. Zudem erfahren Sie, wie Sie mit Application Composer eine Serverless-Anwendung erstellen, die Sie mit AWS SAM oder AWS CloudFormation bereitstellen können.

Führen Sie für dieses Tutorial die folgenden Schritte aus:

- Erstellen Sie eine Beispiel-Lambda-Funktion.
- Verwenden Sie die Lambda-Konsole, um die AWS SAM-Vorlage für die Funktion anzuzeigen.
- Exportieren Sie die Konfiguration Ihrer Funktion nach AWS Application Composer und entwerfen Sie eine einfache Serverless-Anwendung, die auf der Konfiguration Ihrer Funktion basiert.

- Speichern Sie eine aktualisierte AWS SAM-Vorlage, die Sie als Grundlage für die Bereitstellung Ihrer Serverless-Anwendung verwenden können.

Im Abschnitt the section called “Nächste Schritte” finden Sie Ressourcen, mit denen Sie mehr über AWS SAM und Application Composer erfahren können. Diese Ressourcen enthalten Links zu Tutorials für Fortgeschrittene, in denen Sie lernen, wie Sie eine Serverless-Anwendung mit AWS SAM bereitstellen.

Voraussetzungen

In diesem Tutorial verwenden Sie die Funktion für die lokale Synchronisierung von Application Composer, um Ihre Vorlagen- und Codedateien auf Ihrem lokalen Build-Computer zu speichern. Um diese Funktion nutzen zu können, benötigen Sie einen Browser, der die File System Access-API unterstützt. Damit können Webanwendungen Dateien in Ihrem lokalen Dateisystem lesen, schreiben und speichern. Wir empfehlen, entweder Google Chrome oder Microsoft Edge zu verwenden. Weitere Informationen zur File System Access-API finden Sie unter Was ist die File System Access-API?.

Erstellen einer Lambda-Funktion

In diesem ersten Schritt erstellen Sie eine Lambda-Funktion, mit der Sie den Rest des Tutorials abschließen können. Der Einfachheit halber verwenden Sie die Lambda-Konsole, um mithilfe der Python 3.11-Laufzeit eine grundlegende „Hello World“-Funktion zu erstellen.

So erstellen Sie eine „Hello World“-Lambda-Funktion mit der Konsole

1. Öffnen Sie die Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Lassen Sie Ohne Vorgabe erstellen ausgewählt. Geben Sie im Feld Grundlegende Informationen für Funktionsname **`LambdaIaCDemo`** ein.
4. Wählen Sie für Laufzeit die Option Python 3.11 aus.
5. Wählen Sie Funktion erstellen.

Sehen Sie sich die AWS SAM-Vorlage für Ihre Funktion an.

Bevor Sie die Konfiguration Ihrer Funktion nach Application Composer exportieren, verwenden Sie die Lambda-Konsole, um die aktuelle Konfiguration Ihrer Funktion als AWS SAM-Vorlage

anzuzeigen. Wenn Sie die Schritte in diesem Abschnitt befolgen, erfahren Sie mehr über den Aufbau einer AWS SAM-Vorlage und darüber, wie Sie Ressourcen wie Lambda-Funktionen definieren, um mit der Spezifizierung einer Serverless-Anwendung zu beginnen.

So sehen Sie sich die AWS SAM-Vorlage für Ihre Funktion an

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie gerade erstellt haben (`LambdaIaCDemo`).
3. Wählen Sie im Bereich Funktionsübersicht die Option Vorlage.

   Anstelle des Diagramms, das die Konfiguration Ihrer Funktion darstellt, wird eine AWS SAM-Vorlage für Ihre Funktion angezeigt. Die Vorlage sollte jetzt wie folgt aussehen:

```
# This AWS SAM template has been generated from your function's
# configuration. If your function has one or more triggers, note
# that the AWS resources associated with these triggers aren't fully
# specified in this template and include placeholder values.Open this template
# in AWS Application Composer or your favorite IDE and modify
# it to specify a serverless application with other AWS resources.
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
        MaximumRetryAttempts: 2
      EphemeralStorage:
        Size: 512
      RuntimeManagementConfig:
        UpdateRuntimeOn: Auto
      SnapStart:
```

```
        ApplyOn: None
      PackageType: Zip
      Policies:
        Statement:
          - Effect: Allow
            Action:
              - logs:CreateLogGroup
            Resource: arn:aws:logs:us-east-1:123456789012:*
          - Effect: Allow
            Action:
              - logs:CreateLogStream
              - logs:PutLogEvents
            Resource:
              - >-
                arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
LambdaIaCDemo:*
```

Nehmen wir uns einen Moment Zeit, um uns die YAML-Vorlage für Ihre Funktion anzusehen und einige wichtige Konzepte zu verstehen.

Die Vorlage beginnt mit der Deklaration `Transform: AWS::Serverless-2016-10-31`. Diese Deklaration ist erforderlich, weil im Hintergrund AWS SAM-Vorlagen über AWS CloudFormation bereitgestellt werden. Mithilfe der `Transform`-Anweisung wird die Vorlage als AWS SAM-Vorlagendatei identifiziert.

Nach der `Transform`-Deklaration folgt der `Resources`-Abschnitt. Hier werden die AWS-Ressourcen definiert, die Sie mit Ihrer AWS SAM-Vorlage bereitstellen möchten. AWS SAM-Vorlagen können eine Kombination aus AWS SAM-Ressourcen und AWS CloudFormation-Ressourcen enthalten. Das liegt daran, dass AWS SAM-Vorlagen bei der Bereitstellung zu AWS CloudFormation-Vorlagen erweitert werden, sodass jeder AWS SAM-Vorlage jede gültige AWS CloudFormation-Syntax hinzugefügt werden kann.

Im Moment ist im Abschnitt `Resources` der Vorlage nur eine Ressource definiert, Ihre Lambda-Funktion `LambdaIaCDemo`. Um einer AWS SAM-Vorlage eine Lambda-Funktion hinzuzufügen, verwenden Sie den `AWS::Serverless::Function`-Ressourcentyp. Die `Properties` der Ressource einer Lambda-Funktion definieren die Laufzeit, den Funktionshandler und andere Konfigurationsoptionen der Funktion. Der Pfad zum Quellcode Ihrer Funktion, den AWS SAM für die Bereitstellung der Funktion verwenden soll, ist hier ebenfalls definiert. Weitere Informationen zu Lambda-Funktionsressourcen in finden Sie AWS SAMunter AWS::Serverless::Function im AWS SAM -Entwicklerhandbuch.

Neben den Funktionseigenschaften und Konfigurationen ist in der Vorlage auch eine AWS Identity and Access Management-Richtlinie (IAM) für Ihre Funktion angegeben. Diese Richtlinie erteilt Ihrer Funktion die Berechtigung, Protokolle in Amazon CloudWatch Logs zu schreiben. Wenn Sie eine Funktion in der Lambda-Konsole erstellen, hängt Lambda diese Richtlinie automatisch an Ihre Funktion an. Weitere Informationen zum Angeben einer IAM-Richtlinie für eine Funktion in einer -AWS SAMVorlage finden Sie in der -`policies`Eigenschaft auf der -AWS::Serverless::FunctionSeite des AWS SAM -Entwicklerhandbuchs.

Weitere Informationen zur Struktur von AWS SAM-Vorlagen finden Sie unter AWS SAM-Vorlagenaufbau.

Verwenden von AWS Application Composer zum Entwerfen einer Serverless-Anwendung

Um mit der Erstellung einer einfachen Serverless-Anwendung zu beginnen, die die AWS SAM-Vorlage Ihrer Funktion als Ausgangspunkt verwendet, exportieren Sie Ihre Funktionskonfiguration nach Application Composer und aktivieren den lokalen Synchronisierungsmodus von Application Composer. Die Funktion für die lokale Synchronisierung speichert den Code Ihrer Funktion und Ihre AWS SAM-Vorlage automatisch auf Ihrem lokalen Build-Computer und sorgt dafür, dass Ihre gespeicherte Vorlage synchronisiert wird, wenn Sie weitere AWS-Ressourcen in Application Composer hinzufügen.

So exportieren Sie Ihre Funktion nach Application Composer

1. Wählen Sie im Bereich Funktionsübersicht die Option Nach Application Composer exportieren aus.

   Um die Konfiguration und den Code Ihrer Funktion nach Application Composer zu exportieren, erstellt Lambda einen Amazon-S3-Bucket in Ihrem Konto, um diese Daten vorübergehend zu speichern.
2. Wählen Sie im Dialogfeld Projekt bestätigen und erstellen aus, um den Standardnamen für diesen Bucket zu akzeptieren und die Konfiguration und den Code Ihrer Funktion nach Application Composer zu exportieren.
3. (Optional) Um einen anderen Namen für den von Lambda erstellten Amazon-S3-Bucket auszuwählen, geben Sie einen neuen Namen ein und wählen Sie Projekt bestätigen und erstellen aus. Die Amazon-S3-Bucket-Namen müssen global eindeutig sein und den Regeln für die Benennung von Buckets entsprechen.

Wenn Sie Projekt bestätigen und erstellen auswählen, wird die Application-Composer-Konsole geöffnet. Auf der Zeichenfläche sehen Sie Ihre Lambda-Funktion.

4. Wählen Sie in der Menü-Dropdown-Liste die Option Lokale Synchronisierung aktivieren aus.
5. Wählen Sie in dem sich öffnenden Dialogfeld die Option Ordner auswählen aus und wählen Sie einen Ordner auf Ihrem lokalen Build-Computer aus.
6. Wählen Sie Aktivieren aus, um die lokale Synchronisierung zu aktivieren.

Zum Exportieren Ihrer Funktion nach Application Composer benötigen Sie die Berechtigung zur Verwendung von bestimmten API-Aktionen. Wenn Sie Ihre Funktion nicht exportieren können, beachten Sie the section called “Erforderliche Berechtigungen” und stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen.

> **Note**
>
> Für den Bucket, den Lambda erstellt, wenn Sie eine Funktion nach Application Composer exportieren, gelten die Amazon-S3-Standardpreise. Die Objekte, die Lambda in den Bucket einfügt, werden nach 10 Tagen automatisch gelöscht, aber Lambda löscht den Bucket selbst nicht.
> Folgen Sie den Anweisungen unter Löschen eines Buckets, nachdem Sie Ihre Funktion nach Application Composer exportiert haben, um zu vermeiden, dass für Ihr AWS-Konto zusätzliche Kosten anfallen. Weitere Informationen zum Amazon-S3-Bucket-Namen, den Lamda erstellt, finden Sie unter the section called “Application Composer”.

So entwerfen Sie Ihre Serverless-Anwendung in Application Composer

Nach der Aktivierung der lokalen Synchronisierung werden die Änderungen, die Sie in Application Composer vornehmen, in der AWS SAM-Vorlage widergespiegelt, die auf Ihrer lokalen Build-Maschine gespeichert ist. Sie können jetzt zusätzliche AWS-Ressourcen per Drag-and-Drop auf die Application-Composer-Zeichenfläche ziehen, um Ihre Anwendung zu erstellen. In diesem Beispiel fügen Sie eine einfache Amazon-SQS-Warteschlange als Trigger für Ihre Lambda-Funktion und eine DynamoDB-Tabelle für die Funktion hinzu, in die Daten geschrieben werden sollen.

1. Fügen Sie Ihrer Lambda-Funktion einen Amazon-SQS-Trigger hinzu, indem Sie wie folgt vorgehen:

   a. Geben Sie im Suchfeld in der Ressourcenpalette **SQS** ein.

   b. Ziehen Sie die Ressource SQS-Warteschlange auf Ihre Zeichenfläche und positionieren Sie sie links neben Ihrer Lambda-Funktion.

   c. Wählen Sie Details und geben Sie **`LambdaIaCQueue`** als Logische ID ein.

   d. Wählen Sie Speichern.

   e. Verbinden Sie Ihre Amazon-SQS- und Lambda-Ressourcen, indem Sie auf der SQS-Warteschlangenkarte auf den Port Abonnement klicken und ihn auf den linken Port auf der Lambda-Funktionskarte ziehen. Das Erscheinen einer Linie zwischen den beiden Ressourcen weist auf eine erfolgreiche Verbindung hin. Application Composer zeigt außerdem unten auf der Zeichenfläche eine Meldung an, die darauf hinweist, dass die beiden Ressourcen erfolgreich verbunden wurden.

2. Fügen Sie eine Amazon-DynamoDB-Tabelle für Ihre Lambda-Funktion hinzu, in die Daten geschrieben werden sollen, indem Sie so vorgehen:

   a. Geben Sie im Suchfeld in der Ressourcenpalette **`DynamoDB`** ein.

   b. Ziehen Sie die Ressource DynamoDB-Tabelle auf Ihre Zeichenfläche und positionieren Sie sie rechts neben Ihrer Lambda-Funktion.

   c. Wählen Sie Details und geben Sie **`LambdaIaCTable`** als Logische ID ein.

   d. Wählen Sie Speichern.

   e. Verbinden Sie die DynamoDB-Tabelle mit Ihrer Lambda-Funktion, indem Sie auf den rechten Port der Lambda-Funktionskarte klicken und ihn auf den linken Port der DynamoDB-Karte ziehen.

Nachdem Sie diese zusätzlichen Ressourcen hinzugefügt haben, werfen wir einen Blick auf die aktualisierte AWS SAM-Vorlage, die Application Composer erstellt hat.

So zeigen Sie Ihre aktualisierte AWS SAM-Vorlage an

- Wählen Sie auf der Application-Composer-Zeichenfläche Vorlage, um von der Zeichenflächenansicht zur Vorlagenansicht zu wechseln.

Ihre AWS SAM-Vorlage sollte jetzt die folgenden zusätzlichen Ressourcen und Eigenschaften enthalten:

- Eine Amazon-SQS-Warteschlange mit der ID `LambdaIaCQueue`

```
LambdaIaCQueue:
    Type: AWS::SQS::Queue
    Properties:
      MessageRetentionPeriod: 345600
```

Wenn Sie mit Application Composer eine Amazon-SQS-Warteschlange hinzufügen, legt Application Composer die `MessageRetentionPeriod`-Eigenschaft fest. Sie können die `FifoQueue`-Eigenschaft auch festlegen, indem Sie auf der SQS-Warteschlangenkarte Details auswählen und die Fifo-Warteschlange aktivieren oder deaktivieren.

Um weitere Eigenschaften für Ihre Warteschlange festzulegen, können Sie die Vorlage manuell bearbeiten, um sie hinzuzufügen. Weitere Informationen zur `AWS::SQS::Queue`-Ressource und ihre verfügbaren Eigenschaften finden Sie unter AWS::SQS::Queue im AWS CloudFormation-Benutzerhandbuch.

- Eine `Events`-Eigenschaft in Ihrer Lambda-Funktionsdefinition, die die Amazon-SQS-Warteschlange als Trigger für die Funktion angibt

```
Events:
  LambdaIaCQueue:
    Type: SQS
    Properties:
      Queue: !GetAtt LambdaIaCQueue.Arn
      BatchSize: 1
```

Die `Events`-Eigenschaft besteht aus einem Ereignistyp und einer Reihe von Eigenschaften, die vom Typ abhängen. Weitere Informationen zu den verschiedenen , die AWS-Services Sie konfigurieren können, um eine Lambda-Funktion auszulösen, und zu den Eigenschaften, die Sie festlegen können, finden Sie EventSource unter im AWS SAM -Entwicklerhandbuch.

- Eine DynamoDB-Tabelle mit dem Bezeichner `LambdaIaCTable`

```
LambdaIaCTable:
    Type: AWS::DynamoDB::Table
    Properties:
      AttributeDefinitions:
        - AttributeName: id
          AttributeType: S
      BillingMode: PAY_PER_REQUEST
      KeySchema:
```

```
        - AttributeName: id
          KeyType: HASH
      StreamSpecification:
        StreamViewType: NEW_AND_OLD_IMAGES
```

Wenn Sie mit Application Composer eine DynamoDB-Tabelle hinzufügen, können Sie die Schlüssel Ihrer Tabelle festlegen, indem Sie auf der DynamoDB-Tabellenkarte Details auswählen und die Schlüsselwerte bearbeiten. Application Composer legt auch Standardwerte für eine Reihe anderer Eigenschaften fest, darunter `BillingMode` und `StreamViewType`.

Weitere Informationen zu diesen und anderen Eigenschaften, die Sie Ihrer AWS SAM-Vorlage hinzufügen können, finden Sie unter AWS::DynamoDB::Table im AWS CloudFormation-Benutzerhandbuch.

- Eine neue IAM-Richtlinie, die Ihrer Funktion die Berechtigung gewährt, CRUD-Operationen für die von Ihnen hinzugefügte DynamoDB-Tabelle auszuführen.

```
Policies:
...
  - DynamoDBCrudPolicy:
    TableName: !Ref LambdaIaCTable
```

Die endgültige vollständige AWS SAM-Vorlage sollte jetzt so aussehen:

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Specification template describing your function.
Resources:
  LambdaIaCDemo:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 3
      Handler: lambda_function.lambda_handler
      Runtime: python3.11
      Architectures:
        - x86_64
      EventInvokeConfig:
        MaximumEventAgeInSeconds: 21600
```

```
        MaximumRetryAttempts: 2
      EphemeralStorage:
        Size: 512
      RuntimeManagementConfig:
        UpdateRuntimeOn: Auto
      SnapStart:
        ApplyOn: None
      PackageType: Zip
      Policies:
        - Statement:
            - Effect: Allow
              Action:
                - logs:CreateLogGroup
              Resource: arn:aws:logs:us-east-1:594035263019:*
            - Effect: Allow
              Action:
                - logs:CreateLogStream
                - logs:PutLogEvents
              Resource:
                - arn:aws:logs:us-east-1:594035263019:log-group:/aws/lambda/
LambdaIaCDemo:*
        - DynamoDBCrudPolicy:
            TableName: !Ref LambdaIaCTable
      Events:
        LambdaIaCQueue:
          Type: SQS
          Properties:
            Queue: !GetAtt LambdaIaCQueue.Arn
            BatchSize: 1
      Environment:
        Variables:
          LAMBDAIACTABLE_TABLE_NAME: !Ref LambdaIaCTable
          LAMBDAIACTABLE_TABLE_ARN: !GetAtt LambdaIaCTable.Arn
  LambdaIaCQueue:
    Type: AWS::SQS::Queue
    Properties:
      MessageRetentionPeriod: 345600
  LambdaIaCTable:
    Type: AWS::DynamoDB::Table
    Properties:
      AttributeDefinitions:
        - AttributeName: id
          AttributeType: S
      BillingMode: PAY_PER_REQUEST
```

```
      KeySchema:
        - AttributeName: id
          KeyType: HASH
      StreamSpecification:
        StreamViewType: NEW_AND_OLD_IMAGES
```

Stellen Sie Ihre Serverless-Anwendung mithilfe von AWS SAM (optional) bereit

Wenn Sie AWS SAM verwenden möchten, um eine Serverless-Anwendung mithilfe der Vorlage bereitzustellen, die Sie gerade in Application Composer erstellt haben, müssen Sie zuerst die AWS SAM-CLI installieren. Befolgen Sie hierzu die Anweisungen unter Installieren der AWS SAM-CLI.

Bevor Sie Ihre Anwendung bereitstellen, müssen Sie auch den Funktionscode aktualisieren, den Application Composer zusammen mit Ihrer Vorlage gespeichert hat. Derzeit enthält die von Application Composer gespeicherte `lambda_function.py`-Datei nur den grundlegenden „Hello World“-Code, den Lambda bei der Erstellung der Funktion bereitgestellt hat.

Um Ihren Funktionscode zu aktualisieren, kopieren Sie den folgenden Code und fügen Sie ihn in die `lambda_function.py`-Datei ein, die Application Composer auf Ihrer lokalen Build-Maschine gespeichert hat. Sie haben das Verzeichnis, in dem Application Composer diese Datei speichern soll, beim Aktivieren des Modus „Lokale Synchronisation“ angegeben.

Dieser Code akzeptiert ein Schlüssel-Wert-Paar in einer Nachricht von der Amazon-SQS-Warteschlange, die Sie in Application Composer erstellt haben. Wenn sowohl der Schlüssel als auch der Wert Zeichenfolgen sind, verwendet der Code diese Werte, um ein Element in die in Ihrer Vorlage definierte DynamoDB-Tabelle zu schreiben.

Aktualisierter Python-Funktionscode

```
import boto3
import os
import json

# define the DynamoDB table that Lambda will connect to
tablename = os.environ['LAMBDAIACTABLE_TABLE_NAME']

# create the DynamoDB resource
dynamo = boto3.client('dynamodb')

def lambda_handler(event, context):
    # get the message out of the SQS event
    message = event['Records'][0]['body']
```

```
    data = json.loads(message)
    # write event data to DDB table
    if check_message_format(data):
        key = next(iter(data))
        value = data[key]
        dynamo.put_item(
            TableName=tablename,
            Item={
                'id': {'S': key},
                'Value': {'S': value}
            }
        )
    else:
        raise ValueError("Input data not in the correct format")

# check that the event object contains a single key value
# pair that can be written to the database
def check_message_format(message):
    if len(message) != 1:
        return False

    key, value = next(iter(message.items()))

    if not (isinstance(key, str) and isinstance(value, str)):
        return False

    else:
        return True
```

So stellen Sie Ihre Serverless-Anwendung bereit

Gehen Sie wie folgt vor, um Ihre Anwendung mithilfe der AWS SAM-CLI bereitzustellen. Damit Ihre Funktion korrekt erstellt und bereitgestellt werden kann, muss die Python-Version 3.11 auf Ihrem Build-Computer und in Ihrem PATH installiert sein.

1. Führen Sie den folgenden Befehl in dem Verzeichnis aus, in dem Application Composer Ihre Dateien `template.yaml` und `lambda_function.py` gespeichert hat.

   ```
   sam build
   ```

   Dieser Befehl sammelt die Build-Artefakte für Ihre Anwendung und platziert sie im richtigen Format und am richtigen Ort, um sie bereitzustellen.

2. Führen Sie den folgenden Befehl aus, um Ihre Anwendung bereitzustellen und die in Ihrer AWS SAM-Vorlage angegebenen Lambda-, Amazon-SQS- und DynamoDB-Ressourcen zu erstellen.

   ```
   sam deploy --guided
   ```

   Wenn Sie die `--guided`-Markierung verwenden, werden Ihnen in AWS SAM Eingabeaufforderungen angezeigt, die Sie durch den Bereitstellungsprozess führen. Akzeptieren Sie für diese Bereitstellung die Standardoptionen, indem Sie die Eingabetaste drücken.

AWS SAM erstellt während des Bereitstellungsprozesses die folgenden Ressourcen in Ihrem AWS-Konto:

- Ein AWS CloudFormation-Stack mit dem Namen `sam-app`
- Eine Lambda-Funktion mit dem Namensformat `sam-app-LambdaIaCDemo-`*`99VXPpYQVv1M`*
- Eine Amazon-SQS-Warteschlange mit dem Namensformat `sam-app-LambdaIaCQueue-`*`xL87VeKsGiIo`*
- Eine DynamoDB-Tabelle mit dem Namensformat `sam-app-LambdaIaCTable-`*`CN0S66C0VLNV`*

AWS SAM erstellt auch die erforderlichen IAM-Rollen und -Richtlinien, sodass Ihre Lambda-Funktion Nachrichten aus der Amazon-SQS-Warteschlange lesen und CRUD-Operationen in der DynamoDB-Tabelle ausführen kann.

Weitere Informationen zur Bereitstellung von Serverless-Anwendungen mithilfe von AWS SAM finden Sie in den Ressourcen im Abschnitt the section called “Nächste Schritte”.

Testen der bereitgestellten Anwendung (optional)

Um zu überprüfen, ob Ihre Serverless-Anwendung korrekt bereitgestellt wurde, senden Sie eine Nachricht an Ihre Amazon-SQS-Warteschlange, die ein Schlüssel-Wert-Paar enthält, und überprüfen Sie, ob Lambda mit diesen Werten ein Element in Ihre DynamoDB-Tabelle schreibt.

So testen Sie Ihre Serverless-Anwendung

1. Öffnen Sie die Seite Warteschlangen der Amazon-SQS-Konsole und wählen Sie die Warteschlange aus, die AWS SAM aus Ihrer Vorlage erstellt hat. Der Name weist das Format `sam-app-LambdaIaCQueue-`*`xL87VeKsGiIo`* auf.

2. Wählen Sie Nachrichten senden und empfangen aus und fügen Sie den folgenden JSON in den Nachrichtentext im Abschnitt Nachricht senden ein.

```
{
    "myKey": "myValue"
}
```

3. Klicken Sie auf Send Message (Nachricht senden).

   Wenn Sie Ihre Nachricht an die Warteschlange senden, ruft Lambda Ihre Funktion über Ihre Zuordnung von Ereignisquellen auf, die in Ihrer AWS SAM-Vorlage definiert ist. Um zu bestätigen, dass Lambda Ihre Funktion wie erwartet aufgerufen hat, vergewissern Sie sich, dass Ihrer DynamoDB-Tabelle ein Element hinzugefügt wurde.

4. Öffnen Sie die Seite Tabellen der DynamoDB-Konsole und wählen Sie Ihre Tabelle aus. Der Name weist das Format `sam-app-LambdaIaCTable-CN0S66C0VLNV` auf.

5. Wählen Sie Explore Table Items (Tabellenelemente erkudnen) aus. Im Bereich Zurückgegebene Elemente sollten Sie ein Element mit der ID `myKey` und dem Wert `myValue` sehen.

Nächste Schritte

Um mehr über die Verwendung von Application Composer mit AWS SAM und AWS CloudFormation zu erfahren, beginnen Sie mit Verwenden von Application Composer mit AWS CloudFormation und AWS SAM.

Für ein geführtes Tutorial, bei dem AWS SAM zur Bereitstellung einer in Application Composer entwickelten Serverless-Anwendung verwendet wird, empfehlen wir Ihnen außerdem, das AWS Application Composer-Tutorial im AWS-Workshop für Serverless-Muster durchzuführen.

AWS SAM bietet eine Befehlszeilenschnittstelle (CLI), die Sie zusammen mit AWS SAM-Vorlagen und unterstützten Integrationen von Drittanbietern verwenden können, um Ihre Serverless-Anwendungen zu erstellen und auszuführen. Mit der AWS SAM-CLI können Sie Ihre Anwendung erstellen und bereitstellen, lokale Tests und Debugging durchführen, CI/CD-Pipelines konfigurieren und vieles mehr. Weitere Informationen zur Verwendung der AWS SAM-CLI finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model-Entwicklerleitfaden.

Um zu erfahren, wie Sie mithilfe der AWS CloudFormation-Konsole eine Serverless-Anwendung mit einer AWS SAM-Vorlage bereitstellen, beginnen Sie mit Verwenden der AWS CloudFormation-Konsole im AWS CloudFormation-Benutzerhandbuch.

Unterstützte Regionen für die Lambda-Integration mit Application Composer

Die Lambda-Integration in Application Composer wird in den folgenden AWS-Regionen unterstützt:

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)
- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Europa (Frankfurt)
- Europa (Zürich)
- Europa (Irland)
- Europe (London)
- Europa (Stockholm)
- Naher Osten (VAE)

Private Netzwerke mit VPC

Amazon Virtual Private Cloud (Amazon VPC) ist ein virtuelles Netzwerk in der AWS Cloud, das Ihrem AWS Konto gewidmet ist. Mit Amazon VPC können Sie ein privates Netzwerk für Ressourcen wie z. B. Datenbanken, Cache-Instances oder interne Services erstellen. Weitere Informationen zu Amazon VPC; finden Sie unter Was ist Amazon VPC?

Eine Lambda-Funktion läuft immer in einer VPC, die dem Lambda-Dienst gehört. Lambda wendet Netzwerkzugriffs- und Sicherheitsregeln auf diese VPC an und Lambda pflegt und überwacht die VPC automatisch. Wenn Ihre Lambda-Funktion auf die Ressourcen in Ihrer Konto-VPC zugreifen muss, konfigurieren Sie die Funktion für den Zugriff auf die VPC. Lambda stellt verwaltete Ressourcen namens Hyperplane ENIs bereit, die Ihre Lambda-Funktion verwendet, um von der Lambda-VPC eine Verbindung zu einer ENI (Elastic-Network-Schnittstelle) in Ihrer Konto-VPC herzustellen.

Für die Nutzung einer VPC oder Hyperplane ENI fallen keine zusätzlichen Gebühren an. Für einige VPC-Komponenten, wie NAT-Gateways, fallen Gebühren an. Weitere Informationen dazu finden Sie unter Amazon VPC – Preise.

Themen

VPC-Netzwerkelemente

Amazon-VPC-Netzwerke enthalten die folgenden Netzwerkelemente:

- Elastic-Network-Schnittstelle – Eine Elastic-Network-Schnittstelle ist eine logische Netzwerkkomponente in einer VPC, die eine virtuelle Netzwerkkarte darstellt.

- Subnetz – Ein Bereich an IP-Adressen in Ihrer VPC. Sie können AWS Ressourcen zu einem bestimmten Subnetz hinzufügen. Verwenden Sie öffentliche Subnetze für Ressourcen, die mit dem Internet verbunden sein müssen, und private Subnetze für Ressourcen, die nicht mit dem Internet verbunden sind.
- Sicherheitsgruppe — Verwenden Sie Sicherheitsgruppen, um den Zugriff auf die AWS Ressourcen in jedem Subnetz zu steuern.
- Zugriffssteuerungsliste (ACL) – Verwenden Sie eine Netzwerk-ACL, um zusätzliche Sicherheit in einem Subnetz zu gewährleisten. Die Standard-Subnetz-ACL lässt den gesamten ein- und ausgehenden Datenverkehr zu.
- Routentabelle — enthält eine Reihe von Routen, über AWS die der Netzwerkverkehr für Ihre VPC geleitet wird. Sie können ein Subnetz einer bestimmten Routing-Tabelle explizit zuordnen. Standardmäßig ist die Haupt-Routing-Tabelle dem privaten Subnetz zugeordnet.
- Route – Jede Route in einer Routing-Tabelle gibt einen Bereich von IP-Adressen und das Ziel an, an das Lambda den Datenverkehr für diesen Bereich sendet. Die Route gibt auch ein Ziel an, nämlich das Gateway, die Netzwerkschnittstelle oder die Verbindung, über die der Datenverkehr gesendet werden soll.
- NAT-Gateway — Ein AWS Network Address Translation (NAT) -Dienst, der den Zugriff von einem privaten privaten VPC-Subnetz auf das Internet steuert.
- VPC-Endpunkte — Sie können einen Amazon VPC-Endpunkt verwenden, um private Verbindungen zu Diensten herzustellen, auf denen gehostet wird AWS, ohne dass ein Zugriff über das Internet oder über ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. AWS Direct Connect Weitere Informationen finden Sie unter AWS PrivateLink und VPC-Endpoints.

> **Tip**
>
> Um Ihre Lambda-Funktion für den Zugriff auf eine VPC und ein Subnetz zu konfigurieren, können Sie die Lambda-Konsole oder die API verwenden.
> Informationen zur Konfiguration Ihrer Funktion finden CreateFunctionSie im `VpcConfig` Abschnitt unter. Hinzufügen von Lambda-Funktionen zu einer Amazon VPC in Ihrem AWS-KontoAusführliche Schritte finden Sie unter.

Weitere Informationen zu Amazon-VPC-Netzwerkdefinitionen finden Sie unter Funktionsweise von Amazon VPC im Amazon-VPC-Entwicklerhandbuch und unter Häufig gestellte Fragen zu Amazon VPC.

Verbinden von Lambda-Funktionen mit Ihrer VPC

Eine Lambda-Funktion läuft immer in einer VPC, die dem Lambda-Dienst gehört. Standardmäßig ist eine Lambda-Funktion nicht mit VPCs in Ihrem Konto verbunden. Wenn Sie eine Funktion mit einer VPC in Ihrem Konto verbinden, kann die Funktion nicht auf das Internet zugreifen, es sei denn, die VPC ermöglicht den Zugriff.

Lambda greift mithilfe einer Hyperplane ENI auf Ressourcen in Ihrer VPC zu. Hyperplane ENIs bieten NAT-Funktionen von der Lambda-VPC über VPC-zu-VPC (V2N) zu Ihrer Konto-VPC. V2N bietet Konnektivität von der Lambda-VPC zu Ihrer Konto-VPC, jedoch nicht in die andere Richtung.

Wenn Sie eine Lambda-Funktion erstellen (oder ihre VPC-Einstellungen aktualisieren), weist Lambda für jedes Subnetz in der VPC-Konfiguration Ihrer Funktion eine Hyperplane ENI zu. Mehrere Lambda-Funktionen können eine Netzwerkschnittstelle gemeinsam nutzen, wenn die Funktionen dasselbe Subnetz und dieselbe Sicherheitsgruppe verwenden.

Um eine Verbindung zu einem anderen AWS Dienst herzustellen, können Sie VPC-Endpunkte für die private Kommunikation zwischen Ihrer VPC und unterstützten Diensten verwenden. AWS Ein alternativer Ansatz besteht darin, ausgehenden Datenverkehr mithilfe eines NAT-Gateways an einen anderen Dienst weiterzuleiten. AWS

Um Ihrer Funktion Zugriff auf das Internet zu gewähren, leiten Sie ausgehenden Datenverkehr an ein NAT-Gateway in einem öffentlichen Subnetz weiter. Das NAT-Gateway verfügt über eine öffentliche IP-Adresse und kann sich über das Internet-Gateway der VPC mit dem Internet verbinden. Weitere Informationen finden Sie unter Aktivieren Sie den Internetzugang für mit VPN verbundene Lambda-Funktionen.

Gemeinsam genutzte Subnetze

VPC Sharing ermöglicht es mehreren AWS Konten, ihre Anwendungsressourcen, wie Amazon EC2 EC2-Instances und Lambda-Funktionen, in gemeinsam genutzten, zentral verwalteten Virtual Private Clouds (VPCs) zu erstellen. In diesem Modell teilt sich das Konto, dem die VPC gehört (Eigentümer), ein oder mehrere Subnetze mit anderen Konten (Teilnehmern), die derselben AWS Organisation angehören.

Für den Zugriff auf private Ressourcen verbinden Sie Ihre Funktion einem privaten freigegebenen Subnetz in Ihrer VPC. Der Subnetzeigentümer muss ein Subnetz für Sie freigeben, bevor Sie eine Funktion damit verbinden können. Der Subnetzbesitzer kann die gemeinsame Nutzung des Subnetzes auch zu einem späteren Zeitpunkt aufheben, wodurch die Konnektivität entfernt wird.

Einzelheiten zum Freigeben, Aufheben der Freigabe und Verwalten von VPC-Ressourcen in freigegebenen Subnetzen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Leitfaden.

Lambda Hyperplane ENIs

Die Hyperplane ENI ist eine verwaltete Netzwerkressource, die der Lambda-Service erstellt und verwaltet. Mehrere Ausführungsumgebungen in der Lambda-VPC können eine Hyperplane ENI verwenden, um sicher auf Ressourcen innerhalb von VPCs in Ihrem Konto zuzugreifen. Hyperplane ENIs bieten NAT-Funktionen von der Lambda-VPC Ihrer Konto-VPC.

Für jedes Subnetz erstellt Lambda eine Netzwerkschnittstelle für jeden eindeutigen Satz von Sicherheitsgruppen. Funktionen im Konto, die dieselbe Kombination aus Sicherheitsgruppe und Subnetz haben, verwenden dieselben Netzwerkschnittstellen. Über die folgenden Hyperplane-Ebene hergestellte Verbindungen werden automatisch nachverfolgt, auch wenn die Konfiguration der Sicherheitsgruppe keine Nachverfolgung erfordert. Eingehende Pakete von der VPC, die keinen eingerichteten Verbindungen entsprechen, werden auf der Hyperplane-Ebene verworfen. Weitere Informationen finden Sie unter Verbindungsverfolgung von Sicherheitsgruppen im Amazon EC2 EC2-Benutzerhandbuch.

Da die Funktionen in Ihrem Konto die ENI-Ressourcen teilen, ist der ENI-Lebenszyklus komplexer als andere Lambda-Ressourcen. In den folgenden Abschnitten wird der ENI-Lebenszyklus beschrieben.

ENI-Lebenszyklus

- Erstellen von ENIs
- Verwalten von ENIs
- Löschen von ENIs

Erstellen von ENIs

Lambda kann Hyperplane-ENI-Ressourcen für eine neu erstellte VPC-basierte Funktion oder für eine VPC-Konfigurationsänderung an einer vorhandenen Funktion erstellen. Die Funktion bleibt ausstehend, während Lambda die erforderlichen Ressourcen erstellt. Wenn die Hyperplane ENI bereit ist, wechselt die Funktion in den aktiven Status und die ENI steht zur Verwendung zur Verfügung. Lambda kann mehrere Minuten benötigen, um eine Hyperplane ENI zu erstellen.

Bei einer neu erstellten VPC-basierten Funktion schlagen alle Aufrufe oder andere API-Aktionen fehl, die mit der Funktion ausgeführt werden, bis der Funktionsstatus zu „Aktiv“ wechselt.

Für eine VPC-Konfigurationsänderung an einer vorhandenen Funktion verwenden alle Funktionsaufrufe weiterhin die Hyperplane ENI, die mit der alten Subnetz- und Sicherheitsgruppenkonfiguration verknüpft ist, bis der Funktionsstatus zu „Aktiv“ wechselt.

Wenn eine Lambda-Funktion 30 Tage lang inaktiv bleibt, ruft Lambda die unbenutzten Hyperplane-ENIs zurück und setzt den Funktionsstatus auf Inaktiv. Der nächste Aufruf bewirkt, dass Lambda die Funktion im Leerlauf wieder aktiviert. Der Aufruf schlägt fehl und die Funktion wechselt in den Status „Ausstehend“, bis Lambda die Erstellung oder Zuweisung einer Hyperplane ENI abgeschlossen hat.

Weitere Informationen zu Funktionszuständen finden Sie unter Lambda-Funktionszustände.

Verwalten von ENIs

Lambda verwendet Berechtigungen in der Ausführungsrolle Ihrer Funktion, um Netzwerkschnittstellen zu erstellen und zu verwalten. Lambda erstellt eine Hyperplane ENI, wenn Sie eine eindeutige Kombination aus Subnetz und Sicherheitsgruppe für eine VPC-basierte Funktion in einem Konto definieren. Lambda verwendet Hyperplane ENI für andere VPC-basierte Funktionen in Ihrem Konto, die dieselbe Kombination aus Subnetz und Sicherheitsgruppe verwenden.

Es gibt kein Kontingent für die Anzahl der Lambda-Funktionen, die dieselbe Hyperplane ENI verwenden können. Jede Hyperplane ENI unterstützt jedoch bis zu 65.000 Verbindungen/Ports. Wenn die Anzahl der Verbindungen 65.000 überschreitet, erstellt Lambda eine neue Hyperplane ENI, um zusätzliche Verbindungen bereitzustellen.

Wenn Sie Ihre Funktionskonfiguration aktualisieren, um auf eine andere VPC zuzugreifen, trennt Lambda die Verbindung zur Hyperplane ENI in der vorherigen VPC. Der Vorgang zum Aktualisieren der Verbindung zu einer neuen VPC kann mehrere Minuten dauern. Während dieser Zeit verwenden Aufrufe der Funktion weiterhin die vorherige VPC. Nachdem das Update abgeschlossen ist, verwenden neue Aufrufe die Hyperplane ENI in der neuen VPC. Zu diesem Zeitpunkt ist die Lambda-Funktion nicht mehr mit der vorherigen VPC verbunden.

Löschen von ENIs

Wenn Sie eine Funktion aktualisieren, um ihre VPC-Konfiguration zu entfernen, benötigt Lambda bis zu 20 Minuten, um die angehängte Hyperplane ENI zu löschen. Lambda löscht die ENI nur, wenn keine andere Funktion (oder veröffentlichte Funktionsversion) diese Hyperplane ENI verwendet.

Lambda verwendet Berechtigungen in der Ausführungsrolle der Funktion, um die Hyperplane ENI zu löschen. Wenn Sie die Ausführungsrolle löschen, bevor Lambda die Hyperplane ENI löscht, kann Lambda die Hyperplane ENI nicht löschen. Sie können den Löschvorgang manuell durchführen.

Lambda löscht keine Netzwerkschnittstellen, die von Funktionen oder Funktionsversionen in Ihrem Konto verwendet werden. Mit dem Lambda-ENI-Finder können Sie Funktionen oder Funktionsversionen identifizieren, die eine Hyperplane ENI verwenden. Für alle Funktionen oder Funktionsversionen, die Sie nicht mehr benötigen, können Sie die VPC-Konfiguration entfernen, damit Lambda die Hyperplane ENI löscht.

Verbindungen

Lambda unterstützt zwei Arten von Verbindungen: TCP (Transmission Control Protocol) und UDP (User Datagram Protocol).

Wenn Sie eine VPC erstellen, erstellt Lambda automatisch eine DHCP-Optionsliste und ordnet sie der VPC zu. Sie können Ihre eigene DHCP-Optionliste für Ihre VPC konfigurieren. Weitere Informationen finden Sie unter DHCP-Optionen der Amazon VPC.

Amazon stellt einen DNS-Server (den Amazon Route 53 Resolver) für Ihre VPC zur Verfügung. Weitere Informationen finden Sie unter DNS-Support für Ihre VPC.

IPv6-Support

Lambda unterstützt eingehende Verbindungen zu den öffentlichen Dual-Stack-Endpunkten von Lambda und ausgehende Verbindungen zu Dual-Stack-VPC-Subnetzen über IPv6.

Eingehend

Verwenden Sie die öffentlichen Dual-Stack-Endpunkte von Lambda, um Ihre Funktion über IPv6 aufzurufen. Dual-Stack-Endpunkte unterstützen sowohl IPv4 als auch IPv6. Lambda-Dual-Stack-Endpunkte verwenden die folgende Syntax:

```
protocol://lambda.us-east-1.api.aws
```

Sie können auch Lambda-Funktions-URLs verwenden, um Funktionen über IPv6 aufzurufen. Funktions-URL-Endpunkte haben das folgende Format:

```
https://url-id.lambda-url.us-east-1.on.aws
```

Ausgehend

Ihre Funktion kann über IPv6 eine Verbindung zu Ressourcen in Dual-Stack-VPC-Subnetzen herstellen. Diese Option ist standardmäßig deaktiviert. Um ausgehenden

IPv6-Verkehr zuzulassen, verwenden Sie die Konsole oder die `--vpc-config Ipv6AllowedForDualStack=true`-Option mit dem Befehl create-function oder update-function-configuration.

> **Note**
>
> Um ausgehenden IPv6-Verkehr in einer VPC zuzulassen, müssen alle Subnetze, die mit der Funktion verbunden sind, Dual-Stack-Subnetze sein. Lambda unterstützt keine ausgehenden IPv6-Verbindungen für reine IPv6-Subnetze in einer VPC, ausgehende IPv6-Verbindungen für Funktionen, die nicht mit einer VPC verbunden sind, oder eingehende IPv6-Verbindungen mit VPC-Endpunkten (AWS PrivateLink).

Sie können Ihren Funktionscode aktualisieren, um explizit eine Verbindung zu Subnetzressourcen über IPv6 herzustellen. Das folgende Python-Beispiel öffnet einen Socket und stellt eine Verbindung zu einem IPv6-Server her.

Example — Verbindung zum IPv6-Server herstellen

```
def connect_to_server(event, context):
    server_address = event['host']
    server_port = event['port']
    message = event['message']
    run_connect_to_server(server_address, server_port, message)

def run_connect_to_server(server_address, server_port, message):
    sock = socket.socket(socket.AF_INET6, socket.SOCK_STREAM, 0)
    try:
        # Send data
        sock.connect((server_address, int(server_port), 0, 0))
        sock.sendall(message.encode())
        BUFF_SIZE = 4096
        data = b''
        while True:
            segment = sock.recv(BUFF_SIZE)
            data += segment
            # Either 0 or end of data
            if len(segment) < BUFF_SIZE:
                break
        return data
    finally:
```

```
        sock.close()
```

Sicherheit

AWS bietet Sicherheitsgruppen und Netzwerk-ACLs, um die Sicherheit in Ihrer VPC zu erhöhen. Sicherheitsgruppen kontrollieren eingehenden und ausgehenden Verkehr für Ihre Ressourcen, Netzwerk-ACLs kontrollieren eingehenden und ausgehenden Zugriff für Ihre Subnetze. Sicherheitsgruppen bieten ausreichend Zugriffskontrolle für die meisten Subnetze. Sie können Netzwerk-ACLs verwenden, wenn Sie eine zusätzliche Sicherheitsebene für Ihre VPC benötigen. Weitere Informationen finden Sie unter Richtlinie für den Datenverkehr zwischen Netzwerken in Amazon VPC. Jedem Subnetz, das Sie erstellen, wird automatisch die standardmäßige Netzwerk-ACL der VPC zugeordnet. Sie können die Zuordnung und die Inhalte der standardmäßigen Netzwerk-ACL ändern.

Weitere bewährte Methoden für die Sicherheit finden Sie unter Bewährte Methoden für VPC-Sicherheit. Weitere Informationen darüber, wie Sie IAM für die Verwaltung des Zugriffs auf die Lambda-API und Ressourcen verwenden können, finden Sie unter AWS Lambda -Berechtigungen.

Sie können Lambda-spezifische Bedingungsschlüssel für VPC-Einstellungen verwenden, um zusätzliche Berechtigungssteuerungen für Ihre Lambda-Funktionen bereitzustellen. Weitere Informationen zu VPC-Bedingungsschlüsseln finden Sie unter Verwenden von IAM-Bedingungsschlüsseln für VPC-Einstellungen.

> **Note**
>
> Lambda-Funktionen können über das öffentliche Internet oder über AWS PrivateLink-Endpunkte aufgerufen werden. Auf Ihre Funktions-URLs können Sie nur über das öffentliche Internet zugreifen. Lambda-Funktionen unterstützen zwar AWS PrivateLink, Funktions-URLs jedoch nicht.

Beobachtbarkeit

Mit VPC-Flow-Protokollen können Sie Informationen zum IP-Datenverkehr zu und von Netzwerkschnittstellen in Ihrer VPC erfassen. Sie können Flow-Protokolldaten in Amazon CloudWatch Logs oder Amazon S3 veröffentlichen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten abrufen und an dem gewählten Ziel anzeigen.

Hinweis: Wenn Sie eine Funktion an eine VPC anhängen, verwenden die CloudWatch Protokollnachrichten nicht die VPC-Routen. Lambda sendet sie mit dem regulären Routing für Protokolle.

Konfiguration der Befehlssatzarchitektur für eine Lambda-Funktion

Die-Befehlssatz-Architektureiner Lambda-Funktion bestimmt den Typ des Computerprozessors, den Lambda zum Ausführen der Funktion verwendet. Lambda bietet eine Auswahl an Befehlssatz-Architekturen:

- arm64 — 64-Bit-ARM-Architektur für den AWS Graviton2-Prozessor.
- x86_64 — 64-Bit-x86-Architektur für x86-basierte Prozessoren.

> **Note**
>
> Die arm64-Architektur ist in den meisten Versionen verfügbar. AWS-Regionen Weitere Informationen finden Sie unter AWS Lambda -Preisgestaltung. Wählen Sie in der Tabelle mit den Speicherpreisen die Registerkarte Arm-Preis aus und öffnen Sie dann die Dropdownliste Region, um zu sehen, welche Produkte arm64 mit Lambda AWS-Regionen unterstützen. Ein Beispiel für die Erstellung einer Funktion mit der Arm64-Architektur finden Sie unter AWS Lambda Funktionen, die vom Graviton2-Prozessor unterstützt werden. AWS

Themen

Vorteile der Verwendung von arm64-Architektur

Lambda-Funktionen, die die Arm64-Architektur (AWS Graviton2-Prozessor) verwenden, können einen deutlich besseren Preis und eine deutlich bessere Leistung erzielen als die entsprechende Funktion, die auf der x86_64-Architektur ausgeführt wird. Erwägen Sie, arm64 für rechenintensive Anwendungen wie Hochleistungsrechnen, Videocodierung und Simulations-Workloads zu verwenden.

Die Graviton2-CPU verwendet den Neoverse N1-Kern und unterstützt Armv8.2 (einschließlich CRC- und Krypto-Erweiterungen) sowie mehrere andere architektonische Erweiterungen.

Graviton2 reduziert die Lesezeit des Speichers, indem es einen größeren L2-Cache pro vCPU bereitstellt, was die Latenzleistung von Web- und Mobile-Backends, Microservices und Datenverarbeitungssystemen verbessert. Graviton2 bietet auch eine verbesserte Verschlüsselungsleistung und unterstützt Befehlssätze, die die Latenz von CPU-basierten Inferenzen für Machine Learning verbessern.

Weitere Informationen zu Graviton2 finden Sie unter Graviton Processor. AWSAWS

Anforderungen für die Migration zur arm64-Architektur

Wenn Sie eine Lambda-Funktion für die Migration zur arm64-Architektur auswählen, stellen Sie sicher, dass Ihre Funktion die folgenden Anforderungen erfüllt, um eine reibungslose Migration zu gewährleisten:

- Die Funktion verwendet derzeit eine Lambda Amazon Linux 2-Laufzeit.
- Das Bereitstellungspaket enthält nur Open-Source-Komponenten und Quellcode, die Sie steuern, sodass Sie alle notwendigen Updates für die Migration vornehmen können.
- Wenn der Funktionscode Abhängigkeiten von Drittanbietern enthält, bietet jede Bibliothek oder jedes Paket eine arm64-Version.

Funktionscode-Kompatibilität mit arm64-Architektur

Ihr Lambda-Funktionscode muss mit der Befehlssatz-Architektur der Funktion kompatibel sein. Bevor Sie eine Funktion zur arm64-Architektur migrieren, beachten Sie die folgenden Punkte zum aktuellen Funktionscode:

- Wenn Sie Ihren Funktionscode mit dem eingebetteten Code-Editor hinzugefügt haben, läuft Ihr Code wahrscheinlich auf beiden Architekturen ohne Änderung.
- Nach dem Upload Ihres Funktionscodes, müssen Sie neuen Code uploaden, der mit Ihrer Zielarchitektur kompatibel ist.
- Wenn Ihre Funktion Layer verwendet, müssen Sieüberprüfe jede Ebeneum sicherzustellen, dass es mit der neuen Architektur kompatibel ist. Wenn ein Layer nicht kompatibel ist, bearbeiten Sie die Funktion, um die aktuelle Layer-Version durch eine kompatible Layer-Version zu ersetzen.
- Wenn Ihre Funktion Lambda-Erweiterungen verwendet, müssen Sie jede Erweiterung überprüfen, um sicherzustellen, dass sie mit der neuen Architektur kompatibel ist.
- Wenn Ihre Funktion einen Container-Image-Bereitstellungspakettyp verwendet, müssen Sie ein neues Container-Image erstellen, das mit der Architektur der Funktion kompatibel ist.

Migration zur arm64-Architektur

Um eine Lambda-Funktion auf die arm64-Architektur zu migrieren, empfehlen wir die folgenden Schritte:

1. Erstellen Sie die Liste der Abhängigkeiten für Ihre Anwendung oder Ihren Workload. Häufige Abhängigkeiten sind unter anderem:
   - Alle Bibliotheken und Pakete, die die Funktion verwendet.
   - Die Tools, mit denen Sie die Funktion erstellen, bereitstellen und testen, wie Compiler, Test-Suites, Pipelines für Continuous Integration und Continuous Delivery (CI/CD), Bereitstellungstools und Skripte.
   - Die Lambda-Erweiterungen und Tools von Drittanbietern, mit denen Sie die Funktion in der Produktion überwachen.
2. Überprüfen Sie für jede der Abhängigkeiten die Version und prüfen Sie dann, ob arm64-Versionen verfügbar sind.
3. Erstellen Sie eine Umgebung, um Ihre Anwendung zu migrieren.
4. Bootstrap die Anwendung.
5. Testen und debuggen Sie die Anwendung.
6. Testen Sie die Leistung der arm64-Funktion. Vergleichen Sie die Leistung mit der x86_64-Version.
7. Aktualisieren Sie Ihre Infrastruktur-Pipeline, um arm64 Lambda-Funktionen zu unterstützen.
8. Stufen Sie Ihre Bereitstellung in die Produktion ein.

   Verwenden Sie zum Beispiel Alias-Routing-Konfiguration um den Datenverkehr zwischen den Versionen x86 und arm64 der Funktion aufzuteilen und die Leistung und Latenz zu vergleichen.

Weitere Informationen zum Erstellen einer Codeumgebung für die arm64-Architektur, einschließlich sprachspezifischer Informationen für Java, Go, .NET und Python, finden Sie im Repository Erste Schritte mit AWS Graviton. GitHub

Konfigurieren der Befehlssatz-Architektur

Sie können die Befehlssatzarchitektur für neue und bestehende Lambda-Funktionen mithilfe der Lambda-Konsole, AWS SDKs, AWS Command Line Interface (AWS CLI) oder konfigurieren. AWS CloudFormation Führen Sie die folgenden Schritte aus, um die Befehlssatzarchitektur für eine vorhandene Lambda-Funktion von der Konsole aus zu ändern.

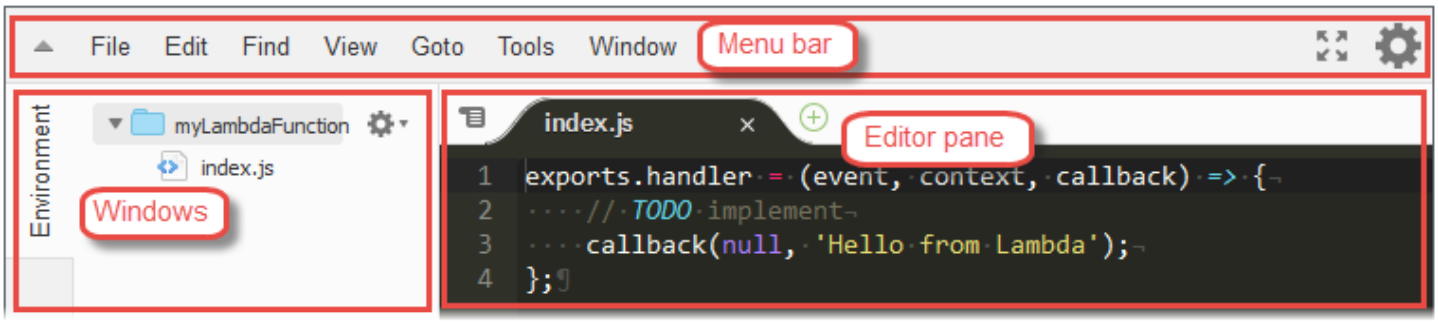
1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Klicken Sie auf den Namen der Funktion, für die Sie die Befehlssatzarchitektur konfigurieren möchten.
3. Wählen Sie auf der Registerkarte Code für den Abschnitt Laufzeiteinstellungen die Option Bearbeiten aus.
4. Unter Architecture (Architektur) wählen Sie die Befehlssatzarchitektur aus, die Ihre Funktion verwenden soll.
5. Wählen Sie Speichern.

> **Note**
>
> Alle Amazon-Linux 2-Laufzeiten unterstützen sowohl x86_64- als auch ARM-CPU-Architekturen.
> Laufzeiten, die das Amazon-Linux 2-Betriebssystem nicht verwenden, z. B. Go 1.x, unterstützen die arm64-Architektur nicht. Um die arm64-Architektur mit Go 1.x zu verwenden, können Sie Ihre Funktion in einer bereitgestellten al2-Laufzeit ausführen. Weitere Informationen finden Sie in der Bereitstellungsanleitung für ZIP-Pakete und Container-Images.

Bearbeiten von Code mit dem Lambda-Konsoleneditor

Mit dem Code-Editor in der Lambda-Konsole können Sie den Code Ihrer Lambda-Funktion schreiben, testen und die Ausführungsergebnisse anzeigen. Der Code-Editor unterstützt Sprachen, die keine Kompilierung erfordern, wie Node.js und Python. Der Code-Editor unterstützt nur ZIP-Dateiarchive als Bereitstellungspakete und das Bereitstellungspaket muss kleiner als 3 MB sein.

Der Code-Editor umfasst die Menüleiste, Fenster, und den Editorbereich.



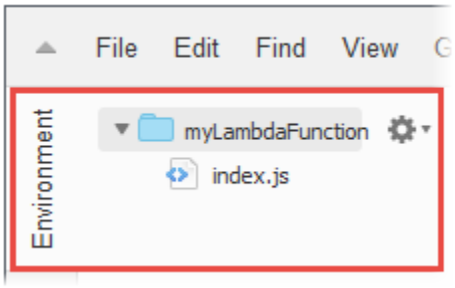
Eine Liste mit Informationen zu den Befehlen finden Sie in der Referenz zu Menübefehlen im AWS Cloud9 -Benutzerhandbuch. Bitte beachten Sie, dass einige der in dieser Referenz aufgeführten Befehle im Code-Editor nicht verfügbar sind.

Themen

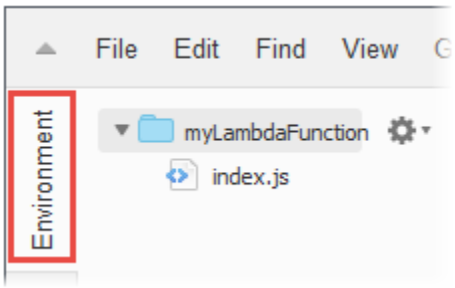
- Arbeiten mit Dateien und Ordnern
- Arbeiten mit Code
- Arbeiten im Vollbildmodus
- Arbeiten mit Präferenzen

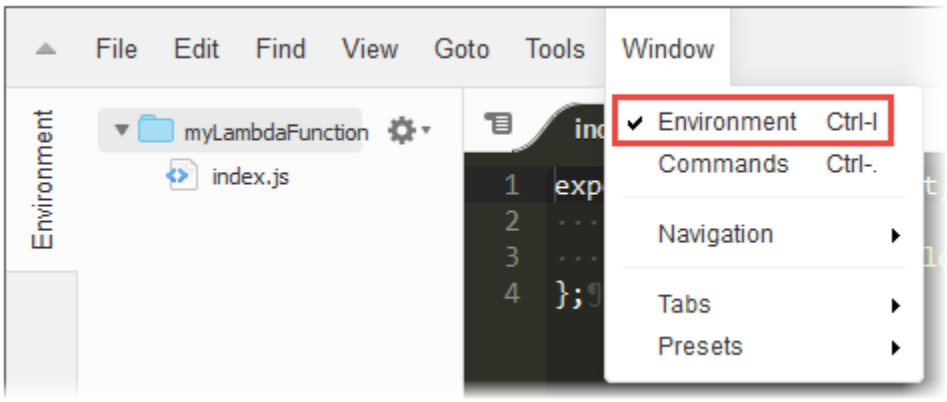
Arbeiten mit Dateien und Ordnern

Sie können mit dem Fenster Environment im Code-Editor Dateien für Ihre Funktion erstellen, öffnen und verwalten.



Um das Fenster „Environment” ein- oder auszublenden,wählen Sie die Schaltfläche Environment. Wenn die Schaltfläche Environment nicht angezeigt wird, wählen Sie Window, Environment auf der Menüleiste.



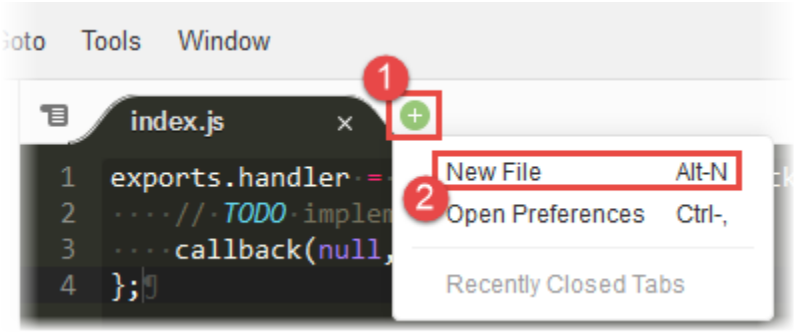


Um eine einzelne Datei zu öffnen und den Inhalt im Editorbereich anzuzeigen, doppelklicken Sie im Fenster Environment auf die entsprechende Datei.

Um mehrere Dateien zu öffnen und den Inhalt im Editorbereich anzuzeigen, wählen Sie die Dateien im Fenster Environment. Klicken Sie mit der rechten Maustaste auf die ausgewählten Dateien und wählen Sie Open.

Um eine neue Datei zu öffnen, führen Sie einen der folgenden Schritte aus:

- Klicken Sie im Fenster Environment mit der rechten Maustaste auf den Ordner, zu dem Sie die neue Datei hinzufügen möchten, und wählen Sie New File. Geben Sie den Pfad und die Erweiterung der Datei ein und drücken Sie dann die Eingabetast.
- Wählen Sie File, New File auf der Menüleiste. Wenn die Datei gespeichert werden kann, wählen Sie File, Save oder File, Save As auf der Menüleiste. Verwenden Sie dann das Dialogfeld Save As, um die Datei zu benennen und den Speicherort festzulegen.
- Wählen Sie in der Tabulatorschaltflächen-Leiste im Editorbereich die Schaltfläche + und anschließend New File. Wenn die Datei gespeichert werden kann, wählen Sie File, Save oder File, Save As auf der Menüleiste. Verwenden Sie dann das Dialogfeld Save As, um die Datei zu benennen und den Speicherort festzulegen.



Um einen neuen Ordner zu erstellen, klicken Sie mit der rechten Maustaste auf den Ordner im Fenster Environment, zu dem Sie den neuen Ordner hinzufügen möchten, und wählen Sie New Folder. Geben Sie den Namen des Ordners ein und drücken Sie die Eingabetaste.

Um eine Datei zu speichern, während diese geöffnet ist und der Inhalt im Editorbereich angezeigt wird, wählen Sie File, Save auf der Menüleiste.

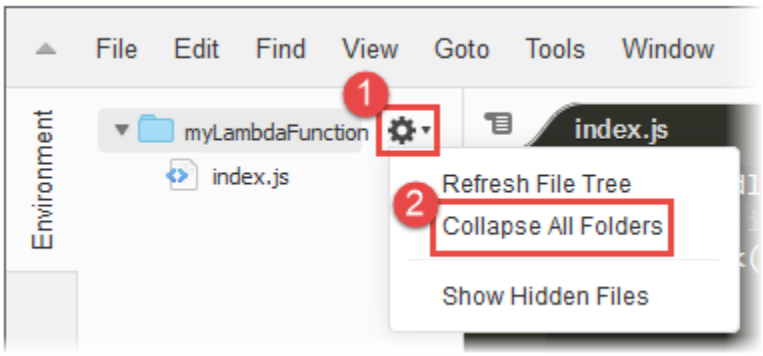
Um eine Datei oder einen Ordner umzubenennen, klicken Sie mit der rechten Maustaste auf die entsprechende Datei bzw. den entsprechenden Ordner im Fenster Environment. Geben Sie den Ersatznamen ein und drücken Sie die Eingabetaste.

Um Dateien oder Ordner zu löschen, wählen Sie die entsprechenden Dateien oder Ordner im Fenster Environment. Klicken Sie mit der rechten Maustaste auf die ausgewählten Dateien oder Ordner und wählen Sie Delete. Bestätigen Sie die Löschung, indem Sie Yes (bei einer Einzelauswahl) oder Yes to All wählen.

Um Dateien oder Ordner auszuschneiden, zu kopieren, einzufügen oder zu duplizieren, wählen Sie die entsprechenden Dateien oder Ordner im Fenster Environment. Klicken Sie mit der rechten

Maustaste auf die ausgewählten Dateien oder Ordner und wählen Sie Cut, Copy, Paste oder Duplicate.

Um Ordner zu reduzieren, wählen Sie das Zahnradsymbol im Fenster Environment und anschließend Collapse All Folders.



Um ausgeblendete Dateien ein- bzw. wieder auszublenden, wählen Sie das Zahnradsymbol im Fenster Environment und anschließend Show Hidden Files.

Gehen Sie wie folgt vor, um Umgebungsvariablen zu sehen, die für die Funktion konfiguriert sind:

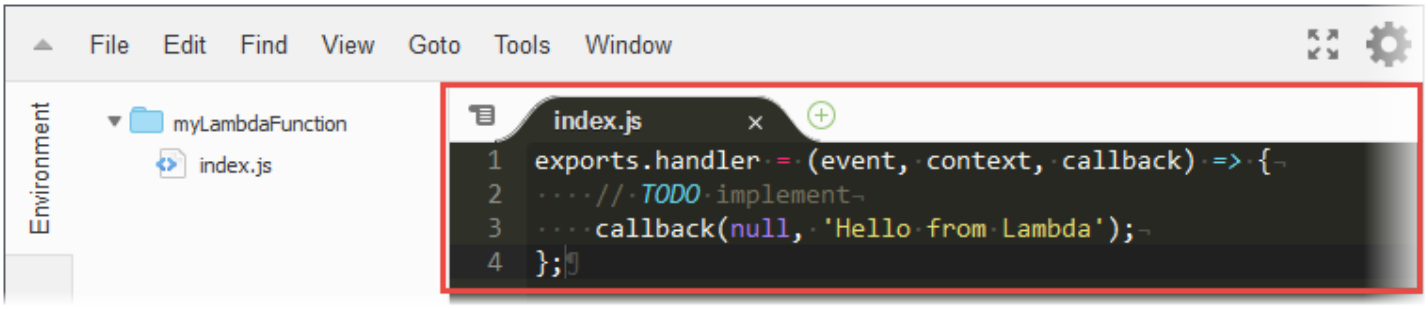
1. Wählen Sie die Registerkarte Code.
2. Wählen Sie die Registerkarte Umgebungsvariablen.
3. Wählen Sie Tools, Umgebungsvariablen anzeigen.

Umgebungsvariablen bleiben verschlüsselt, wenn sie im Code-Editor der Konsole aufgeführt werden. Wenn Sie Verschlüsselungshilfen für die Verschlüsselung während der Übertragung aktiviert haben, bleiben diese Einstellungen unverändert. Weitere Informationen finden Sie unter Sicherung von Lambda-Umgebungsvariablen.

Die Liste der Umgebungsvariablen ist schreibgeschützt und nur auf der Lambda-Konsole verfügbar. Diese Datei ist nicht enthalten, wenn Sie das ZIP-Dateiarchiv der Funktion herunterladen, und Sie können keine Umgebungsvariablen hinzufügen, indem Sie diese Datei hochladen.

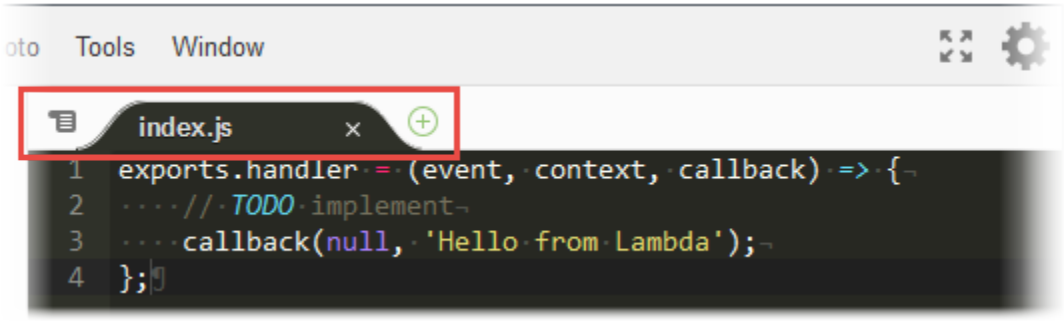
Arbeiten mit Code

Verwenden Sie den Editorbereich im Code-Editor zum Anzeigen und Schreiben von Code.



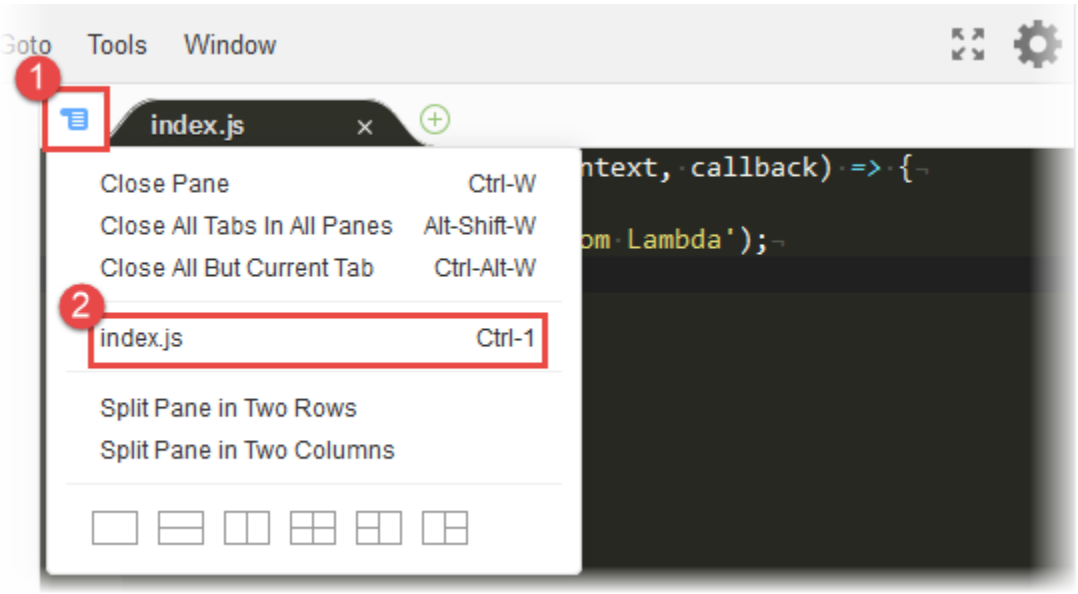
Arbeiten mit Tabulatorschaltflächen

Verwenden Sie die Tabulatorschaltflächen-Leiste zum Auswählen, Anzeigen und Erstellen von Dateien.



Um den Inhalt einer geöffneten Datei anzuzeigen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie die Registerkarte der Datei aus.
- Wählen Sie die Dropdownmenü-Schaltfläche in der Tabulatorschaltflächen-Leiste und wählen Sie den Namen der Datei.



Um eine geöffnete Datei zu schließen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie das Symbol X in der Registerkarte der Datei.
- Wählen Sie die Registerkarte der Datei aus. Wählen Sie anschließend die Dropdownmenü-Schaltfläche in der Tabulatorschaltflächen-Leiste und Close Pane.

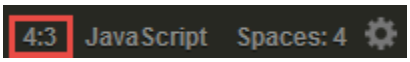
Um mehrere geöffnete Dateien zu schließen, wählen Sie das Dropdownmenü in der Tabulatorschaltflächen-Leiste und anschließend nach Bedarf Close All Tabs in All Panes oder Close All But Current Tab.

Um eine neue Datei zu erstellen, wählen Sie die Schaltfläche + in der Tabulatorschaltflächen-Leiste und anschließend New File. Wenn die Datei gespeichert werden kann, wählen Sie File, Save oder File, Save As auf der Menüleiste. Verwenden Sie dann das Dialogfeld Save As, um die Datei zu benennen und den Speicherort festzulegen.

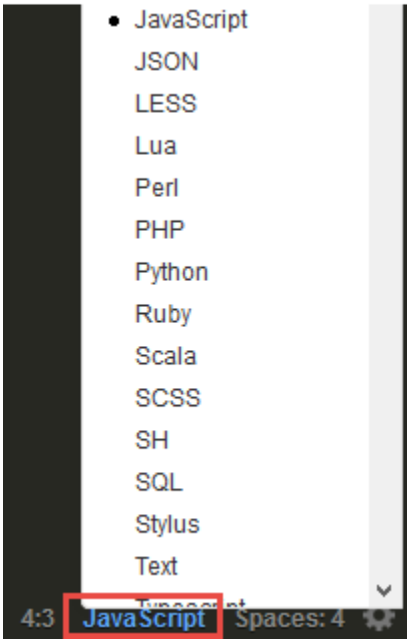
Arbeiten mit der Statusleiste

Verwenden Sie die Statusleiste, um schnell zu einer Zeile in der aktiven Datei zu navigieren und um die Anzeige von Code zu ändern.

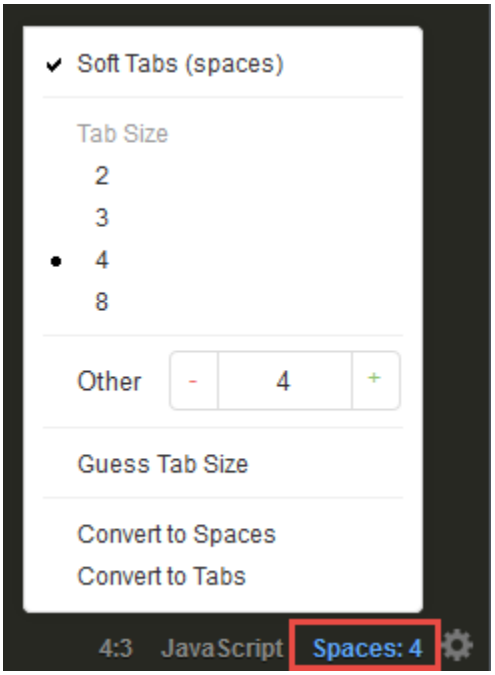
Um schnell zu einer Zeile in der aktiven Datei zu navigieren, wählen Sie die Zeilenauswahl, geben die Zeilennummer ein, zu der Sie navigieren möchten, und drücken Sie die Eingabetaste.



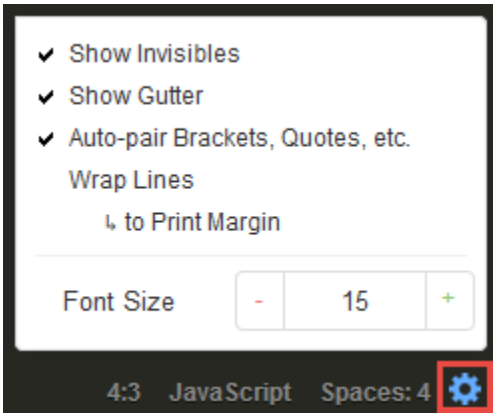
Um das Farbschema für Code in der aktiven Datei zu ändern, wählen Sie die Code-Farbschemenauswahl und anschließend das neue Code-Farbschema.



Um in der aktiven Datei zu ändern, ob weiche Tabulatoren oder Leerzeichen verwendet oder ob eine Konvertierung in Leerzeichen oder Tabulatoren erfolgen soll oder um die Tabulatorgröße festzulegen, wählen Sie die Auswahl für Leerzeichen und Tabulatoren und anschließend die neuen Einstellungen.



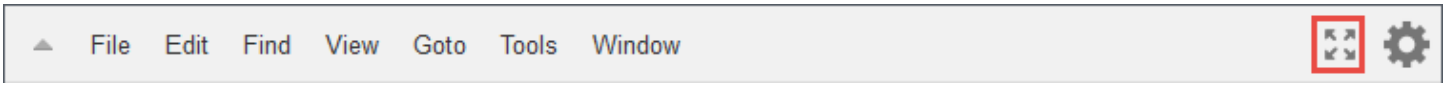
Um für alle Dateien zu ändern, ob nicht sichtbare Zeichen oder der Bundsteg ein- oder ausgeblendet, ob Klammern oder Zitate automatisch verbunden oder Zeilen umgebrochen werden sollen, oder um die Schriftart zu ändern, wählen Sie das Zahnradsymbol und anschließend die neuen Einstellungen.



Arbeiten im Vollbildmodus

Sie können den Code-Editor erweitern, um mehr Platz für die Arbeit mit Ihrem Code zu haben.

Um den Code-Editor bis zu den Kanten des Webbrowserfensters zu erweitern, wählen Sie die Schaltfläche Toggle fullscreen in der Menüleiste.



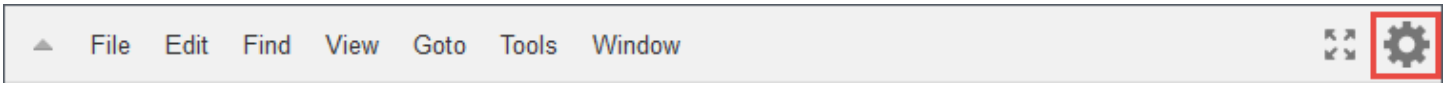
Um den Code-Editor auf seine ursprüngliche Größe zu reduzieren, wählen Sie erneut die Schaltfläche Toggle fullscreen.

Im Vollbildmodus werden zusätzliche Optionen auf der Menüleiste angezeigt: Save (Speichern) und Test (Testen). Wenn Sie Save wählen, wird der Funktionscode gespeichert. Wenn Sie Test oder Configure Events wählen, können Sie die Testereignisse der Funktion erstellen oder bearbeiten.

Arbeiten mit Präferenzen

Sie können verschiedene Code-Editoreinstellungen ändern, wie beispielsweise welche Hinweise und Warnmeldungen zu Codierungen angezeigt werden, das Code-Folding-Verhalten, das automatische Code-Vervollständigungsverhalten und vieles mehr.

Um die Code-Editoreinstellungen zu ändern, wählen Sie das Zahnradsymbol Preferences in der Menüleiste.



Eine Liste mit Informationen zu den Einstellungen finden Sie in den folgenden Referenzen im AWS Cloud9 -Benutzerhandbuch.

- Projekteinstellungen, die geändert werden können
- Mögliche Änderungen an Benutzereinstellungen

Bitte beachten Sie, dass einige der in diesen Referenzen aufgeführten Einstellungen im Code-Editor nicht verfügbar sind.

Zusätzliche Lambda-Funktionalitäten

Lambda bietet eine Managementkonsole und eine API für die Verwaltung und den Aufruf von Funktionen. Sie bietet Laufzeiten, die eine Standardgruppe von Funktionen unterstützen, sodass Sie je nach Ihren Anforderungen problemlos zwischen Sprachen und Frameworks wechseln können. Zusätzlich zu den Funktionen können Sie auch Versionen, Aliasse, Ebenen und benutzerdefinierte Laufzeiten erstellen.

Erweiterte Funktionen

- Skalierung
- Steuerelemente für die Gleichzeitigkeit
- Funktions-URLs
- Asynchroner Aufruf
- Zuweisung von Ereignisquellen
- Ziele
- Funktionsentwürfe
- Test- und Bereitstellungstoools
- Anwendungsvorlagen

Skalierung

Lambda verwaltet die Infrastruktur, die Ihren Code ausführt, und skaliert automatisch als Reaktion auf eingehende Anforderungen. Wenn Ihre Funktion schneller aufgerufen wird, als eine einzelne Instance Ihrer Funktion Ereignisse verarbeiten kann, führt Lambda durch Ausführen zusätzlicher Instances eine Skalierung nach oben durch. Wenn der Datenverkehr nachlässt, werden inaktive Instances eingefroren oder beendet. Sie zahlen nur für die Zeit, in der Ihre Funktion Ereignisse initialisiert oder verarbeitet.

Weitere Informationen finden Sie unter Die Lambda-Funktionsskalierung verstehen.

Steuerelemente für die Gleichzeitigkeit

Verwenden Sie die Gleichzeitigkeitseinstellungen, um sicherzustellen, dass Ihre Produktionsanwendungen hochverfügbar und reaktionsschnell sind.

Um zu verhindern, dass eine Funktion zu viel Gleichzeitigkeit verwendet, und um einen Teil der verfügbaren Gleichzeitigkeit Ihres Kontos für eine Funktion zu reservieren, verwenden Sie die reservierte Gleichzeitigkeit. Mit reservierter Parallelität wird der Pool der verfügbaren Parallelität in Teilmengen aufgeteilt. Eine Funktion mit reservierter Gleichzeitigkeit verwendet nur die Gleichzeitigkeit aus ihrer dedizierten Untermenge.

Um Funktionen ohne Schwankungen der Latenz skalieren zu können, verwenden Sie Provisioned Concurrency. Bei Funktionen, die lange dauern oder für die bei allen Aufrufen eine extrem geringe Latenz erforderlich ist, können Sie mithilfe der bereitgestellten Parallelität Instances Ihrer Funktion vorinitialisieren und sie jederzeit ausführen. Lambda wird in Application Auto Scaling integriert, um die automatische Skalierung für bereitgestellte Parallelität basierend auf der Auslastung zu unterstützen.

Weitere Informationen finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.

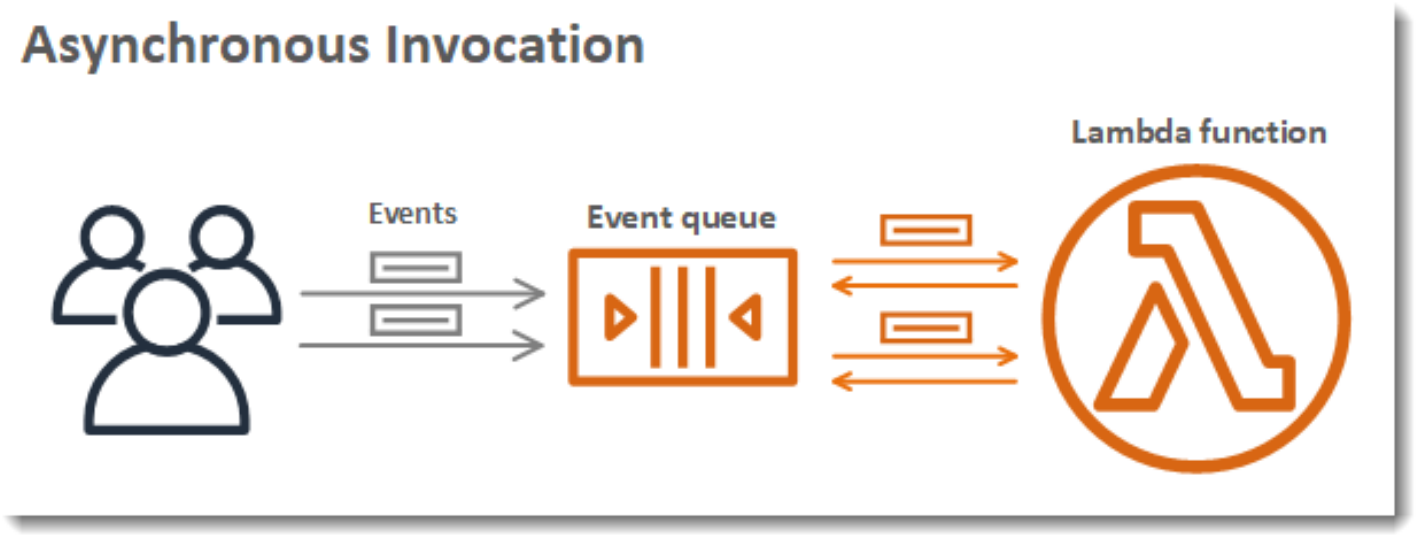
Funktions-URLs

Lambda bietet integrierte HTTP(S)-Endpunktunterstützung durch Funktions-URLs an. Mit Funktions-URLs können Sie Ihrer Lambda-Funktion einen dedizierten HTTP-Endpunkt zuweisen. Wenn Ihre Funktions-URL konfiguriert ist, können Sie sie verwenden, um Ihre Funktion über einen Webbrowser, curl, Postman oder einen beliebigen HTTP-Client aufzurufen.

Sie können einer vorhandenen Funktion eine Funktions-URL hinzufügen oder eine neue Funktion mit einer Funktions-URL erstellen. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktions-URLs.

Asynchroner Aufruf

Wenn Sie eine Funktion aufrufen, können Sie bestimmen, ob sie synchron oder asynchron aufgerufen wird. Bei einem synchronen Aufruf warten Sie, bis die Funktion das Ereignis verarbeitet und eine Antwort zurückgegeben hat. Bei einem asynchronen Aufruf stellt Lambda das Ereignis für die Verarbeitung in eine Warteschlangen und gibt umgehend eine Antwort zurück.

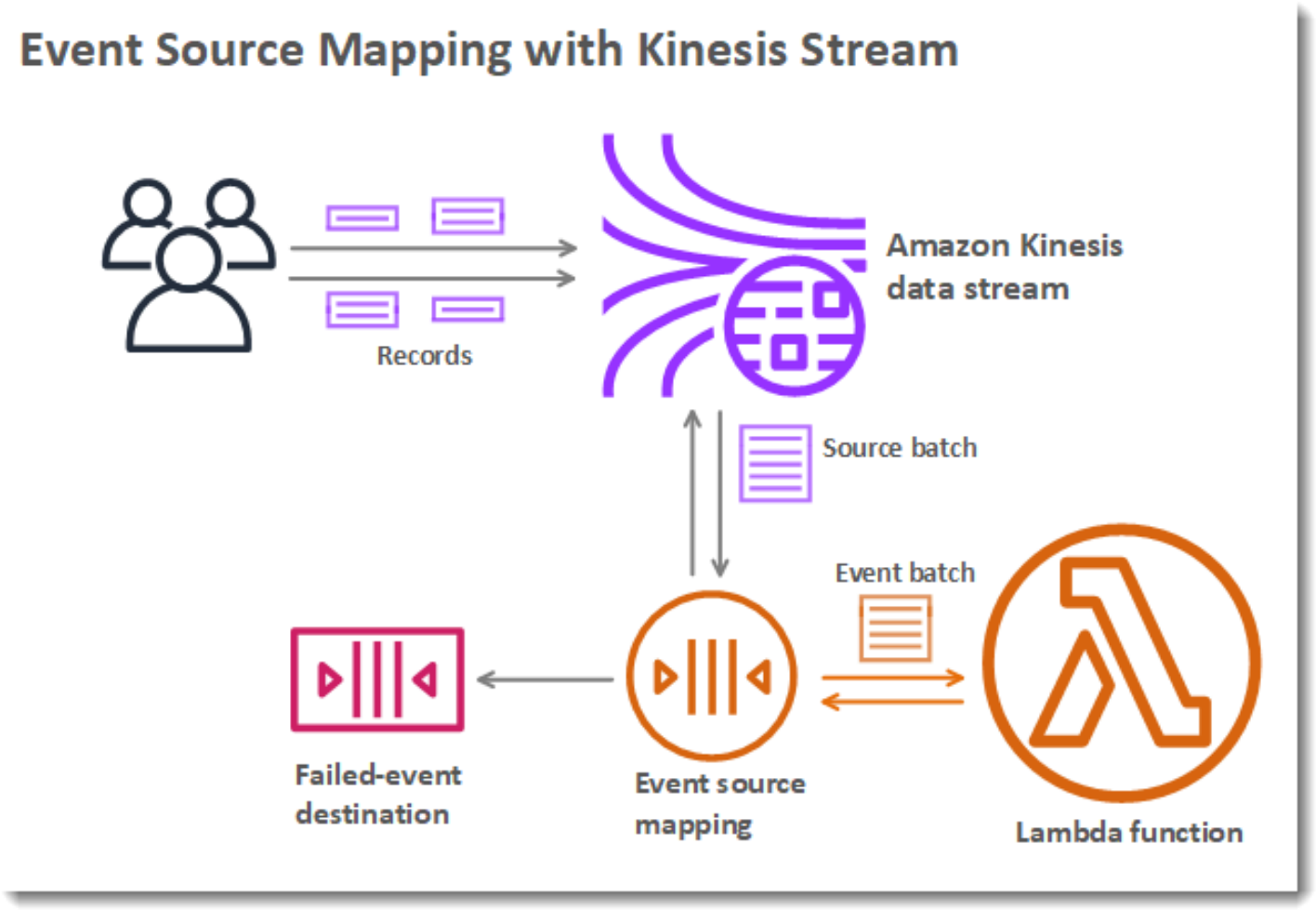


Bei asynchronen Aufrufen werden Wiederholungsversuche von Lambda behandelt, wenn die Funktion einen Fehler zurückgibt oder sie abgelehnt wird. Um dieses Verhalten anzupassen, können Sie Einstellungen für die Fehlerbehandlung einer Funktion, eine Version oder einen Alias konfigurieren. Sie können auch konfigurieren, dass Lambda Ereignisse, bei denen die Verarbeitung fehlgeschlagen ist, an eine Warteschlange für unzustellbare Nachrichten oder den Datensatz eines beliebigen Aufrufs an ein Ziel sendet.

Weitere Informationen finden Sie unter Asynchroner Aufruf.

Zuweisung von Ereignisquellen

Zur Verarbeitung der Elemente aus einem Stream oder einer Warteschlange können Sie eine Ereignisquellen-Zuweisung erstellen. Eine Ereignisquellen-Zuweisung ist eine Ressource in Lambda, die Elemente aus einer Amazon-Simple-Queue-Service-(Amazon-SQS)-Warteschlange, einem Amazon-Kinesis-Stream oder einem Amazon-DynamoDB-Stream liest und die Elemente in Batches an Ihre Funktion sendet. Jedes von Ihrer Funktion verarbeitete Ereignis kann Hunderte oder Tausende von Elementen enthalten.



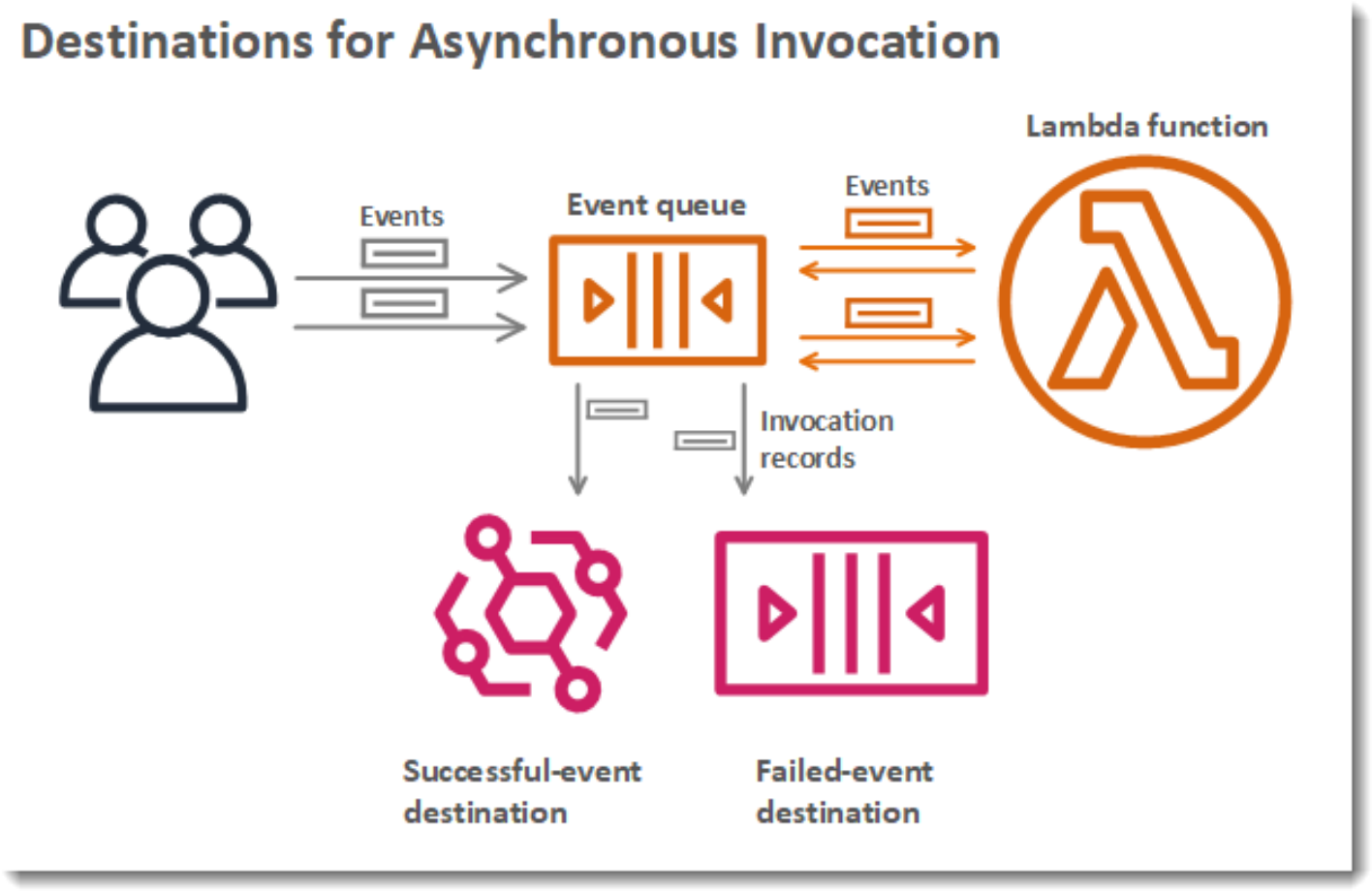
Ereignisquellen-Zuweisungen verwalten eine lokale Warteschlange mit nicht verarbeiteten Elementen und behandeln Wiederholungen, wenn die Funktion einen Fehler zurückgibt oder abgelehnt wird. Sie können eine Ereignisquellen-Zuweisung konfigurieren, um das Stapelverhalten und die Fehlerbehandlung anzupassen oder einen Datensatz von Elementen, die nicht verarbeitet werden, an ein Ziel zu senden.

Weitere Informationen finden Sie unter Wie Lambda Datensätze aus Stream- und warteschlangenbasierten Ereignisquellen verarbeitet.

Ziele

Ein Ziel ist eine AWS Ressource, die Aufrufdatensätze für eine Funktion empfängt. Für asynchrone Aufrufe können Sie konfigurieren, dass Lambda Aufrufdatensätze an eine Warteschlange, ein Thema, eine Funktion oder einen Event Bus sendet. Sie können separate Ziele für erfolgreiche Aufrufe und Ereignisse konfigurieren, bei denen die Verarbeitung fehlgeschlagen ist. Der Aufrufdatensatz enthält

Details zum Ereignis, zur Antwort der Funktion und zu dem Grund, warum der Datensatz gesendet wurde.



Bei Ereignisquellen-Mapping die aus Streams gelesen werden, können Sie konfigurieren, dass Lambda einen Datensatz mit Batches, bei denen die Verarbeitung fehlgeschlagen ist, an eine Warteschlange oder ein Thema sendet. Ein Fehlerdatensatz für eine Ereignisquellen-Zuweisung enthält Metadaten zum Stapel und weist auf die Elemente im Stream.

Weitere Informationen finden Sie unter Konfigurieren von Zielen für den asynchronen Aufruf und in den Abschnitten zur Fehlerbehandlung von Verwendung AWS Lambda mit Amazon DynamoDB und So verarbeitet Lambda Datensätze aus Amazon Kinesis Data Streams.

Funktionsentwürfe

Wenn Sie eine Funktion in der Lambda-Konsole erstellen, können Sie wählen, ob Sie von vorne anfangen, eine Vorlage verwenden oder ein Container-Image verwenden möchten. Ein Blueprint enthält Beispielcode, der zeigt, wie Lambda mit einem AWS Dienst oder einer

beliebten Drittanbieteranwendung verwendet wird. Entwürfe enthalten Beispielcode und Funktionskonfigurationsvoreinstellungen für Node.js- und Python-Laufzeiten.

Entwürfe werden zur Verwendung unter der Amazon Software License bereitgestellt. Sie sind nur in der Lambda-Konsole verfügbar.

Test- und Bereitstellungstoools

Lambda unterstützt die Bereitstellung von Code in unveränderter Form oder als Container-Images. Sie können AWS Dienste und beliebte Community-Tools wie die Docker-Befehlszeilenschnittstelle (CLI) verwenden, um Ihre Lambda-Funktionen zu erstellen, zu erstellen und bereitzustellen. Informationen zum Einrichten der Docker CLI finden Sie unter Get Docker auf der Docker Docs-Website. Eine Einführung in die Verwendung von Docker mit AWS finden Sie unter Erste Schritte mit Amazon ECR using the AWS CLI im Amazon Elastic Container Registry-Benutzerhandbuch.

Die AWS CLI und AWS SAM -CLI sind Befehlszeilentools zum Verwalten von Lambda-Anwendungs-Stacks. Zusätzlich zu Befehlen für die Verwaltung von Anwendungsstapeln mit der AWS CloudFormation API AWS CLI unterstützt The Befehle auf höherer Ebene, die Aufgaben wie das Hochladen von Bereitstellungspaketen und das Aktualisieren von Vorlagen vereinfachen. Die AWS SAM CLI bietet zusätzliche Funktionen, darunter die Validierung von Vorlagen, lokales Testen und die Integration in CI/CD-Systeme.

- Installation der AWS SAM CLI
- Testen und Debuggen serverloser Anwendungen mit AWS SAM
- Bereitstellung serverloser Anwendungen mithilfe von CI/CD-Systemen mit AWS SAM

Anwendungsvorlagen

Sie können die Lambda-Konsole verwenden, um eine Anwendung mit einer kontinuierlichen Bereitstellungs-Pipeline zu erstellen. Anwendungsvorlagen in der Lambda-Konsole enthalten Code für eine oder mehrere Funktionen, eine Anwendungsvorlage, die Funktionen und unterstützende AWS Ressourcen definiert, und eine Infrastrukturvorlage, die eine AWS CodePipeline Pipeline definiert. Die Pipeline verfügt über Entwicklungs- und Bereitstellungsphasen, die jedes Mal ausgeführt werden, wenn Sie Änderungen in das mitgelieferte Git-Repository verschieben.

Anwendungsvorlagen werden für die Verwendung unter der Lizenz MIT No Attribution zur Verfügung gestellt. Sie sind nur in der Lambda-Konsole verfügbar.

Weitere Informationen finden Sie unter Verwalten von Anwendungen in der AWS Lambda-Konsole.

Lernen Sie, wie man Serverless-Lösungen erstellt

> **Tip**
>
> Weitere Informationen zum Erstellen von Serverless-Lösungen finden Sie im Serverless-Benutzerhandbuch.

Lambda-Laufzeiten

Lambda unterstützt mehrere Sprachen durch die Verwendung von Laufzeiten. Eine Laufzeit bietet eine sprachspezifische Umgebung, die Aufrufereignisse, Kontextinformationen und Antworten zwischen Lambda und der Funktion weiterleitet. Sie können von Lambda bereitgestellte Laufzeiten verwenden oder Ihre eigenen erstellen.

Jede größere Programmiersprachenversion verfügt über eine separate Laufzeit mit einer eindeutigen Laufzeitkennung, z. B. `nodejs20.x` oder `python3.12`. Um eine Funktion für die Verwendung einer neuen Hauptsprachversion zu konfigurieren, müssen Sie die Laufzeitkennung ändern. Da die Abwärtskompatibilität zwischen Hauptversionen AWS Lambda nicht garantiert werden kann, handelt es sich um einen kundenorientierten Vorgang.

Bei einer Funktion, die als Container-Image definiert ist, wählen Sie beim Erstellen des Container-Images eine Laufzeit und die Linux-Distribution aus. Um die Laufzeit zu ändern, erstellen Sie ein neues Container-Image.

Wenn Sie ein ZIP-Dateiarchiv für das Bereitstellungspaket verwenden, wählen Sie beim Erstellen der Funktion eine Laufzeit aus. Um die Laufzeit zu ändern, können Sie die Konfiguration Ihrer Funktion aktualisieren. Die Laufzeit ist mit einer der Amazon Linux-Distributionen gepaart. Die zugrunde liegende Ausführungsumgebung bietet zusätzliche Bibliotheken und Umgebungsvariablen, auf die Sie über Ihren Funktionscode zugreifen können.

Lambda ruft Ihre Funktion in einer Ausführungsumgebung auf. Die Ausführungsumgebung bietet eine sichere und isolierte Laufzeitumgebung, die die zum Ausführen Ihrer Funktion erforderlichen Ressourcen verwaltet. Lambda verwendet die Ausführungsumgebung eines vorherigen Aufrufs wieder, sofern vorhanden, oder kann eine neue Ausführungsumgebung erstellen.

Um andere Sprachen in Lambda zu verwenden, wie Go oder Rust, verwenden Sie eine reine OS-Laufzeit. Die Lambda-Ausführungsumgebung bietet eine Laufzeitschnittstelle zum Abrufen von Aufrufereignissen und Senden von Antworten. Sie können andere Sprachen bereitstellen, indem Sie zusammen mit Ihrem Funktionscode oder in einem Layer eine benutzerdefinierte Laufzeit implementieren.

Unterstützte Laufzeiten

In der folgenden Tabelle sind die unterstützten Lambda-Laufzeiten und ihre voraussichtlichen Ablauftermine aufgeführt. Wenn eine Laufzeit als veraltet gilt, können Sie für einen begrenzten

Zeitraum weiterhin Funktionen erstellen und aktualisieren. Weitere Informationen finden Sie unter the section called “Verwendung zur Laufzeit nach Ablauf der Version”. Die Tabelle enthält die aktuell angenommenen Ablaufdaten für die Laufzeit. Diese Daten dienen zu Planungszwecken und können sich ändern.

Unterstützte Laufzeitumgebungen

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Node.js 20	`nodejs20.x`	Amazon Linux 2023			
Node.js 18	`nodejs18.x`	Amazon Linux 2			
Node.js 16	`nodejs16.x`	Amazon Linux 2	12. Juni 2024	28. Februar 2025	31. März 2025
Python 3.12	`python3.12`	Amazon Linux 2023			
Python 3.11	`python3.11`	Amazon Linux 2			
Python 3.10	`python3.10`	Amazon Linux 2			
Python 3.9	`python3.9`	Amazon Linux 2			
Python 3.8	`python3.8`	Amazon Linux 2	14. Oktober 202	28. Februar 2025	31. März 2025
Java 21	`java21`	Amazon Linux 2023			
Java 17	`java17`	Amazon Linux 2			

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Java 11	`java11`	Amazon Linux 2			
Java 8	`java8.al2`	Amazon Linux 2			
.NET 8	`dotnet8`	Amazon Linux 2023			
.NET 6	`dotnet6`	Amazon Linux 2	12. November 2	28. Februar 2025	31. März 2025
Rubin 3.3	`ruby3.3`	Amazon Linux 2023			
Ruby 3.2	`ruby3.2`	Amazon Linux 2			
Reine OS-Laufzeit	`provided.al2023`	Amazon Linux 2023			
Reine OS-Laufzeit	`provided.al2`	Amazon Linux 2			

> **Note**
>
> Für neue Regionen wird Lambda keine Laufzeiten unterstützen, die innerhalb der nächsten sechs Monate veraltet sein werden.

Lambda hält verwaltete Laufzeiten und ihre entsprechenden Container-Basis-Images mit Patches und Unterstützung für kleinere Versionen auf dem neuesten Stand. Weitere Informationen finden Sie unter Lambda-Laufzeitaktualisierungen.

Lambda unterstützt weiterhin die Programmiersprache Go, auch nachdem die Go 1.x-Laufzeit veraltet ist. Weitere Informationen finden Sie im Compute-Blog unter AWS Lambda Funktionen von der GO1.x-Laufzeit zur benutzerdefinierten Laufzeit auf Amazon Linux 2 migrieren.AWS

Alle unterstützten Lambda-Laufzeiten unterstützen sowohl x86_64- als auch arm64-Architekturen.

Neue Laufzeit-Versionen

Lambda stellt verwaltete Laufzeiten für neue Sprachversionen nur dann zur Verfügung, wenn die Version die LTS-Phase (Long-Term Support) des Veröffentlichungszyklus der Sprache erreicht. Zum Beispiel für den Node.js-Veröffentlichungszyklus, wenn die Version die Active LTS-Phase erreicht.

Bevor die Version die LTS-Phase erreicht, befindet sie sich noch in der Entwicklung und kann noch grundlegenden Änderungen unterliegen. Lambda wendet Laufzeit-Updates standardmäßig automatisch an. Wenn Sie also Änderungen an einer Laufzeitversion vornehmen, funktionieren Ihre Funktionen möglicherweise nicht mehr wie erwartet.

Lambda bietet keine verwalteten Laufzeiten für Sprachversionen, die nicht für die LTS-Veröffentlichung geplant sind.

Im Folgenden ist der geplante Startmonat für die kommenden Lambda-Laufzeiten aufgeführt. Diese Termine sind nur Richtwerte und können sich ändern.

- Python 3.13 – November 2024
- Node.js 22 – November 2024

Richtlinie für den Laufzeitablauf

Lambda-Laufzeiten für ZIP-Dateiarchive werden um eine Kombination aus Betriebssystem, Programmiersprache und Softwarebibliotheken aufgebaut, die Wartungen und Sicherheits-Updates erfordern. Die Standardrichtlinie von Lambda sieht vor, dass eine Laufzeit als veraltet eingestuft wird, wenn für eine wichtige Komponente der Laufzeit der Community Long-Term Support (LTS) ausläuft und keine Sicherheitsupdates mehr verfügbar sind. In den meisten Fällen handelt es sich dabei um die Sprachlaufzeit. In einigen Fällen kann eine Laufzeit jedoch als veraltet gelten, weil das Betriebssystem das LTS-Ende erreicht.

Wenn eine Runtime veraltet ist, AWS darf sie keine Sicherheitspatches oder Updates mehr auf diese Runtime anwenden und Funktionen, die diese Runtime verwenden, haben keinen Anspruch mehr auf technischen Support. Solche veralteten Laufzeiten werden „wie sie sind“ ohne jegliche

Gewährleistung bereitgestellt und können Bugs, Fehler, Defekte oder andere Sicherheitslücken enthalten.

Weitere Informationen zur Verwaltung von Runtime-Upgrades und veralteten Versionen finden Sie in den folgenden Abschnitten und unter AWS Lambda Runtime-Upgrades verwalten im Compute-Blog.AWS

> **Important**
>
> Lambda verzögert gelegentlich die Einstellung einer Lambda-Laufzeit für einen begrenzten Zeitraum über das Ende der Unterstützung der Sprachversion hinaus, die von der Laufzeit unterstützt wird. Während dieses Zeitraums wendet Lambda nur Sicherheits-Patches auf das Laufzeit-Betriebssystem an. Lambda wendet keine Sicherheits-Patches auf Laufzeiten von Programmiersprachen an, nachdem diese das Ende der Unterstützung erreicht haben.

Veraltete Laufzeit für Node.js 16

Als Reaktion auf Kundenfeedback verschiebt AWS sich die Einstellung der Laufzeit von Node.js 16 bis 9 Monate nach dem Ende von Community-LTS. Die Laufzeit für Node.js 16 wird an dem Datum eingestellt, das in der Tabelle „Unterstützte Laufzeitumgebungen“ angegeben ist. Wie in der vorherigen Anmerkung erwähnt, wird Lambda zwischen dem Ende der LTS am 11. September 2023 und dem Einstellungsdatum nur Betriebssystem-Patches auf die Laufzeit anwenden. In diesem Zeitraum werden keine Sicherheits-Patches für die Sprachlaufzeit angewendet.

Durch die Verzögerung der Einstellung von Node.js 16 haben Kunden, die diese Laufzeit verwenden, die Möglichkeit, ihre Funktionen direkt auf Node.js 20 zu migrieren und Node.js 18 zu überspringen.

Modell der geteilten Verantwortung

Lambda ist verantwortlich für die Kuratierung und Veröffentlichung von Sicherheitsupdates für alle unterstützten verwalteten Laufzeiten und Container-Basis-Images. Standardmäßig wendet Lambda diese Updates automatisch auf Funktionen an, die verwaltete Laufzeiten verwenden. Wenn die Standardeinstellung für automatische Laufzeitaktualisierungen geändert wurde, finden Sie weitere Informationen im Modell der gemeinsamen Verantwortung von Runtime Management Controls. Bei Funktionen, die mithilfe von Container-Images bereitgestellt werden, sind Sie dafür verantwortlich, das Container-Image Ihrer Funktion aus dem neuesten Basis-Image neu zu erstellen und das Container-Image erneut bereitzustellen.

Wenn eine Laufzeit veraltet ist, entfällt die Verantwortung von Lambda für die Aktualisierung der verwalteten Laufzeit- und Container-Basis-Images. Sie sind dafür verantwortlich, Ihre Funktionen so zu aktualisieren, dass sie ein unterstütztes Laufzeit- oder Basis-Image verwenden.

In allen Fällen sind Sie dafür verantwortlich, Aktualisierungen an Ihrem Funktionscode, einschließlich seiner Abhängigkeiten, vorzunehmen. Ihre Verantwortlichkeiten im Rahmen des Modells der gemeinsamen Verantwortung sind in der folgenden Tabelle zusammengefasst.

Phase des Lebenszyklus der Laufzeit	Die Aufgaben von Lambda	Ihre Aufgaben
Unterstützte verwaltete Laufzeit	Stellen Sie regelmäßige Runtime-Updates mit Sicherheitspatches und anderen Updates bereit. Wenden Sie Runtime-Updates standardmäßig automatisch an (Informationen zu nicht standardmäßigen Verhaltensweisen finden Sie unterthe section called “Kontrollen der Laufzeitverwaltung”).	Aktualisieren Sie Ihren Funktionscode, einschließlich der Abhängigkeiten, um Sicherheitslücken zu schließen.
Unterstütztes Container-Image	Stellen Sie regelmäßige Updates für das Container-Basisimage mit Sicherheitspatches und anderen Updates bereit.	Aktualisieren Sie Ihren Funktionscode, einschließlich der Abhängigkeiten, um Sicherheitslücken zu schließen. Erstellen Sie Ihr Container-Image regelmäßig neu und stellen Sie es erneut bereit, indem Sie das neueste Basis-Image verwenden.
Verwaltete Laufzeit nähert sich dem Verfall	Informieren Sie Kunden per Dokumentation, E-Mail und,	Überwachen Sie die Lambda-Dokumentation AWS Health

Phase des Lebenszyklus der Laufzeit	Die Aufgaben von Lambda	Ihre Aufgaben
	AWS Health Dashboard bevor Runtime nicht mehr unterstützt wird. Trusted Advisor Die Verantwortung für Runtime-Updates endet, wenn sie veraltet sind.	Dashboard, E-Mails oder Informationen Trusted Advisor zu veralteten Laufzeiten. Führen Sie ein Upgrade von Funktionen auf eine unterstützte Laufzeit durch, bevor die vorherige Laufzeit veraltet ist.
Container-Image wird bald veraltet	Benachrichtigungen über veraltete Versionen sind für Funktionen, die Container-Images verwenden, nicht verfügbar. Die Verantwortung für die Aktualisierung von Container-Basis-Images endet mit dem Zeitpunkt ihrer Veröffentlichung.	Beachten Sie die Zeitpläne für veraltete Versionen und aktualisieren Sie Funktionen auf ein unterstütztes Basis-Image, bevor das vorherige Image veraltet ist.

Verwendung zur Laufzeit nach Ablauf der Version

Wenn eine Runtime als veraltet gilt, AWS darf sie keine Sicherheitspatches oder Updates mehr auf diese Runtime anwenden, und Funktionen, die diese Runtime verwenden, sind nicht mehr für technischen Support berechtigt. Solche veralteten Laufzeiten werden „wie sie sind“ ohne jegliche Gewährleistung bereitgestellt und können Bugs, Fehler, Defekte oder andere Sicherheitslücken enthalten. Bei Funktionen, die eine veraltete Runtime verwenden, kann es auch zu Leistungseinbußen oder anderen Problemen kommen, z. B. wenn das Zertifikat abläuft, die dazu führen können, dass sie nicht mehr richtig funktionieren.

Mindestens 30 Tage, nachdem eine Laufzeit als veraltet gilt, können Sie noch neue Lambda-Funktionen mit dieser Laufzeit erstellen. 30 Tage nach Ende der Unterstützung beginnt Lambda, die Erstellung neuer Funktionen zu blockieren.

Sie können den Funktionscode und die Konfiguration vorhandener Funktionen noch mindestens 60 Tage lang aktualisieren, nachdem eine Runtime veraltet ist. Ab 60 Tagen nach der Deprecation beginnt Lambda, die Aktualisierung von Funktionscode und Konfiguration für bestehende Funktionen zu blockieren.

> **Note**
>
> Bei einigen Laufzeiten werden die AWS block-function-update Enddaten über die üblichen 30 block-function-create und 60 Tage nach der Deprecation hinaus verschoben. AWS hat diese Änderung als Reaktion auf Kundenfeedback vorgenommen, damit Sie mehr Zeit haben, Ihre Funktionen zu aktualisieren. Die Daten für Ihre Laufzeit finden the section called “Veraltete Laufzeitumgebungen” Sie in den Tabellen unter the section called “Unterstützte Laufzeiten” und.

Sie können eine Funktion so aktualisieren, dass sie auf unbestimmte Zeit eine neuere unterstützte Laufzeit verwendet, nachdem eine Laufzeit veraltet ist. Sie sollten testen, ob Ihre Funktion mit der neuen Laufzeit funktioniert, bevor Sie die Laufzeitänderung in Produktionsumgebungen anwenden, da Sie nach Ablauf der 60-Tage-Frist nicht mehr zur veralteten Laufzeit zurückkehren können. Wir empfehlen die Verwendung von Funktionsversionen und Aliasnamen, um eine sichere Bereitstellung mit Rollback zu ermöglichen.

Beachten Sie, dass die genaue Dauer, für die Sie weiterhin Funktionen erstellen und aktualisieren können, nicht festgelegt ist. Dieser Zeitraum kann für jede veraltete Version und für verschiedene Versionen unterschiedlich sein. AWS-Regionen Nominelle Termine für die Blockierung von Funktionserstellungen und -aktualisierungen finden Sie in der Tabelle „Unterstützte Laufzeiten“ im ersten Abschnitt dieser Seite. Lambda beginnt nicht vor den in dieser Tabelle angegebenen Terminen mit dem Blockieren von Funktionserstellungen oder -aktualisierungen.

Sie können Ihre Funktionen auf unbestimmte Zeit weiter aufrufen, auch wenn die Laufzeit veraltet ist. Es wird jedoch AWS dringend empfohlen, Funktionen auf eine unterstützte Runtime zu migrieren, damit Ihre Funktionen weiterhin Sicherheitspatches erhalten und weiterhin Anspruch auf technischen Support haben.

Empfangen von Benachrichtigungen über veraltete Laufzeitversionen

Wenn sich eine Laufzeit ihrem Verfallsdatum nähert, sendet Lambda Ihnen eine E-Mail-Benachrichtigung, falls Funktionen in Ihrer Umgebung diese Laufzeit AWS-Konto verwenden. Benachrichtigungen werden auch in und in angezeigt. AWS Health Dashboard AWS Trusted Advisor

- Empfangen von E-Mail-Benachrichtigungen:

  Lambda sendet Ihnen mindestens 180 Tage, bevor eine Laufzeit veraltet ist, eine E-Mail-Warnung. In dieser E-Mail sind die $LATEST-Versionen aller Funktionen aufgeführt, die die Laufzeit verwenden. Eine vollständige Liste der betroffenen Funktionsversionen finden Sie unter Trusted Advisor oderthe section called “Listet Funktionen auf, die eine veraltete Runtime verwenden”.

  Lambda sendet eine E-Mail-Benachrichtigung an Ihren AWS-Konto primären Kontokontakt. Informationen zum Anzeigen oder Aktualisieren der E-Mail-Adressen in Ihrem Konto finden Sie in der allgemeinen AWS -Referenz unter Updating contact information.
- Empfangen von Benachrichtigungen über: AWS Health Dashboard

  AWS Health Dashboard Zeigt mindestens 180 Tage, bevor eine Laufzeit veraltet ist, eine Benachrichtigung an. Benachrichtigungen werden auf der Seite Ihr Kontostatus unter Andere Benachrichtigungen angezeigt. Auf der Registerkarte Betroffene Ressourcen in der Benachrichtigung sind die $LATEST-Versionen aller Funktionen aufgeführt, die die Laufzeit verwenden.

  > **Note**
  >
  > Eine vollständige up-to-date Liste der betroffenen Funktionsversionen finden Sie unter Trusted Advisor oder. the section called “Listet Funktionen auf, die eine veraltete Runtime verwenden”

  AWS Health Dashboard Benachrichtigungen laufen 90 Tage ab, nachdem die betroffene Runtime veraltet ist.
- Verwenden AWS Trusted Advisor

  Trusted Advisor zeigt 180 Tage, bevor eine Laufzeit veraltet ist, eine Benachrichtigung an. Benachrichtigungen werden auf der Seite Sicherheit angezeigt. Eine Liste der betroffenen

Funktionen wird unter AWS Lambda -Funktionen, die veraltete Laufzeiten verwenden angezeigt. Diese Liste von Funktionen zeigt sowohl die $LATEST als auch veröffentlichte Versionen und wird automatisch aktualisiert, um den aktuellen Status Ihrer Funktionen widerzuspiegeln.

Sie können wöchentliche E-Mail-Benachrichtigungen auf der Trusted Advisor Seite „Einstellungen“ der Trusted Advisor Konsole aktivieren.

Listet Funktionen auf, die eine veraltete Runtime verwenden

Sie können nicht nur eine Live-Liste der Funktionen anzeigen, die von geplanten Laufzeitveraltungen betroffen sind, sondern auch das AWS Command Line Interface (AWS CLI) oder eines der AWS SDKs verwenden, um all Ihre Funktionsversionen aufzulisten, die eine bestimmte Laufzeit verwenden. Trusted Advisor

Führen Sie den folgenden Befehl aus AWS CLI, um diese Liste mit dem zu generieren. `RUNTIME_IDENTIFIER`Ersetzen Sie es durch den Namen der Laufzeit, die veraltet ist, und wählen Sie Ihren eigenen aus. AWS-Region Um nur die $LATEST-Funktionsversionen aufzulisten, lassen Sie `--function-version ALL` im Befehl weg.

```
aws lambda list-functions --function-version ALL --region us-east-1 --output text --
query "Functions[?Runtime=='RUNTIME_IDENTIFIER'].FunctionArn"
```

> **Tip**
>
> Der Beispielbefehl listet Funktionen in der `us-east-1` Region für eine bestimmte Region auf. AWS-Konto Sie müssen diesen Befehl für jede Region wiederholen, in der Ihr Konto Funktionen hat, und für jede Ihrer Regionen. AWS-Konten

Weitere Informationen zur Verwendung eines AWS SDK zum Auflisten Ihrer Funktionen, die die ListFunctionsAktion verwenden, finden Sie in der SDK-Dokumentation für Ihre bevorzugte Programmiersprache. Sie können auch eines der AWS SDKs verwenden, um mithilfe der API-Aktionen DescribeLogStreams und GetMetric Statistics Statistiken Statistiken über Ihre am häufigsten aufgerufenen most-recently-invoked Funktionen zu sammeln.

Sie können auch die Funktion für AWS Config erweiterte Abfragen verwenden, um all Ihre Funktionen aufzulisten, die eine betroffene Laufzeit verwenden. Diese Abfrage gibt nur die Versionen der Funktion $LATEST zurück, aber Sie können Abfragen aggregieren, um Funktionen für alle Regionen

und mehrere Regionen AWS-Konten mit einem einzigen Befehl aufzulisten. Weitere Informationen finden Sie unter Abfragen des aktuellen Konfigurationsstatus von AWS Auto Scaling Ressourcen im AWS Config Entwicklerhandbuch.

Veraltete Laufzeitumgebungen

Die folgenden Laufzeiten haben das Ende der Unterstützung erreicht:

Veraltete Laufzeitumgebungen

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
.NET 7 (nur Container)	`dotnet7`	Amazon Linux 2	14. Mai 2024		
Java 8	`java8`	Amazon Linux	8. Januar 2024	8. Februar 2024	28. Februar 2025
Go 1.x	`go1.x`	Amazon Linux	8. Januar 2024	8. Februar 2024	28. Februar 2025
Reine OS-Laufzeit	`provided`	Amazon Linux	8. Januar 2024	8. Februar 2024	28. Februar 2025
Ruby 2.7	`ruby2.7`	Amazon Linux 2	7. Dezember 20	9. Januar 2024	28. Februar 2025
Node.js 14	`nodejs14.x`	Amazon Linux 2	4. Dezember 20	9. Januar 2024	28. Februar 2025
Python 3.7	`python3.7`	Amazon Linux	4. Dezember 20	9. Januar 2024	28. Februar 2025
.NET Core 3.1	`dotnetcore3.1`	Amazon Linux 2	3. Apr 2023	3. Apr 2023	3. Mai 2023
Node.js 12	`nodejs12.x`	Amazon Linux 2	31. März 2023	31. März 2023	30. Apr 2023

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Python 3.6	`python3.6`	Amazon Linux	18. Juli 2022	18. Juli 2022	29. August 2022
.NET 5 (nur Container)	`dotnet5.0`	Amazon Linux 2	10. Mai 2022		
.NET Core 2.1	`dotnetcore2.1`	Amazon Linux	5. Januar 2022	5. Januar 2022	13. Apr 2022
Node.js 10	`nodejs10.x`	Amazon Linux 2	30. Juli 2021	30. Juli 2021	14. Februar 2022
Ruby 2.5	`ruby2.5`	Amazon Linux	30. Juli 2021	30. Juli 2021	31. März 2022
Python 2.7	`python2.7`	Amazon Linux	15. Juli 2021	15. Juli 2021	30. Mai 2022
Node.js 8.10	`nodejs8.10`	Amazon Linux	6. März 2020		6. März 2020
Node.js 4.3	`nodejs4.3`	Amazon Linux	5. März 2020		5. März 2020
Node.js 4.3 edge	`nodejs4.3-edge`	Amazon Linux	5. März 2020		30. Apr 2019
Node.js 6.10	`nodejs6.10`	Amazon Linux	12. August 201	12. August 201	
.NET Core 1.0	`dotnetcore1.0`	Amazon Linux	27. Juni 2019		30. Juli 2019
.NET Core 2.0	`dotnetcore2.0`	Amazon Linux	30. Mai 2019		30. Mai 2019

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Node.js 0.10	`nodejs`	Amazon Linux			31. Oktober 2016

In fast allen Fällen ist das end-of-life Datum einer Sprachversion oder eines Betriebssystems weit im Voraus bekannt. Die folgenden Links enthalten end-of-life Zeitpläne für jede Sprache, die Lambda als verwaltete Laufzeit unterstützt.

Richtlinien für die Unterstützung von Sprache und Framework-Bedingungen

- Node.js – github.com
- Python – devguide.python.org
- Ruby – www.ruby-lang.org
- Java – www.oracle.com and Corretto FAQs
- Go – golang.org
- .NET – dotnet.microsoft.com

Lambda-Laufzeitaktualisierungen

Lambda hält jede verwaltete Laufzeit mit Sicherheitsupdates, Fehlerbehebungen, neuen Funktionen, Leistungsverbesserungen und Unterstützung für Nebenversionen auf dem neuesten Stand. Diese Laufzeitaktualisierungen werden als Laufzeitversionen veröffentlicht. Lambda wendet Laufzeitaktualisierungen auf Funktionen an, indem es die Funktion von einer früheren Laufzeitversion auf eine neue Laufzeitversion migriert.

Für Funktionen, die verwaltete Laufzeiten verwenden, wendet Lambda Laufzeitaktualisierungen standardmäßig automatisch an. Mit automatischen Laufzeitaktualisierungen übernimmt Lambda den operativen Aufwand für das Patchen der Laufzeitversionen. Für die meisten Kunden sind automatische Aktualisierungen die richtige Wahl. Weitere Informationen finden Sie unter Kontrollen der Laufzeitverwaltung.

Lambda veröffentlicht auch jede neue Laufzeitversion als Container-Image. Um Laufzeitversionen für Container-basierte Funktionen zu aktualisieren, müssen Sie ein neues Container-Image aus dem aktualisierten Basis-Image erstellen und Ihre Funktion erneut bereitstellen.

Jeder Laufzeitversion ist eine Versionsnummer und ein ARN (Amazon Resource Name) zugeordnet. Laufzeitversionsnummern verwenden ein von Lambda definiertes Nummerierungsschema, unabhängig von den Versionsnummern, die die Programmiersprache verwendet. Der Laufzeitversions-ARN ist eine eindeutige Kennung für jede Laufzeitversion.

Sie können den ARN der aktuellen Laufzeitversion Ihrer Funktion in der `INIT_START`-Zeile Ihrer Funktionsprotokolle und in der Lambda-Konsole anzeigen.

Laufzeitversionen sollten nicht mit Laufzeitkennungen verwechselt werden. Jede Laufzeit hat eine eindeutige Laufzeitkennung, z. B. `python3.9` oder `nodejs18.x`. Diese entsprechen den jeweiligen Hauptversionen der Programmiersprachen. Laufzeitversionen beschreiben die Patch-Version einer einzelnen Laufzeit.

> **Note**
>
> Der ARN für dieselbe Laufzeitversionsnummer kann zwischen AWS-Regionen und CPU-Architekturen variieren.

Themen

- Kontrollen der Laufzeitverwaltung
- Zweiphasiges Rollout der Laufzeitversion
- Zurücksetzen einer Laufzeitversion
- Identifizieren von Änderungen der Laufzeitversion
- Konfigurieren von Einstellungen für die Laufzeitverwaltung
- Modell der geteilten Verantwortung
- Anwendungen mit hoher Compliance

Kontrollen der Laufzeitverwaltung

Lambda ist bestrebt, Laufzeitaktualisierungen bereitzustellen, die mit vorhandenen Funktionen abwärtskompatibel sind. Wie beim Software-Patching gibt es jedoch seltene Fälle, in denen sich eine Laufzeitaktualisierung negativ auf eine vorhandene Funktion auswirken kann. Beispielsweise können Sicherheits-Patches ein zugrunde liegendes Problem mit einer vorhandenen Funktion aufdecken, das vom vorherigen, unsicheren Verhalten abhängt. Lambda-Laufzeitverwaltungskontrollen tragen dazu bei, das Risiko von Auswirkungen auf Ihre Workloads im seltenen Fall einer Inkompatibilität einer Laufzeitversion zu verringern. Für jede Funktionsversion (`$LATEST` oder veröffentlichte Version) können Sie einen der folgenden Laufzeitaktualisierungsmodi wählen:

- Automatisch (Standard) – Automatische Aktualisierung auf die neueste und sicherste Laufzeitversion mit Zweiphasiges Rollout der Laufzeitversion. Diesen Modus empfehlen wir den meisten Kunden, damit Sie immer von Laufzeitaktualisierungen profitieren.
- Funktion aktualisieren – Aktualisieren Sie die Laufzeit Ihrer Funktion auf die neueste und sicherste Laufzeitversion. Wenn Sie Ihre Funktion aktualisieren, aktualisiert Lambda die Laufzeit Ihrer Funktion auf die neueste und sicherste Laufzeitversion. Dieser Ansatz synchronisiert Laufzeitaktualisierungen mit Funktionsbereitstellungen, sodass Sie die Kontrolle darüber haben, wann Lambda Laufzeitaktualisierungen anwendet. In diesem Modus können Sie seltene Inkompatibilitäten bei Laufzeitaktualisierungen frühzeitig erkennen und beheben. Wenn Sie diesen Modus verwenden, müssen Sie Ihre Funktionen regelmäßig aktualisieren, um deren Laufzeit auf dem neuesten Stand zu halten.
- Manuell – Aktualisieren Sie Ihre Laufzeitversion manuell. Sie geben in Ihrer Funktionskonfiguration eine Laufzeitversion an. Die Funktion verwendet diese Laufzeitversion unbegrenzt. In dem seltenen Fall, dass eine neue Laufzeitversion mit einer vorhandenen Funktion nicht kompatibel ist, können Sie diesen Modus verwenden, um Ihre Funktion auf eine frühere Laufzeitversion zurückzusetzen. Wir raten davon ab, den Modus Manual (Manuell) zu verwenden, um Laufzeitkonsistenz über

Bereitstellungen hinweg zu erreichen. Weitere Informationen finden Sie unter Zurücksetzen einer Laufzeitversion.

Die Verantwortung für das Anwenden von Laufzeitaktualisierungen auf Ihre Funktionen hängt davon ab, welchen Laufzeitaktualisierungsmodus Sie auswählen. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

Zweiphasiges Rollout der Laufzeitversion

Lambda führt neue Laufzeitversionen in der folgenden Reihenfolge ein:

1. In der ersten Phase wendet Lambda die neue Laufzeitversion an, sobald Sie eine Funktion erstellen oder aktualisieren. Eine Funktion wird aktualisiert, wenn Sie die - UpdateFunctionCode oder UpdateFunctionConfiguration-API-Operationen aufrufen.
2. In der zweiten Phase aktualisiert Lambda alle Funktionen, die den Auto (Automatischen) Laufzeitaktualisierungsmodus verwenden und die noch nicht auf die neue Laufzeitversion aktualisiert wurden.

Die Gesamtdauer des Rollout-Prozesses hängt von mehreren Faktoren ab, einschließlich des Schweregrads von Sicherheits-Patches, die in der Laufzeitaktualisierung enthalten sind.

Wenn Sie Ihre Funktionen aktiv entwickeln und bereitstellen, werden Sie höchstwahrscheinlich in der ersten Phase neue Laufzeitversionen abrufen. Dadurch werden Laufzeitaktualisierungen mit Funktionsaktualisierungen synchronisiert. In dem seltenen Fall, dass die neueste Laufzeitversion Ihre Anwendung negativ beeinflusst, können Sie mit diesem Ansatz, umgehend Korrekturmaßnahmen ergreifen. Funktionen, die sich nicht in der aktiven Entwicklung befinden, erhalten auch in der zweiten Phase den operativen Nutzen von automatischen Laufzeitaktualisierungen.

Dieser Ansatz wirkt sich nicht auf Funktionen aus, die auf Function update (Funktionsaktualisierung) oder Manual (Manuell) festgelegt sind. Funktionen, die den Modus Function update (Funktionsaktualisierung) verwenden, erhalten die neuesten Laufzeitaktualisierungen nur, wenn Sie sie erstellen oder aktualisieren. Funktionen, die den Modus Manual (Manuell) verwenden, erhalten keine Laufzeitaktualisierungen.

Lambda veröffentlicht neue Laufzeitversionen schrittweise und fortlaufend in allen AWS-Regionen. Wenn Ihre Funktionen auf die Modi Auto (Automatisch) oder Function update (Funktionsaktualisierung) festgelegt sind, ist es möglich, dass Funktionen, die zur gleichen Zeit in verschiedenen Regionen oder zu verschiedenen Zeiten in derselben Region eingesetzt

werden, unterschiedliche Laufzeitversionen abrufen. Kunden, die eine garantierte Konsistenz der Laufzeitversionen in ihren Umgebungen benötigen, sollten Container-Images verwenden, um ihre Lambda-Funktionen bereitzustellen. Der Modus Manuell ist als vorübergehende Gegenmaßnahme gedacht, um im seltenen Fall eines Laufzeitzeitproblems ein Laufzeit-Rollback zu ermöglichen, dass eine Laufzeitversion nicht mit Ihrer Funktion kompatibel ist.

Zurücksetzen einer Laufzeitversion

In dem seltenen Ereignis, dass eine neue Laufzeitversion nicht mit Ihrer vorhandenen Funktion kompatibel ist, können Sie deren Laufzeitversion auf eine frühere Version zurücksetzen. Dadurch bleibt Ihre Anwendung funktionsfähig und die Unterbrechung wird minimiert. Gleichzeitig wird Zeit bereitgestellt, um die Inkompatibilität zu beheben, bevor Sie zur neuesten Laufzeitversion zurückkehren.

Lambda legt keine zeitliche Begrenzung fest, wie lange Sie eine bestimmte Laufzeitversion verwenden können. Wir empfehlen jedoch dringend, so schnell wie möglich auf die neueste Laufzeitversion zu aktualisieren, um von den neuesten Sicherheits-Patches, Leistungsverbesserungen und Funktionen zu profitieren. Lambda bietet die Option, auf eine frühere Laufzeitversion zurückzusetzen, nur als vorübergehende Abhilfe für den seltenen Fall eines Kompatibilitätsproblems bei Laufzeitaktualisierungen. Bei Funktionen, die über einen längeren Zeitraum eine frühere Laufzeitversion verwenden, kann es zu Leistungseinbußen oder Problemen kommen, wie z. B. dem Ablauf eines Zertifikats, was dazu führen kann, dass sie nicht mehr richtig funktionieren.

Sie können eine Laufzeitversion auf die folgenden Arten zurücksetzen:

- Verwenden des Manual (Manuellen) Laufzeitaktualisierungsmodus
- Verwenden veröffentlichter Funktionsversionen

Weitere Informationen finden Sie unter Einführung von AWS Lambda-Laufzeitverwaltungs-Kontrollen im AWS-Computing-Blog.

Rollback einer Laufzeitversion mit dem Manual (Manuellen) Laufzeitaktualisierungsmodus

Wenn Sie den Auto (Automatischen) Aktualisierungsmodus für die Laufzeitversion oder die `$LATEST`-Laufzeitversion verwenden, können Sie Ihre Laufzeitversion im Manual (Manuellen) Modus zurücksetzen. Ändern Sie für die Funktionsversion, die Sie zurücksetzen möchten, den

Aktualisierungsmodus der Laufzeitversion zu Manual (Manuell) und geben Sie den ARN der vorherigen Laufzeitversion an. Weitere Informationen zum Ermitteln des ARN der vorherigen Laufzeitversion finden Sie unter Identifizieren von Änderungen der Laufzeitversion.

> **Note**
>
> Wenn die `$LATEST`-Version Ihrer Funktion für den Modus Manual (Manuell) konfiguriert ist, können Sie die von Ihrer Funktion verwendete CPU-Architektur oder Laufzeitversion nicht ändern. Um diese Änderungen vorzunehmen, müssen Sie in den Modus Auto (Automatisch) oder Function update (Funktionsaktualisierung) wechseln.

Rollback einer Laufzeitversion mit veröffentlichten Funktionsversionen

Veröffentlichte Funktionsversionen sind eine unveränderliche Momentaufnahme des `$LATEST`-Funktionscodes und der Konfiguration zum Zeitpunkt ihrer Erstellung. Im Modus Auto (Automatisch) aktualisiert Lambda während der zweiten Phase des Rollouts der Laufzeitversion automatisch die Laufzeitversion der veröffentlichten Funktionsversionen. Im Modus Function update (Funktionsaktualisierung) aktualisiert Lambda die Laufzeitversion veröffentlichter Funktionsversionen nicht.

Veröffentlichte Funktionsversionen, die den Modus Function update (Funktionsaktualisierung) verwenden, erstellen daher einen statischen Snapshot des Funktionscodes, der Konfiguration und der Laufzeitversion. Wenn Sie den Modus Function update (Funktionsaktualisierung) mit Funktionsversionen verwenden, können Sie Laufzeitaktualisierungen mit Ihren Bereitstellungen synchronisieren. Sie können auch das Rollback von Code-, Konfigurations- und Laufzeitversionen koordinieren, indem Sie den Datenverkehr auf eine zuvor veröffentlichte Funktionsversion umleiten. Sie können diesen Ansatz in Ihre kontinuierliche Integration und kontinuierliche Bereitstellung (CI/CD) integrieren, um im seltenen Fall einer Inkompatibilität von Laufzeitaktualisierungen ein vollautomatisches Rollback durchzuführen. Wenn Sie diesen Ansatz verwenden, müssen Sie Ihre Funktion regelmäßig aktualisieren und neue Funktionsversionen veröffentlichen, um die neuesten Laufzeitaktualisierungen zu erhalten. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

Identifizieren von Änderungen der Laufzeitversion

Die Laufzeitversionsnummer und der ARN werden in der `INIT_START` Protokollzeile protokolliert, die Lambda jedes Mal an CloudWatch Logs ausgibt, wenn es eine neue Ausführungsumgebung erstellt.

Da die Ausführungsumgebung für alle Funktionsaufrufe dieselbeLaufzeit verwendet, gibt Lambda die `INIT_START`-Protokollzeile nur aus, wenn Lambda die Init-Phase ausführt. Lambda gibt diese Protokollzeile nicht für jeden Funktionsaufruf aus. Lambda gibt die Protokollzeile an CloudWatch Protokolle aus, sie ist jedoch in der Konsole nicht sichtbar.

Example Beispiel für die INIT_START-Protokollzeile

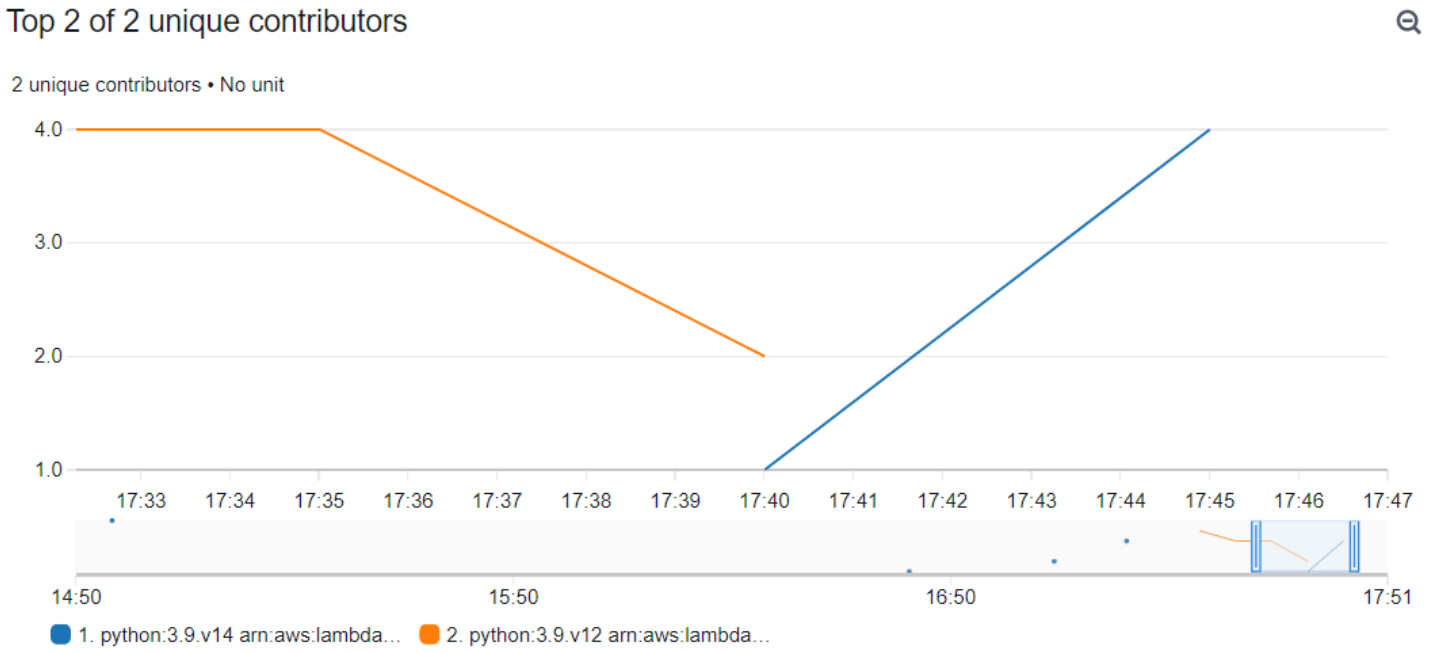
```
INIT_START Runtime Version: python:3.9.v14    Runtime Version ARN: arn:aws:lambda:eu-
south-1::runtime:7b620fc2e66107a1046b140b9d320295811af3ad5d4c6a011fad1fa65127e9e6I
```

Anstatt direkt mit den Protokollen zu arbeiten, können Sie Amazon CloudWatch Contributor Insights verwenden, um Übergänge zwischen Laufzeitversionen zu identifizieren. Die folgende Regel zählt die verschiedenen Laufzeitversionen aus jeder `INIT_START`-Protokollzeile. Um die Regel zu verwenden, ersetzen Sie den Beispiel-Protokollgruppennamen `/aws/lambda/*` durch das entsprechende Präfix für Ihre Funktion oder Funktionsgruppe.

```
{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "eventType",
        "In": [
          "INIT_START"
        ]
      }
    ],
    "Keys": [
      "runtimeVersion",
      "runtimeVersionArn"
    ]
  },
  "LogFormat": "CLF",
  "LogGroupNames": [
    "/aws/lambda/*"
  ],
  "Fields": {
    "1": "eventType",
```

```
    "4": "runtimeVersion",
    "8": "runtimeVersionArn"
  }
}
```

Der folgende CloudWatch Contributor-Insights-Bericht zeigt ein Beispiel für einen Laufzeitversionsübergang, wie er von der vorherigen Regel erfasst wird. Die orange Linie zeigt die Initialisierung der Ausführungsumgebung für die frühere Laufzeitversion (python:3.9.v12), während die blaue Linie die Initialisierung der Ausführungsumgebung für die neue Laufzeitversion (python:3.9.v14) anzeigt.



Konfigurieren von Einstellungen für die Laufzeitverwaltung

Sie können die Laufzeitverwaltungseinstellungen mithilfe der Lambda-Konsole oder der AWS Command Line Interface (AWS CLI) konfigurieren.

> **Note**
>
> Sie können die Laufzeitverwaltungseinstellungen für jede Funktionsversion separat konfigurieren.

So konfigurieren Sie, wie Lambda Ihre Laufzeitversion aktualisiert (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie auf der Registerkarte Code unter Runtime settings (Laufzeiteinstellungen) die Option Edit runtime management configuration (Laufzeitverwaltungskonfiguration bearbeiten) aus.
4. Wählen Sie unter Runtime management configuration (Laufzeitverwaltungskonfiguration) eine der folgenden Optionen aus:

   - Um Ihre Funktion automatisch auf die neueste Laufzeitversion aktualisieren zu lassen, wählen Sie Auto (Automatisch).
   - Um Ihre Funktion auf die neueste Laufzeitversion zu aktualisieren, wenn Sie die Funktion ändern, wählen Sie Function update (Funktionsaktualisierung).
   - Damit Ihre Funktion nur dann auf die neueste Laufzeitversion aktualisiert wird, wenn Sie den Laufzeitversions-ARN ändern, wählen Sie Manual (Manuell).

   > **Note**
   >
   > Sie finden den Laufzeitversions-ARN unter Runtime management configuration (Laufzeitverwaltungskonfiguration). Sie finden den ARN auch in der `INIT_START`-Zeile Ihrer Funktionsprotokolle.

5. Wählen Sie Speichern.

So konfigurieren Sie, wie Lambda Ihre Laufzeitversion aktualisiert (AWS CLI)

Um die Laufzeitverwaltung für eine Funktion zu konfigurieren, können Sie den `put-runtime-management-config` AWS CLI-Befehl zusammen mit dem Laufzeitaktualisierungsmodus verwenden. Wenn Sie den `Manual`-Modus verwenden, müssen Sie auch den ARN der Laufzeitversion angeben.

```
aws lambda put-runtime-management-config --function-name arn:aws:lambda:eu-west-1:069549076217:function:myfunction --update-runtime-on Manual --runtime-version-arn arn:aws:lambda:eu-west-1::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
  "UpdateRuntimeOn": "Manual",
  "FunctionArn": "arn:aws:lambda:eu-west-1:069549076217:function:myfunction",
  "RuntimeVersionArn": "arn:aws:lambda:eu-
west-1::runtime:8eeff65f6809a3ce81507fe733fe09b835899b99481ba22fd75b5a7338290ec1"
}
```

Modell der geteilten Verantwortung

Lambda ist für das Kuratieren und Veröffentlichen von Sicherheitsupdates für alle unterstützten verwalteten Laufzeiten und Container-Images verantwortlich. Die Verantwortung für die Aktualisierung vorhandener Funktionen zur Verwendung der neuesten Laufzeitversion hängt davon ab, welchen Laufzeitaktualisierungsmodus Sie verwenden.

Lambda ist dafür verantwortlich, Laufzeitaktualisierungen auf alle Funktionen anzuwenden, die für den Laufzeitaktualisierungsmodus Auto (Automatisch) konfiguriert sind.

Für Funktionen, die mit dem Laufzeitaktualisierungsmodus Function update (Funktionsaktualisierung) konfiguriert sind, sind Sie für die regelmäßige Aktualisierung Ihrer Funktion verantwortlich. Lambda ist dafür verantwortlich, Laufzeitaktualisierungen anzuwenden, wenn Sie diese Aktualisierungen vornehmen. Wenn Sie Ihre Funktion nicht aktualisieren, aktualisiert Lambda die Laufzeit nicht. Wenn Sie Ihre Funktion nicht regelmäßig aktualisieren, empfehlen wir dringend, diese für automatische Laufzeitaktualisierungen zu konfigurieren, damit sie weiterhin Sicherheitsupdates erhält.

Bei Funktionen, die für den Laufzeitaktualisierungsmodus Manual (Manuell) konfiguriert sind, sind Sie dafür verantwortlich, Ihre Funktion zu aktualisieren, damit sie die neueste Laufzeitversion verwendet. Wir empfehlen dringend, diesen Modus nur zu verwenden, um im seltenen Ereignis einer Inkompatibilität der Laufzeitaktualisierung die Laufzeitversion vorübergehend zurückzusetzen. Wir empfehlen Ihnen außerdem, so schnell wie möglich in den Modus Auto (Automatisch) zu wechseln, um die Zeit zu minimieren, in der Ihre Funktionen nicht gepatcht werden.

Wenn Sie Container-Images zum Bereitstellen Ihrer Funktionen verwenden, ist Lambda für das Veröffentlichen aktualisierter Basis-Images verantwortlich. In diesem Fall sind Sie dafür verantwortlich, das Container-Image Ihrer Funktion aus dem neuesten Basis-Image neu zu erstellen und das Container-Image erneut bereitzustellen.

Dies ist in der folgenden Tabelle zusammengefasst:

Bereitstellungsmodus	Verantwortung von Lambda	Verantwortung des Kunden
Verwaltete Laufzeit, Modus Auto (Automatisch)	Veröffentlichen Sie neue Laufzeitversionen mit den neuesten Patches. Wenden Sie Laufzeit-Patches auf vorhandene Funktionen an.	Führen Sie im seltenen Fall eines Kompatibilitätsproblems bei Laufzeitaktualisierungen ein Rollback auf eine frühere Laufzeitversion durch.
Verwaltete Laufzeit, Modus Function update (Funktionsaktualisierung)	Veröffentlichen Sie neue Laufzeitversionen mit den neuesten Patches.	Aktualisieren Sie die Funktionen regelmäßig, um die neueste Laufzeitversion zu erhalten. Schalten Sie eine Funktion in den Modus Auto (Automatisch), wenn Sie die Funktion nicht regelmäßig aktualisieren. Führen Sie im seltenen Fall eines Kompatibilitätsproblems bei Laufzeitaktualisierungen ein Rollback auf eine frühere Laufzeitversion durch.
Verwaltete Laufzeit, Modus Manual (Manuell)	Veröffentlichen Sie neue Laufzeitversionen mit den neuesten Patches.	Verwenden Sie diesen Modus nur für ein vorübergehendes Laufzeit-Rollback im seltenen Fall eines Kompatibilitätsproblems bei der Aktualisierung. Schalten Sie die Funktionen so schnell wie möglich in den Modus Auto (Automatisch) oder Function update (Funktionsaktualisierung) und auf die neueste Laufzeitversion.
Container-Image	Veröffentlichen Sie neue Container-Images mit den neuesten Patches.	Stellen Sie die Funktionen regelmäßig neu bereit, indem Sie das neueste Container-Basis-Image verwenden, um die neuesten Patches abzurufen.

Weitere Informationen zur geteilten Verantwortung mit AWS finden Sie unter Modell der geteilten Verantwortung auf der AWS Cloud-Sicherheitsseite.

Anwendungen mit hoher Compliance

Um Patching-Anforderungen zu erfüllen, verlassen sich Lambda-Kunden in der Regel auf automatische Laufzeitaktualisierungen. Wenn Ihre Anwendung strengen Anforderungen an die Aktualität von Patches unterliegt, sollten Sie die Verwendung früherer Laufzeitversionen einschränken. Sie können die Laufzeitverwaltungskontrollen von Lambda einschränken, indem Sie AWS Identity and Access Management (IAM) verwenden, um Benutzern in Ihrem AWS Konto den Zugriff auf den PutRuntimeManagementConfig API-Vorgang zu verweigern. Dieser Vorgang wird verwendet, um den Laufzeitaktualisierungsmodus für eine Funktion auszuwählen. Wenn Sie den Zugriff auf diesen Vorgang verweigern, werden alle Funktionen standardmäßig auf den Modus Auto (Automatisch) umgestellt. Sie können diese Einschränkung unternehmensweit anwenden, indem Sie Service-Kontrollrichtlinien (SCP) verwenden. Für den Fall, dass Sie eine Funktion auf eine frühere Laufzeitversion zurücksetzen müssen, können Sie eine Richtlinienausnahme auf der case-by-case Grundlage von gewähren.

Ändern der Laufzeitumgebung

Sie können interne Erweiterungen verwenden, um den Laufzeitprozess zu ändern. Interne Erweiterungen sind keine separaten Prozesse – sie werden als Teil des Laufzeitprozesses ausgeführt.

Lambda bietet sprachspezifische Umgebungsvariablen, die Sie festlegen können, um Optionen und Werkzeuge zur Laufzeit hinzuzufügen. Lambda bietet auch Wrapper-Skripts, die Lambda erlauben, den Laufzeit-Startup an Ihr Skript zu delegieren. Sie können ein Wrapper-Skript erstellen, um das Laufzeit-Startup-Verhalten anzupassen.

Sprachspezifische Umgebungsvariablen

Lambda unterstützt Konfigurationsmöglichkeiten, mit denen Code während der Funktionsinitialisierung über die folgenden sprachspezifischen Umgebungsvariablen vorgeladen werden kann:

- `JAVA_TOOL_OPTIONS` – Unter Java unterstützt Lambda diese Umgebungsvariable, um zusätzliche Befehlszeilenvariablen in Lambda zu setzen. Mit dieser Umgebungsvariablen können Sie die Initialisierung von Werkzeugen angeben, insbesondere das Starten von nativen oder Java-Agenten mit den Optionen `agentlib` oder `javaagent`. Weitere Informationen finden Sie unter `JAVA_TOOL_OPTIONS`-Umgebungsvariablen.
- `NODE_OPTIONS` – Verfügbar in Node.js-Laufzeiten.
- `DOTNET_STARTUP_HOOKS` – Auf .NET Core 3.1 und höher gibt diese Umgebungsvariable einen Pfad zu einer Assembly (DLL) an, die Lambda verwenden kann.

Die Verwendung sprachspezifischer Umgebungsvariablen ist die bevorzugte Methode zum Festlegen von Startup-Eigenschaften.

Wrapper-Skripte

Sie können ein Wrapper-Skript erstellen, um das Laufzeit-Startup-Verhalten Ihrer Lambda-Funktion anzupassen. Mit einem Wrapper-Skript können Sie Konfigurationsparameter festlegen, die nicht über sprachspezifische Umgebungsvariablen festgelegt werden können.

> **Note**
>
> Aufrufe können fehlschlagen, wenn das Wrapper-Skript den Laufzeitprozess nicht erfolgreich startet.

Wrapper-Skripts werden auf allen nativen Lambda-Laufzeiten unterstützt. Wrapper-Skripts werden auf Reine OS-Laufzeiten (der `provided`-Laufzeitfamilie) nicht unterstützt.

Wenn Sie ein Wrapper-Skript für Ihre Funktion verwenden, startet Lambda die Laufzeit mit Ihrem Skript. Lambda sendet den Pfad an Ihr Skript zum Interpreter und alle ursprünglichen Argumente für den Startup der Standardlaufzeit. Ihr Skript kann das Startup-Verhalten des Programms erweitern oder transformieren. Beispielsweise kann das Skript Argumente injizieren und ändern, Umgebungsvariablen festlegen oder Metriken, Fehler und andere Diagnoseinformationen erfassen.

Sie geben das Skript an, indem Sie den Wert der `AWS_LAMBDA_EXEC_WRAPPER`-Umgebungsvariablen als Dateisystempfad einer ausführbaren Binärdatei oder eines Skripts festlegen.

Beispiel: Erstellen und Verwenden eines Wrapper-Skripts mit Python 3.8

Im folgenden Beispiel erstellen Sie ein Wrapper-Skript, um den Python-Interpreter mit der `-X importtime`-Option zu starten. Wenn Sie die Funktion ausführen, generiert Lambda einen Protokolleintrag, der die Dauer der Importzeit für jeden Import anzeigt.

So erstellen und verwenden Sie ein Wrapper-Skript mit Python 3.8:

1. Um das Wrapper-Skript zu erstellen, fügen Sie den folgenden Code in eine Datei mit dem Namen ei `importtime_wrapper`:

```
#!/bin/bash

# the path to the interpreter and all of the originally intended arguments
args=("$@")

# the extra options to pass to the interpreter
extra_args=("-X" "importtime")

# insert the extra options
args=("${args[@]:0:$#-1}" "${extra_args[@]}" "${args[@]: -1}")
```

```
# start the runtime with the extra options
exec "${args[@]}"
```

2. Um dem Skript ausführbare Berechtigungen zu erteilen, geben Sie `chmod +x importtime_wrapper` in der Befehlszeile ein.
3. Stellen Sie das Skript als Lambda-Ebene bereit.
4. Erstellen Sie eine Funktion mit der Lambda-Konsole.
   a. Öffnen Sie die Lambda-Konsole.
   b. Wählen Sie Funktion erstellen.
   c. Geben Sie unter Basic Information (Grundlegende Informationen) für Function name (Funktionsname) **`wrapper-test-function`** ein.
   d. Wählen Sie für Runtime (Laufzeit) die Option Python 3.8 aus.
   e. Wählen Sie Funktion erstellen.
5. Fügen Sie die Ebene zu Ihrer Funktion hinzu.
   a. Wählen Sie Ihre Funktion und dann Code aus, wenn er noch nicht ausgewählt ist.
   b. Wählen Sie Add a layer (Layer hinzufügen) aus.
   c. Wählen Sie unter Choose a layer (Ebene auswählen) Name und Version der kompatiblen Ebene, die Sie vorher erstellt haben.
   d. Wählen Sie Add aus.
6. Fügen Sie der Funktion den Code und die Umgebungsvariable hinzu.
   a. Fügen Sie im Funktionscode-Editor den folgenden Funktionscode ein:

```
import json

  def lambda_handler(event, context):
      # TODO implement
      return {
          'statusCode': 200,
          'body': json.dumps('Hello from Lambda!')
      }
```

   b. Wählen Sie Save aus.

c. Wählen Sie unter Environment variables (Umgebungsvariablen) die Option Edit (Bearbeiten).

d. Wählen Sie Umgebungsvariablen hinzufügen aus.

e. Geben Sie für Key (Schlüssel) `AWS_LAMBDA_EXEC_WRAPPER` ein.

f. Geben Sie für Wert `/opt/importtime_wrapper` ein.

g. Wählen Sie Save aus.

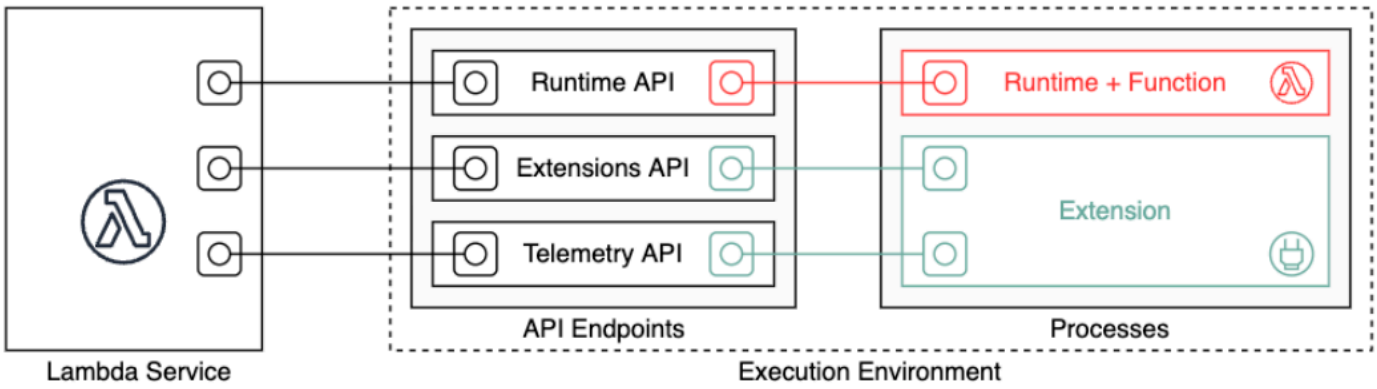
7. Um die Funktion auszuführen, wählen Sie Test.

   Da Ihr Wrapper-Skript den Python-Interpreter mit der `-X importtime`-Option gestartet hat, zeigen die Protokolle die für jeden Import erforderliche Zeit an. Zum Beispiel:

```
...
2020-06-30T18:48:46.780+01:00 import time: 213 | 213 | simplejson
2020-06-30T18:48:46.780+01:00 import time: 50 | 263 | simplejson.raw_json
...
```

Lambda-Laufzeiten-API

AWS Lambda stellt eine HTTP-API für benutzerdefinierte Laufzeiten bereit, um Aufrufereignisse aus Lambda zu erhalten und Antwortdaten innerhalb der Lambda-Ausführungsumgebung zurückzusenden.



Die OpenAPI-Spezifikation für die Laufzeit-API-Version 2018-06-01 ist unter runtime-api.zip verfügbar.

Um eine API-Anforderungs-URL zu erstellen, rufen Laufzeitumgebungen den API-Endpunkt aus der `AWS_LAMBDA_RUNTIME_API`-Umgebungsvariablen ab, fügen die API-Version und dann den gewünschten Ressourcenpfad hinzu.

Example Anforderung

```
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next"
```

API-Methoden

- Nächster Aufruf
- Aufrufantwort
- Initialisierungsfehler
- Aufruffehler

Nächster Aufruf

Pfad – `/runtime/invocation/next`

Methode – GET

Die Laufzeit sendet diese Meldung an Lambda, um ein Aufrufereignis anzufordern. Der Antworttext enthält die Nutzlast aus dem Aufruf. Dabei handelt es sich um ein JSON-Dokument, das Ereignisdaten aus dem Funktionsauslöser enthält. Die Antwort-Header enthalten zusätzliche Daten zum Aufruf.

Antwort-Header

- `Lambda-Runtime-Aws-Request-Id` – Die Anforderungs-ID, mit der die Anforderung identifiziert wird, die den Aufruf der Funktion ausgelöst hat.

  Beispiel, `8476a536-e9f4-11e8-9739-2dfe598c3fcd`.
- `Lambda-Runtime-Deadline-Ms` – Das Datum, an dem eine Zeitüberschreitung für die Funktion eintritt (in Unix-Millisekunden).

  Beispiel, `1542409706888`.
- `Lambda-Runtime-Invoked-Function-Arn` – Der ARN der/des Lambda-Funktion, -Version oder -Alias, die/der im Aufruf angegeben ist.

  Beispiel, `arn:aws:lambda:us-east-2:123456789012:function:custom-runtime`.
- `Lambda-Runtime-Trace-Id` – Der AWS X-Ray-Nachverfolgungs-Header.

  Beispiel, `Root=1-5bef4de7-ad49b0e87f6ef6c87fc2e700;Parent=9a9197af755a6419;Sampled=1`.
- `Lambda-Runtime-Client-Context` – Für Aufrufe aus dem AWS Mobile SDK, Daten zur Clientanwendung und Daten zum Gerät.
- `Lambda-Runtime-Cognito-Identity` – Für Aufrufe aus dem AWS Mobile SDK, Daten zum Amazon-Cognito-Identitätsanbieter.

Legen Sie kein Timeout für die `GET`-Anfrage fest, da sich die Antwort verzögern könnte. Zwischen dem Bootstrap der Laufzeit durch Lambda und der Rückgabe eines Ereignisses durch die Laufzeit ist der Laufzeitprozess möglicherweise für mehrere Sekunden eingefroren.

Die Anforderungs-ID verfolgt den Aufruf innerhalb von Lambda nach. Sie verwenden sie, um den Aufruf anzugeben, wenn Sie die Antwort senden.

Der Nachverfolgungs-Header enthält die Nachverfolgungs-ID, die ID des übergeordneten Segments und die Erfassungsentscheidung Wenn die Anforderung erfasst wurde, wurde die Anforderung von Lambda oder einem Upstream-Service erfasst. Die Laufzeit sollte die `_X_AMZN_TRACE_ID` auf den

Wert des Headers festlegen. Das X-Ray SDK liest dies, um die IDs abzurufen und festzulegen, ob die Anforderung nachverfolgt werden soll.

Aufrufantwort

Pfad – `/runtime/invocation/AwsRequestId/response`

Methode – POST

Nachdem die Funktion bis zum Abschluss ausgeführt wurde, schickt die Laufzeitumgebung eine Aufrufantwort an Lambda. Im Fall synchroner Aufrufe schickt Lambda die Antwort anschließend an den Client zurück.

Example Erfolg für Anforderung

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response"  -d "SUCCESS"
```

Initialisierungsfehler

Wenn die Funktion einen Fehler zurückgibt oder die Laufzeit während der Initialisierung auf einen Fehler stößt, verwendet die Laufzeit diese Methode, um den Fehler an Lambda zu melden.

Pfad – `/runtime/init/error`

Methode – POST

Header

`Lambda-Runtime-Function-Error-Type` – Der Fehlertyp, auf den die Laufzeit gestoßen ist. Erforderlich: Nein.

Dieser Header besteht aus einem Zeichenfolgen-Wert. Lambda akzeptiert jede Zeichenfolge, aber wir empfehlen ein Format von <category.reason>. Beispielsweise:

- Laufzeit.NoSuchHandler
- Laufzeit.APIKeyNotFound
- Laufzeit.ConfigInvalid

- Laufzeit.UnknownReason

Body-Parameter

`ErrorRequest` – Informationen über den Fehler. Erforderlich: Nein

Dieses Feld ist ein JSON-Objekt mit der folgenden Struktur:

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Beachten Sie, dass Lambda jeden Wert für `errorType` akzeptiert.

Das folgende Beispiel zeigt eine Lambda-Funktionsfehlermeldung, in der die Funktion die im Aufruf bereitgestellten Ereignisdaten nicht analysieren konnte.

Example Funktionsfehler

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Antworttextparameter:

- `StatusResponse` – Zeichenfolge. Statusinformationen, gesendet mit 202 Antwortcodes.
- `ErrorResponse` – Zusätzliche Fehlerinformationen, die mit den Fehlerantwortcodes gesendet werden. ErrorResponse enthält einen Fehlertyp und eine Fehlermeldung.

Antwortcodes

- 202 – Akzeptiert
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Laufzeit sollte umgehend beendet werden.

Example Initialisierungsfehleranforderung

```
ERROR="{\"errorMessage\" : \"Failed to load function.\", \"errorType\" :
 \"InvalidFunctionException\"}"
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/init/error" -d "$ERROR" --
header "Lambda-Runtime-Function-Error-Type: Unhandled"
```

Aufruffehler

Wenn die Funktion einen Fehler zurückgibt oder die Laufzeit auf einen Fehler stößt, verwendet die Laufzeitumgebung diese Methode, um den Fehler an Lambda zu melden.

Pfad – `/runtime/invocation/AwsRequestId/error`

Methode – POST

Header

`Lambda-Runtime-Function-Error-Type` – Der Fehlertyp, auf den die Laufzeit gestoßen ist. Erforderlich: Nein.

Dieser Header besteht aus einem Zeichenfolgen-Wert. Lambda akzeptiert jede Zeichenfolge, aber wir empfehlen ein Format von <category.reason>. Beispielsweise:

- Laufzeit.NoSuchHandler
- Laufzeit.APIKeyNotFound
- Laufzeit.ConfigInvalid
- Laufzeit.UnknownReason

Body-Parameter

`ErrorRequest` – Informationen über den Fehler. Erforderlich: Nein

Dieses Feld ist ein JSON-Objekt mit der folgenden Struktur:

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Beachten Sie, dass Lambda jeden Wert für `errorType` akzeptiert.

Das folgende Beispiel zeigt eine Lambda-Funktionsfehlermeldung, in der die Funktion die im Aufruf bereitgestellten Ereignisdaten nicht analysieren konnte.

Example Funktionsfehler

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Antworttextparameter:

- `StatusResponse` – Zeichenfolge. Statusinformationen, gesendet mit 202 Antwortcodes.
- `ErrorResponse` – Zusätzliche Fehlerinformationen, die mit den Fehlerantwortcodes gesendet werden. ErrorResponse enthält einen Fehlertyp und eine Fehlermeldung.

Antwortcodes

- 202 – Akzeptiert
- 400 – Ungültige Anfrage
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Laufzeit sollte umgehend beendet werden.

Example Fehler für Anforderung

```
REQUEST_ID=156cb537-e2d4-11e8-9b34-d36013741fb9
ERROR="{\"errorMessage\" : \"Error parsing event data.\", \"errorType\" :
 \"InvalidEventDataException\"}"
curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/error"
 -d "$ERROR" --header "Lambda-Runtime-Function-Error-Type: Unhandled"
```

Wann sollten die reinen Betriebssystemlaufzeiten von Lambda verwendet werden

Lambda bietet verwaltete Laufzeiten für Java, Python, Node.js, .NET und Ruby. Um Lambda-Funktionen in einer Programmiersprache zu erstellen, die nicht als verwaltete Laufzeit verfügbar ist, verwenden Sie eine reine OS-Laufzeit (die `provided`-Laufzeitfamilie). Es gibt drei Hauptanwendungsfälle für reine OS-Laufzeiten:

- Native Kompilierung ahead-of-time (AOT): Sprachen wie Go, Rust und C++ werden nativ zu einer ausführbaren Binärdatei kompiliert, für die keine spezielle Sprachlaufzeit erforderlich ist. Diese Sprachen benötigen nur eine Betriebssystemumgebung, in der die kompilierte Binärdatei ausgeführt werden kann. Sie können auch reine Lambda-OS-Laufzeiten verwenden, um Binärdateien bereitzustellen, die mit.NET Native AOT und Java GraalVM Native kompiliert wurden.

  Sie müssen einen Laufzeitschnitten-Client in Ihre Binärdatei aufnehmen. Der Laufzeitenschnittstellen-Client ruft die Lambda-Laufzeiten-API auf, um Funktionsaufrufe abzurufen, und ruft dann den Funktionshandler auf. Lambda stellt Laufzeitschnittstellen-Clients für Go, .NET Native AOT, C++ und Rust (experimentell) bereit.

  Sie müssen Ihre Binärdatei für eine Linux-Umgebung und für dieselbe Befehlssatzarchitektur kompilieren, die Sie für die Funktion verwenden möchten (x86_64 oder arm64).
- Laufzeiten von Drittanbietern: Sie können Lambda-Funktionen mit off-the-shelf Laufzeiten wie Bref für PHP oder Swift Runtime für Swift AWS Lambda ausführen.
- Benutzerdefinierte Laufzeiten: Sie können Ihre eigene Laufzeit für eine Sprache oder Sprachversion erstellen, für die Lambda keine verwaltete Laufzeit bereitstellt, z. B. Node.js 19. Weitere Informationen finden Sie unter Erstellen einer benutzerdefinierten Laufzeit für AWS Lambda. Dies ist der am wenigsten verbreitete Anwendungsfall für reine OS-Laufzeiten.

Lambda unterstützt die folgenden reinen OS-Laufzeiten.

Nur OS

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Reine OS-Laufzeit	`provided.al2023`	Amazon Linux 2023			

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Reine OS-Laufzeit	`provided.al2`	Amazon Linux 2			

Die Laufzeit von Amazon Linux 2023 (`provided.al2023`) bietet mehrere Vorteile gegenüber Amazon Linux 2, darunter einen geringeren Bereitstellungsaufwand und aktualisierte Versionen von Bibliotheken wie `glibc`.

Die `provided.al2023`-Laufzeit verwendet `dnf` als Paketmanager anstelle von `yum`, was der Standard-Paketmanager in Amazon Linux 2 ist. Weitere Informationen zu den Unterschieden zwischen `provided.al2023` und `provided.al2` finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.

Erstellen einer benutzerdefinierten Laufzeit für AWS Lambda

Sie können eine AWS Lambda -Laufzeit in jeder Programmiersprache implementieren. Eine Laufzeit ist ein Programm, das die Handler-Methode einer Lambda-Funktion ausführt, wenn die Funktion aufgerufen wird. Die Laufzeit kann im Bereitstellungspaket Ihrer Funktion enthalten sein oder in einem Layer verteilt werden. Wenn Sie die Lambda-Funktion erstellen, wählen Sie eine reine OS-Laufzeit (die `provided`-Laufzeitfamilie) aus.

> **Note**
>
> Das Erstellen einer benutzerdefinierten Laufzeit ist ein Anwendungsfall für Fortgeschrittene. Informationen zum Kompilieren in einer nativen Binärdatei oder zum Verwenden einer Drittanbieter- off-the-shelf Laufzeit finden Sie unter Wann sollten die reinen Betriebssystemlaufzeiten von Lambda verwendet werden.

Eine exemplarische Vorgehensweise für die Bereitstellung einer benutzerdefinierten Laufzeit finden Sie unter Tutorial: Erstellen einer benutzerdefinierten Laufzeit. Sie können auch eine in C++ implementierte benutzerdefinierte Laufzeit unter awslabs/aws-lambda-cpp auf erkunden GitHub.

Themen

- Voraussetzungen

- Implementieren von Antwort-Streaming in einer benutzerdefinierten Laufzeitumgebung

Voraussetzungen

Benutzerdefinierte Laufzeiten müssen bestimmte Initialisierungs- und Verarbeitungsaufgaben abschließen. Eine Laufzeit führt den Setup-Code der Funktion aus, liest den Namen des Handlers aus einer Umgebungsvariablen und liest Aufrufereignisse von der Lambda-Laufzeit-API. Die Laufzeit übergibt die Ereignisdaten an den Funktions-Handler und sendet die Antwort aus dem Handler zurück an Lambda.

Initialisierungsaufgaben

Die Initialisierungsaufgaben werden einmal pro Instance der Funktion ausgeführt, um die Umgebung auf die Verarbeitung von Aufrufen vorzubereiten.

- Einstellungen abrufen – Liest Umgebungsvariablen, um Details zu Funktion und Umgebung abzurufen.
  - `_HANDLER` – Der Speicherort für den Handler aus der Konfiguration der Funktion. Das Standardformat ist *`file`*`.`*`method`*, wobei `file` der Name der Datei ohne Erweiterung und `method` der Name einer Methode oder Funktion ist, die in der Datei definiert ist.
  - `LAMBDA_TASK_ROOT` – Das Verzeichnis, das den Funktionscode enthält.
  - `AWS_LAMBDA_RUNTIME_API` – Host und Port der Laufzeit-API.

  Unter Definierte Laufzeitumgebungsvariablen finden Sie eine vollständige Liste der verfügbaren Variablen.
- Funktion initialisieren – Lädt die Handler-Datei und führt den globalen oder statischen Code aus, den sie enthält. Funktionen sollten statische Ressourcen wie SDK-Clients und Datenbankverbindungen einmal erstellen und für mehrere Aufrufe wiederverwenden.
- Fehler verarbeiten – Wenn ein Fehler auftritt, werden die Initialisierungsfehler-API aufgerufen die Ausführung sofort beendet.

Die Initialisierung zählt zur fakturierten Ausführungszeit und zum Timeout. Wenn eine Ausführung die Initialisierung einer neuen Instance Ihrer Funktion auslöst, sehen Sie die Initialisierungszeit in den Protokollen und in der AWS X-Ray -Nachverfolgung.

Example log

```
REPORT RequestId: f8ac1208... Init Duration: 48.26 ms   Duration: 237.17 ms   Billed
 Duration: 300 ms   Memory Size: 128 MB   Max Memory Used: 26 MB
```

Verarbeitungsaufgaben

Während der Ausführung verwendet eine Laufzeit die Lambda-Laufzeitschnittstelle, um eingehende Ereignisse zu verwalten und Fehler zu melden. Nach Abschluss der Initialisierungsaufgaben verarbeitet die Laufzeit eingehende Ereignisse in einer Schleife. Führen Sie in Ihrem Laufzeitcode die folgenden Schritte in der angegebenen Reihenfolge aus.

- Ereignis abrufen – Ruft die API für den nächsten Aufruf auf, um das nächste Ereignis abzurufen. Der Antworttext enthält die Ereignisdaten. De Antwort-Header enthalten die Anforderungs-ID und andere Informationen.
- Nachverfolgungs-Header propagieren – Ruft den X-Ray-Nachverfolgungs-Header aus dem `Lambda-Runtime-Trace-Id`-Header in der API-Antwort ab. Legen Sie die `_X_AMZN_TRACE_ID`-Umgebungsvariable lokal mit demselben Wert fest. Das X-Ray-SDK verwendet diesen Wert, um Ablaufverfolgungsdaten zwischen Services miteinander zu verbinden.
- Context-Objekt erstellen – Erstellt ein Objekt mit Kontextinformationen aus Umgebungsvariablen und Headern in den API-Antworten.
- Funktions-Handler aufrufen – Übergibt Ereignis und Context-Objekt an den Handler.
- Antwort verarbeiten – Ruft die API für die Aufrufantwort ab, um die Antwort aus dem Handler zu veröffentlichen.
- Fehler verarbeiten – Ruft die API für Aufruffehler auf, wenn ein Fehler auftritt.
- Bereinigen Gibt nicht verwendete Ressourcen frei, sendet Daten an andere Services oder führt zusätzliche Aufgaben aus, bevor das nächste Ereignis abgerufen wird.

Eintrittspunkt

Der Eintrittspunkt einer benutzerdefinierten Laufzeit ist eine ausführbare Datei mit dem Namen `bootstrap`. Bei der Bootstrap-Datei kann es sich um die Laufzeit handeln oder es wird eine andere Datei aufgerufen, die die Laufzeit erstellt. Wenn das Stammverzeichnis Ihres Bereitstellungspakets keine Datei mit dem Namen `bootstrap` enthält, sucht Lambda in den Funktionsschichten nach der Datei. Wenn die `bootstrap`-Datei nicht existiert oder nicht ausgeführt werden kann, gibt die Funktion beim Aufruf einen `Runtime.InvalidEntrypoint`-Fehler zurück.

Im Folgenden finden Sie eine `bootstrap` Beispieldatei, die eine gebündelte Version von Node.js verwendet, um eine JavaScript Laufzeit in einer separaten Datei namens auszuführen`runtime.js`.

Example bootstrap

```
#!/bin/sh
    cd $LAMBDA_TASK_ROOT
    ./node-v11.1.0-linux-x64/bin/node runtime.js
```

Implementieren von Antwort-Streaming in einer benutzerdefinierten Laufzeitumgebung

Für Antwort-Streaming-Funktionen haben die Endpunkte `response` und `error` ein leicht geändertes Verhalten, das es der Laufzeit ermöglicht, Teilantworten an den Client zu streamen und Nutzlasten in Paketen zurückzugeben. Weitere Informationen zu dem spezifischen Verhalten finden Sie unter:

- `/runtime/invocation/AwsRequestId/response` – Gibt den `Content-Type`-Header von der Laufzeit zum Senden an den Client weiter. Lambda gibt die Nutzlasten der Antwort in Blöcken über HTTP/1.1-Blocktransfer-Codierungsschema zurück. Der Antwort-Stream darf maximal 20 MiB groß sein. Um die Antwort an Lambda zu streamen, muss die Laufzeit:
  - Den `Lambda-Runtime-Function-Response-Mode`-HTTP-Header auf `streaming` festlegen.
  - Legen Sie den `Transfer-Encoding`-Header auf `chunked` fest.
  - Die Antwort in Übereinstimmung mit der HTTP/1.1-Blocktransfer-Codierungsspezifikation schreiben.
  - Schließt die zugrunde liegende Verbindung, nachdem sie die Antwort erfolgreich geschrieben hat.
- `/runtime/invocation/AwsRequestId/error` – Die Laufzeit kann diesen Endpunkt verwenden, um Funktions- oder Laufzeitfehler an Lambda zu melden, das auch den `Transfer-Encoding`-Header akzeptiert. Dieser Endpunkt kann nur aufgerufen werden, bevor die Laufzeit mit dem Senden einer Aufrufantwort beginnt.
- Melden von Fehlern in der Mitte des Prozesses mit Hilfe von Fehler-Trailern in `/runtime/invocation/AwsRequestId/response` – Um Fehler zu melden, die auftreten, nachdem die Laufzeit mit dem Schreiben der Antwort auf den Aufruf begonnen hat, kann die Laufzeit optional HTTP-Trailing-Header namens `Lambda-Runtime-Function-Error-Type` und `Lambda-Runtime-Function-Error-Body` anfügen. Lambda behandelt dies als erfolgreiche Antwort und leitet die Fehler-Metadaten, die die Laufzeit bereitstellt, an den Client weiter.

> **Note**
>
> Um nachgestellte `Trailer`-Header anzufügen, muss die Laufzeit den Header-Wert am Anfang der HTTP-Anfrage festlegen. Dies ist eine Voraussetzung der HTTP/1.1-Blocktransfer-Codierungs-Spezifikation.

- `Lambda-Runtime-Function-Error-Type` – Der Fehlertyp, auf den die Laufzeit gestoßen ist. Dieser Header besteht aus einem Zeichenfolgen-Wert. Lambda akzeptiert jede Zeichenfolge, aber wir empfehlen ein Format von *`<category.reason>`*. Beispiel: `Runtime.APIKeyNotFound`
- `Lambda-Runtime-Function-Error-Body` – Base64-kodierte Informationen über den Fehler.

Tutorial: Erstellen einer benutzerdefinierten Laufzeit

In diesem Tutorial erstellen Sie eine Lambda-Funktion mit einer benutzerdefinierten Laufzeit. Sie beginnen, indem Sie die Laufzeit in das Bereitstellungspaket der Funktion einfügen. Anschließend migrieren Sie sie zu einer Ebene, die Sie unabhängig von der Funktion verwalten. Schließlich geben Sie die Laufzeitebene frei, indem Sie ihre ressourcenbasierte Berechtigungsrichtlinie aktualisieren.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Sie benötigen eine IAM-Rolle, um eine Lambda Funktion zu erstellen. Die Rolle benötigt die Berechtigung zum Senden von Protokollen an CloudWatch Logs und zum Zugriff auf die AWS Services, die Ihre Funktion verwendet. Wenn Sie nicht über eine Rolle für die Funktionserstellung verfügen, erstellen Sie jetzt eine.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.
   - Trusted entity (Vertrauenswürdige Entität) – Lambda.
   - Berechtigungen – AWSLambdaBasicExecutionRole.
   - Role name (Name der Rolle – **`lambda-role`**.

   Die AWSLambdaBasicExecutionRole Richtlinie verfügt über die Berechtigungen, die die Funktion zum Schreiben von Protokollen in CloudWatch -Protokolle benötigt.

Erstellen einer -Funktion

Erstellen Sie eine Lambda-Funktion mit einer benutzerdefinierten Laufzeit. Dieses Beispiel enthält zwei Dateien: eine `bootstrap`-Laufzeitdatei und einen Funktions-Handler. Beide sind in Bash implementiert.

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

   ```
   mkdir runtime-tutorial
   cd runtime-tutorial
   ```

2. Erstellen Sie eine neue Datei mit dem Namen `bootstrap`. Dies ist die benutzerdefinierte Laufzeit.

   Example bootstrap

   ```
   #!/bin/sh

   set -euo pipefail

   # Initialization - load function handler
   source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"

   # Processing
   while true
   do
     HEADERS="$(mktemp)"
     # Get an event. The HTTP request will block until one is received
     EVENT_DATA=$(curl -sS -LD "$HEADERS" "http://
   ${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

     # Extract request ID by scraping response headers received above
     REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
    '[:space:]' | cut -d: -f2)

     # Run the handler function from the script
     RESPONSE=$($(echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

     # Send the response
     curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
   response"  -d "$RESPONSE"
   done
   ```

Die Laufzeit lädt ein Funktionsskript aus dem Bereitstellungspaket. Sie verwendet zwei Variablen, um das Skript zu finden. `LAMBDA_TASK_ROOT` gibt an, wohin das Paket extrahiert wurde, und `_HANDLER` enthält den Namen des Skripts.

Nachdem die Laufzeit das Funktionsskript geladen hat, verwendet sie die Laufzeit-API, um ein Aufrufereignis aus Lambda abzurufen, übergibt das Ereignis an den Handler und sendet die Antwort zurück an Lambda. Um die Anforderungs-ID abzurufen, speichert die Laufzeit die Header aus der API-Antwort in einer temporären Datei und liest den `Lambda-Runtime-Aws-Request-Id`-Header aus der Datei.

> **Note**
>
> Laufzeit besitzen zusätzliche Verantwortlichkeiten, darunter Fehlerbehandlung und Bereitstellung von Kontextinformationen für den Handler. Details hierzu finden Sie unter Voraussetzungen.

3. Erstellen Sie ein Skript für die Funktion. Das folgende Beispielskript definiert eine Handler-Funktion, die Ereignisdaten annimmt, protokolliert sie in `stderr` und gibt sie zurück.

   Example function.sh

   ```
   function handler () {
     EVENT_DATA=$1
     echo "$EVENT_DATA" 1>&2;
     RESPONSE="Echoing request: '$EVENT_DATA'"

     echo $RESPONSE
   }
   ```

   Das `runtime-tutorial`-Verzeichnis sollte jetzt wie folgt aussehen:

   ```
   runtime-tutorial
   # bootstrap
   # function.sh
   ```

4. Konvertieren Sie die Dateien zu ausführbaren Dateien und fügen Sie sie einem ZIP-Dateiarchiv hinzu. Dies ist das Bereitstellungspaket.

   ```
   chmod 755 function.sh bootstrap
   ```

```
zip function.zip function.sh bootstrap
```

5. Erstellen Sie eine Funktion mit dem Namen `bash-runtime`. Geben Sie für `--role` den ARN Ihrer Lambda-Ausführungsrolle ein.

```
aws lambda create-function --function-name bash-runtime \
--zip-file fileb://function.zip --handler function.handler --runtime
 provided.al2023 \
--role arn:aws:iam::123456789012:role/lambda-role
```

6. Die Funktion aufrufen.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'
 response.txt --cli-binary-format raw-in-base64-out
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

7. Überprüfen Sie die Antwort.

```
cat response.txt
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
Echoing request: '{"text":"Hello"}'
```

Erstellen einer Ebene

Um Laufzeitcode und Funktionscode voneinander zu trennen, erstellen Sie eine Ebene, die nur die Laufzeit enthält. Mit Ebenen können Sie die Abhängigkeiten Ihrer Funktion unabhängig entwickeln. Sie können darüber hinaus die Speichernutzung reduzieren, wenn Sie dieselbe Ebene für mehrere Funktionen verwenden. Weitere Informationen finden Sie unter Verwaltung von Lambda-Abhängigkeiten mit Ebenen.

1. Erstellen Sie eine ZIP-Datei, die die `bootstrap`-Datei enthält.

   ```
   zip runtime.zip bootstrap
   ```

2. Erstellen Sie mit dem Befehl publish-layer-version eine Ebene.

   ```
   aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://
   runtime.zip
   ```

   Hierdurch wird die erste Version der Ebene erstellt.

Aktualisieren der Funktion

Um die Laufzeitebene in der Funktion zu verwenden, konfigurieren Sie die Funktion für die Verwendung der Ebene und entfernen den Laufzeitcode aus der Funktion.

1. Aktualisieren Sie die Konfiguration der Funktion, um die Ebene einzubeziehen.

   ```
   aws lambda update-function-configuration --function-name bash-runtime \
   --layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:1
   ```

   Dadurch wird die Laufzeit zur Funktion im `/opt`-Verzeichnis hinzugefügt. Um sicherzustellen, dass Lambda die Laufzeit in der Ebene verwendet, müssen Sie die `boostrap`-Datei aus dem Bereitstellungspaket der Funktion entfernen, wie in den nächsten beiden Schritten gezeigt.

2. Erstellen Sie eine ZIP-Datei, die den Funktionscode enthält.

   ```
   zip function-only.zip function.sh
   ```

3. Aktualisieren Sie den Funktionscode so, dass er nur das Handler-Skript enthält.

```
aws lambda update-function-code --function-name bash-runtime --zip-file fileb://
function-only.zip
```

4. Rufen Sie die Funktion auf, um zu überprüfen, ob sie mit der Laufzeitebene funktioniert.

```
aws lambda invoke --function-name bash-runtime --payload '{"text":"Hello"}'
 response.txt --cli-binary-format raw-in-base64-out
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

5. Überprüfen Sie die Antwort.

```
cat response.txt
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
Echoing request: '{"text":"Hello"}'
```

Aktualisieren der Laufzeit

1. Um Informationen zur Ausführungsumgebung zu protokollieren, aktualisieren Sie das Laufzeitskript, sodass es Umgebungsvariablen ausgibt.

Example bootstrap

```
#!/bin/sh
```

```
set -euo pipefail

# Configure runtime to output environment variables
echo "##  Environment variables:"
env

# Load function handler
source $LAMBDA_TASK_ROOT/"$(echo $_HANDLER | cut -d. -f1).sh"

# Processing
while true
do
  HEADERS="$(mktemp)"
  # Get an event. The HTTP request will block until one is received
  EVENT_DATA=$(curl -sS -LD "$HEADERS" "http://
${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/next")

  # Extract request ID by scraping response headers received above
  REQUEST_ID=$(grep -Fi Lambda-Runtime-Aws-Request-Id "$HEADERS" | tr -d
 '[:space:]' | cut -d: -f2)

  # Run the handler function from the script
  RESPONSE=$($(echo "$_HANDLER" | cut -d. -f2) "$EVENT_DATA")

  # Send the response
  curl "http://${AWS_LAMBDA_RUNTIME_API}/2018-06-01/runtime/invocation/$REQUEST_ID/
response"  -d "$RESPONSE"
done
```

2. Erstellen Sie eine ZIP-Datei mit der neuen Version der `bootstrap`-Datei.

```
zip runtime.zip bootstrap
```

3. Erstellt eine neue Version der `bash-runtime`-Ebene.

```
aws lambda publish-layer-version --layer-name bash-runtime --zip-file fileb://
runtime.zip
```

4. Konfigurieren Sie die Funktion für die Verwendung der neuen Version der Ebene.

```
aws lambda update-function-configuration --function-name bash-runtime \
--layers arn:aws:lambda:us-east-1:123456789012:layer:bash-runtime:2
```

Freigeben der Ebene

Um einem anderen Konto Nutzungsberechtigungen für Ebenen zu erteilen, fügen Sie der Berechtigungsrichtlinie der Ebenenversion mithilfe des Befehls add-layer-version-permission eine Anweisung hinzu. In jeder Anweisung können Sie einem einzelnen Konto, allen Konten oder einer Organisation eine Berechtigung erteilen.

Im folgenden Beispiel wird dem Konto 111122223333 Zugriff auf Version 2 der `bash-runtime`-Ebene gewährt.

```
aws lambda add-layer-version-permission --layer-name bash-runtime --statement-id
 xaccount \
--action lambda:GetLayerVersion --principal 111122223333 --version-number 2 --output
 text
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
e210ffdc-e901-43b0-824b-5fcd0dd26d16    {"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:GetLayerVersion","Resource":"arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```

Berechtigungen gelten nur für eine Version mit einer Ebene. Wiederholen Sie den Vorgang bei jeder Erstellung einer neuen Ebenenversion.

Bereinigen

Löschen Sie alle Versionen der Ebene.

```
aws lambda delete-layer-version --layer-name bash-runtime --version-number 1
aws lambda delete-layer-version --layer-name bash-runtime --version-number 2
```

Da die Funktion einen Verweis auf Version 2 der Ebene enthält, ist diese nach wie vor in Lambda vorhanden. Die Funktion funktioniert weiter. Es können jedoch keine weiteren Funktionen für die Verwendung der gelöschten Version konfiguriert werden. Wenn Sie die Liste der Ebenen in der Funktion ändern, müssen Sie eine neue Version angeben oder die gelöschte Ebene auslassen.

Löschen Sie die Funktion mit dem Befehl delete-function.

```
aws lambda delete-function --function-name bash-runtime
```

Verwenden der AVX2-Vektorisierung in Lambda

Advanced Vector Extensions 2 (AVX2) ist eine Vektorisierungserweiterung für den Intel x86-Befehlssatz, die SIMD (Single Instruction Multiple Data)-Anweisungen über Vektoren von 256 Bit ausführen kann. Bei vektorisierbaren Algorithmen mit hochgradig parallelisierbarem Betrieb kann die Verwendung von AVX2 die CPU-Leistung verbessern, was zu niedrigeren Latenzen und höherem Durchsatz führt. Verwenden Sie den AVX2-Befehlssatz für rechenintensive Workloads wie Inferencing für Machine-Learning, Multimedia-Verarbeitung, wissenschaftliche Simulationen und Finanzmodellierungsanwendungen.

> **Note**
>
> Lambda arm64 verwendet NEON SIMD-Architektur und unterstützt die x86 AVX2-Erweiterungen nicht.

Um AVX2 mit Ihrer Lambda-Funktion zu verwenden, stellen Sie sicher, dass Ihr Funktionscode auf AVX2-optimierten Code zugreift. Für einige Sprachen können Sie die von AVX2 unterstützte Version von Bibliotheken und Paketen installieren. Für andere Sprachen können Sie Ihren Code und Ihre Abhängigkeiten mit den entsprechenden Compiler-Flags neu kompilieren (wenn der Compiler die automatische Vektorisierung unterstützt). Sie können Ihren Code auch mit Bibliotheken von Drittanbietern kompilieren, die AVX2 zur Optimierung von mathematischen Vorgängen verwenden. Zum Beispiel Intel Math Kernel Library (Intel MKL), OpenBLAS (Basic Linear Algebra Subprogramme) und AMD BLAS-ähnliche Library Instantiation Software (BLIS). Automatisch vektorisierte Sprachen wie Java verwenden AVX2 automatisch für Berechnungen.

Sie können neue Lambda-Workloads erstellen oder vorhandene AVX2-fähige Workloads ohne zusätzliche Kosten in Lambda verschieben.

Weitere Informationen zu AVX2 finden Sie unter Advanced Vector Extensions 2 in Wikipedia.

Kompilieren aus der Quelle

Wenn Ihre Lambda-Funktion eine C- oder C++-Bibliothek verwendet, um rechenintensive vektorisierbare Operationen durchzuführen, können Sie die entsprechenden Compiler-Flags festlegen und den Funktionscode neu kompilieren. Dann vektorisiert der Compiler Ihren Code automatisch.

Fügen Sie für den `gcc`- oder `clang`-Compiler dem Befehl `-march=haswell` hinzu oder legen Sie `-mavx2` als Befehlsoption fest.

```
~ gcc -march=haswell main.c
or
~ gcc -mavx2 main.c

~ clang -march=haswell main.c
or
~ clang -mavx2 main.c
```

Um eine bestimmte Bibliothek zu verwenden, befolgen Sie die Anweisungen in der Dokumentation der Bibliothek, um die Bibliothek zu kompilieren und zu erstellen. Um beispielsweise TensorFlow aus der Quelle zu erstellen, können Sie den Installationsanweisungen auf der TensorFlow Website folgen. Stellen Sie sicher, dass Sie die `-march=haswell`-Kompilieroption verwenden.

Aktivieren von AVX2 für Intel MKL

Intel MKL ist eine Bibliothek optimierter mathematischer Vorgänge, die implizit AVX2-Anweisungen verwenden, wenn die Rechenplattform sie unterstützt. Frameworks wie das standardmäßige PyTorch Erstellen mit Intel MKL, sodass Sie AVX2 nicht aktivieren müssen.

Einige Bibliotheken, wie z. B. TensorFlow, bieten Optionen in ihrem Build-Prozess, um die Intel MKL-Optimierung anzugeben. Verwenden Sie beispielsweise bei TensorFlowdie `--config=mkl` Option .

Mit NumPyIntel MKL können Sie auch beliebte wissenschaftliche Python-Bibliotheken wie SciPy und erstellen. Anweisungen zum Aufbau dieser Bibliotheken mit Intel MKL finden Sie unter Numpy/Scipy mit Intel MKL und Intel Compilers auf der Intel-Website.

Weitere Informationen zu Intel MKL und ähnlichen Bibliotheken finden Sie unter Mathematische Kernel-Bibliothek in Wikipedia, auf der OpenBLAS-Website und im AMD BLAN-Repository auf GitHub.

AVX2-Unterstützung in anderen Sprachen

Wenn Sie keine C- oder C++-Bibliotheken verwenden und nicht mit Intel MKL erstellen, können Sie dennoch eine gewisse Verbesserung der AVX2-Leistung für Ihre Anwendungen erzielen. Beachten

Sie, dass die tatsächliche Verbesserung von der Fähigkeit des Compilers oder Interpreters abhängt, die AVX2-Funktionen für Ihren Code zu nutzen.

Python

Python-Benutzer verwenden im Allgemeinen - SciPy und - NumPy Bibliotheken für rechenintensive Workloads. Sie können diese Bibliotheken kompilieren, um AVX2 zu aktivieren, oder Sie können die Intel MKL-fähigen Versionen der Bibliotheken verwenden.

Knoten

Verwenden Sie für rechenintensive Workloads AVX2-fähige oder Intel MKL-fähige Versionen der von Ihnen benötigten Bibliotheken.

Java

Der JIT-Compiler von Java kann Ihren Code automatisch vektorisieren, um mit AVX2-Anweisungen ausgeführt zu werden. Informationen zum Erkennen von vektorisiertem Code finden Sie in der Code-Vektorisierung in der JVM-Präsentation auf der OpenJDK-Website.

Go

Der Standard-Go-Compiler unterstützt derzeit keine automatische Vektorisierung, aber Sie können gccgo, den GCC-Compiler für Go, verwenden. Legen Sie die `-mavx2`-Option fest:

```
gcc -o avx2 -mavx2 -Wall main.c
```

Intrinsische Funktionen

Es ist möglich, intrinsische Funktionen in vielen Sprachen zu verwenden, um Ihren Code für die Verwendung von AVX2 manuell zu vektorisieren. Wir empfehlen diesen Ansatz jedoch nicht. Das manuelle Schreiben von vektorisiertem Code erfordert erhebliche Anstrengungen. Außerdem ist das Debuggen und Verwalten eines solchen Codes schwieriger als die Verwendung von Code, der von der automatischen Vektorisierung abhängt.

AWS Lambda Funktionen konfigurieren

Erfahren Sie, wie Sie die wichtigsten Funktionen und Optionen für Ihre Lambda-Funktion mithilfe der Lambda-API oder der Konsole konfigurieren.

Arbeitsspeicher

Erfahren Sie, wie und wann Sie den Funktionsspeicher vergrößern können.

Kurzlebiger Speicher

Erfahren Sie, wie und wann Sie die temporäre Speicherkapazität Ihrer Funktion erhöhen können.

Timeout (Zeitüberschreitung)

Erfahren Sie, wie und wann Sie den Timeout-Wert Ihrer Funktion erhöhen können.

Umgebungsvariablen

Sie können Ihren Funktionscode portabel machen und Geheimnisse aus Ihrem Code heraushalten, indem Sie sie mithilfe von Umgebungsvariablen in der Konfiguration Ihrer Funktion speichern.

Ausgehende Netzwerke

Sie können Ihre Lambda-Funktion mit AWS Ressourcen in einer Amazon VPC verwenden. Wenn Sie Ihre Funktion mit einer VPC verbinden, können Sie auf Ressourcen in einem privaten Subnetz wie relationale Datenbanken und Caches zugreifen.

Eingehende Netzwerke

Sie können einen Schnittstellen-VPC-Endpunkt verwenden, um Ihre Lambda-Funktionen aufzurufen, ohne das öffentliche Internet zu nutzen.

Dateisystem

Sie können Ihre Lambda-Funktion verwenden, um ein Amazon EFS in ein lokales Verzeichnis einzubinden. Ein Dateisystem ermöglicht es Ihrem Funktionscode, sicher und mit hoher Gleichzeitigkeit auf gemeinsam genutzte Ressourcen zuzugreifen und diese zu ändern.

Aliasnamen

Sie können Ihre Clients so konfigurieren, dass sie eine bestimmte Lambda-Funktionsversion aufrufen, indem Sie einen Alias verwenden, anstatt den Client zu aktualisieren.

Versionen

Durch die Veröffentlichung einer Version Ihrer Funktion können Sie Ihren Code und Ihre Konfiguration als separate Ressource speichern, die nicht geändert werden kann.

Antwort-Streaming

Sie können Ihre Lambda-Funktions-URLs so konfigurieren, dass sie Antwort-Nutzlasten zurück an Clients streamen. Antwort-Streaming kann für latenzempfindliche Anwendungen von Vorteil sein, da es die Leistung in der Zeit bis zum ersten Byte (TTFB) verbessert. Dies liegt daran, dass Sie Teilantworten an den Client zurücksenden können, sobald sie verfügbar sind. Darüber hinaus können Sie Response-Streaming verwenden, um Funktionen zu erstellen, die größere Nutzlasten zurückgeben.

Konfigurieren des Lambda-Funktionsspeichers

Lambda weist die Rechenleistung proportional zur Menge des konfigurierten Arbeitsspeichers zu. Arbeitsspeicher ist die Menge an Arbeitsspeicher, die Ihrer Lambda-Funktion zur Laufzeit zur Verfügung steht. Sie können den Arbeitsspeicher und die CPU-Leistung, die Ihrer Funktion zugewiesen sind, mithilfe der Einstellung Speicher erhöhen oder verringern. Sie können den Speicher zwischen 128 MB und 10 240 MB in Schritten von 1-MB konfigurieren. Bei 1.769 MB weist eine Funktion das Äquivalent einer vCPU auf (eine vCPU-Sekunde Guthaben pro Sekunde).

Auf dieser Seite wird beschrieben, wie und wann die Speichereinstellung für eine Lambda-Funktion aktualisiert wird.

Sections

Bestimmen der geeigneten Speichereinstellung für eine Lambda-Funktion

Speicher ist der Haupthelf zur Steuerung der Leistung einer Funktion. Die Standardeinstellung, 128 MB, ist die niedrigstmögliche Einstellung. Wir empfehlen, nur 128 MB für einfache Lambda-Funktionen zu verwenden, z. B. für Funktionen, die Ereignisse transformieren und an andere AWS -Services weiterleiten. Eine höhere Speicherzuweisung kann die Leistung für Funktionen verbessern, die importierte Bibliotheken, Lambda-Ebenen, Amazon Simple Storage Service (Amazon S3) oder Amazon Elastic File System (Amazon EFS) verwenden. Durch das Hinzufügen von mehr Arbeitsspeicher wird die CPU-Menge proportional erhöht, wodurch die verfügbare Rechenleistung insgesamt erhöht wird. Wenn eine Funktion CPU-, Netzwerk- oder Arbeitsspeichergebunden ist, kann eine Erhöhung der Speichereinstellung ihre Leistung erheblich verbessern.

Um die richtige Speicherkonfiguration für Ihre Funktionen zu finden, empfehlen wir die Verwendung des Open-SourceAWS Lambda -Power-Tuning-Tools. Dieses Tool verwendet AWS Step Functions , um mehrere gleichzeitige Versionen einer Lambda-Funktion mit unterschiedlichen Speicherzuweisungen auszuführen und die Leistung zu messen. Die Eingabefunktion wird in Ihrem AWS Konto ausgeführt und führt Live-HTTP-Aufrufe und SDK-Interaktion durch, um die

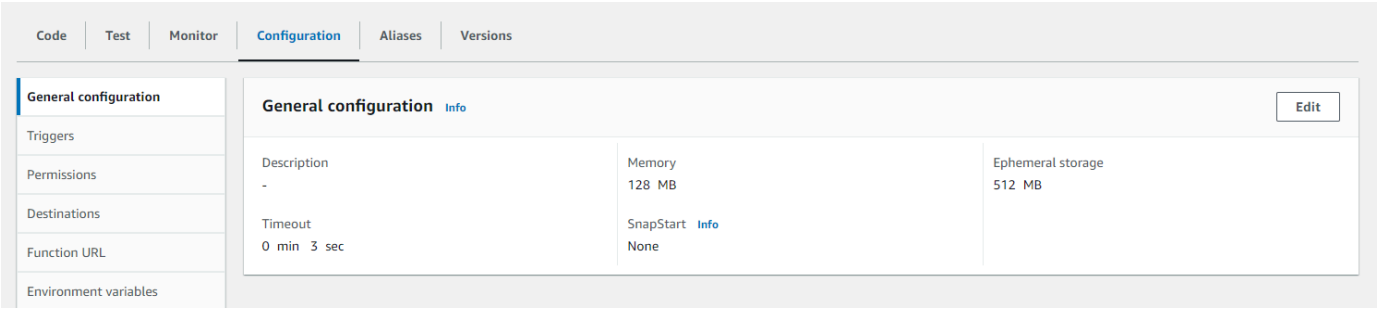
wahrscheinliche Leistung in einem Live-Produktionsszenario zu messen. Sie können auch einen CI/CD-Prozess implementieren, um dieses Tool zu verwenden, um die Leistung neuer Funktionen, die Sie bereitstellen, automatisch zu messen.

Konfigurieren des Funktionsspeichers (Konsole)

Sie können den Speicher Ihrer Funktion in der Lambda-Konsole konfigurieren.

So aktualisieren Sie den Speicher einer Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Allgemeine Konfiguration aus.



4. Wählen Sie unter Allgemeine Konfiguration die Option Bearbeiten aus.
5. Legen Sie für Speicher einen Wert zwischen 128 MB und 10.240 MB fest.
6. Wählen Sie Speichern.

Konfigurieren des Funktionsspeichers (AWS CLI)

Sie können den update-function-configuration Befehl verwenden, um den Speicher Ihrer Funktion zu konfigurieren.

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --memory-size 1024
```

Konfigurieren des Funktionsspeichers (AWS SAM)

Sie können die verwendenAWS Serverless Application Model, um den Speicher für Ihre Funktion zu konfigurieren. Aktualisieren Sie die -MemorySizeEigenschaft in Ihrer -`template.yaml`Datei und führen Sie dann sam deploy aus.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 1024
      # Other function properties...
```

Akzeptieren von Empfehlungen für den Funktionsspeicher (Konsole)

Wenn Sie über Administratorberechtigungen in AWS Identity and Access Management (IAM) verfügen, können Sie sich dafür entscheiden, Empfehlungen für Lambda-Funktionsspeichereinstellungen von zu erhalten AWS Compute Optimizer. Anweisungen dazu, wie Sie Speicherempfehlungen für Ihr Konto oder Ihr Unternehmen aktivieren, finden Sie unter Aktivieren Ihres Kontos im AWS Compute Optimizer -Benutzerhandbuch.

> **Note**
>
> Compute Optimizer unterstützt nur Funktionen, die die x86_64-Architektur verwenden.

Wenn Sie sich angemeldet haben und Ihre Lambda-Funktion die Anforderungen von Compute Optimizer erfüllt, können Sie Empfehlungen zum Funktionsspeicher von Compute Optimizer in der Lambda-Konsole unter Allgemeine Konfiguration anzeigen und akzeptieren.

Konfigurieren des flüchtigen Speichers für Lambda-Funktionen

Lambda bietet flüchtigen Speicher für Funktionen im `/tmp` Verzeichnis . Dieser Speicher ist temporär und für jede Ausführungsumgebung eindeutig. Mit der Einstellung Flüchtiger Speicher können Sie die Menge des Ihrer Funktion zugewiesenen flüchtigen Speichers steuern. Sie können flüchtigen Speicher zwischen 512 MB und 10 240 MB in Schritten von 1-MB konfigurieren. Alle in gespeicherten Daten `/tmp` werden im Ruhezustand mit einem von verwalteten Schlüssel verschlüsselt AWS.

Auf dieser Seite werden häufige Anwendungsfälle und die Aktualisierung des flüchtigen Speichers für eine Lambda-Funktion beschrieben.

Sections

Häufige Anwendungsfälle für erhöhten flüchtigen Speicher

Hier sind einige häufige Anwendungsfälle, die von erhöhtem flüchtigem Speicher profitieren:

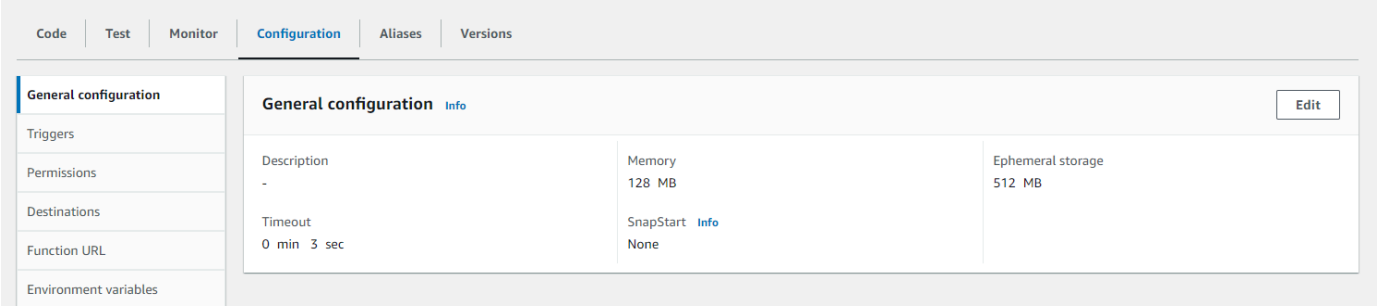
- E xtract-transform-load (ETL)-Aufträge: Erhöhen Sie den flüchtigen Speicher, wenn Ihr Code eine Zwischenberechnung durchführt oder andere Ressourcen herunterlädt, um die Verarbeitung abzuschließen. Durch den temporäreren Speicherplatz können komplexere ETL-Aufträge in Lambda-Funktionen ausgeführt werden.
- Machine Learning (ML)-Inferenz: Viele Inferenzaufgaben basieren auf großen Referenzdatendateien, einschließlich Bibliotheken und Modellen. Mit mehr flüchtigem Speicher können Sie größere Modelle von Amazon Simple Storage Service (Amazon S3) auf herunterladen `/tmp` und sie in Ihrer Verarbeitung verwenden.
- Datenverarbeitung: Bei Workloads, die Objekte von Amazon S3 als Reaktion auf S3-Ereignisse herunterladen, ermöglicht mehr `/tmp` Speicherplatz die Verarbeitung größerer Objekte, ohne die In-Memory-Verarbeitung zu verwenden. Workloads, die PDFs erstellen oder Medien verarbeiten, profitieren auch von flüchtigem Speicher.
- Grafikverarbeitung: Die Bildverarbeitung ist ein häufiger Anwendungsfall für Lambda-basierte Anwendungen. Bei Workloads, die große TIFF-Dateien oder Satellitenbilder verarbeiten, erleichtert ein flüchtiger Speicher die Verwendung von Bibliotheken und die Berechnung in Lambda.

Flüchtigen Speicher konfigurieren (Konsole)

Sie können den flüchtigen Speicher in der Lambda-Konsole konfigurieren.

So ändern Sie den flüchtigen Speicher für eine Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Allgemeine Konfiguration aus.



4. Wählen Sie unter Allgemeine Konfiguration die Option Bearbeiten aus.
5. Legen Sie für Flüchtigen Speicher einen Wert zwischen 512 MB und 10 240 MB in Schritten von 1-MB fest.
6. Wählen Sie Speichern.

Konfigurieren des flüchtigen Speichers (AWS CLI)

Sie können den update-function-configuration Befehl verwenden, um flüchtigen Speicher zu konfigurieren.

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --ephemeral-storage '{"Size": 1024}'
```

Konfigurieren des flüchtigen Speichers (AWS SAM)

Sie können die verwendenAWS Serverless Application Model, um den flüchtigen Speicher für Ihre Funktion zu konfigurieren. Aktualisieren Sie die -EphemeralStorageEigenschaft in Ihrer `-template.yaml`Datei und führen Sie dann sam deploy aus.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs20.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      # Other function properties...
```

Timeout für Lambda-Funktionen konfigurieren

Lambda führt Ihren Code für eine festgelegte Zeitspanne aus, bevor ein Timeout erfolgt. Beim Timeout handelt es sich um die maximale Zeitspanne in Sekunden, die eine Lambda-Funktion ausgeführt werden kann. Der Standardwert für diese Einstellung ist 3 Sekunden, Sie können ihn jedoch in Schritten von 1 Sekunde bis zu einem Maximalwert von 900 Sekunden (15 Minuten) anpassen.

Auf dieser Seite wird beschrieben, wie und wann die Timeout-Einstellung für eine Lambda-Funktion aktualisiert werden muss.

Sections

Ermitteln des geeigneten Timeout-Werts für eine Lambda-Funktion

Wenn der Timeout-Wert nahe an der durchschnittlichen Dauer einer Funktion liegt, besteht ein höheres Risiko, dass die Funktion unerwartet beendet wird. Die Dauer einer Funktion kann je nach Umfang der Datenübertragung und -verarbeitung sowie der Latenz aller Dienste, mit denen die Funktion interagiert, variieren. Zu den häufigsten Ursachen für Timeouts gehören:

- Downloads von Amazon Simple Storage Service (Amazon S3) sind größer oder dauern länger als der Durchschnitt.
- Eine Funktion sendet eine Anfrage an einen anderen Service, dessen Beantwortung länger dauert.
- Die einer Funktion zur Verfügung gestellten Parameter erfordern eine höhere Rechenkomplexität in der Funktion, wodurch der Aufruf länger dauert.

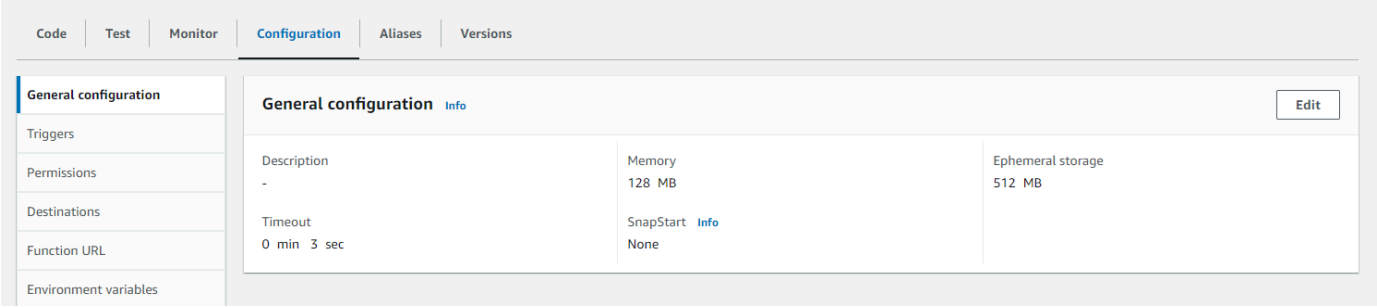
Stellen Sie beim Testen Ihrer Anwendung sicher, dass Ihre Tests die Größe und Menge der Daten sowie realistische Parameterwerte genau wiedergeben. Tests verwenden aus Gründen der Benutzerfreundlichkeit häufig kleine Stichproben. Sie sollten jedoch Datensätze verwenden, die sich an der Obergrenze dessen befinden, was für Ihre Arbeitslast vernünftigerweise zu erwarten ist.

Timeout konfigurieren (Konsole)

Sie können das Funktions-Timeout in der Lambda-Konsole konfigurieren.

Um das Timeout für eine Funktion zu ändern

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Allgemeine Konfiguration.



4. Wählen Sie unter Allgemeine Konfiguration die Option Bearbeiten aus.
5. Stellen Sie für Timeout einen Wert zwischen 1 und 900 Sekunden (15 Minuten) ein.
6. Wählen Sie Speichern.

Timeout () konfigurieren AWS CLI

Sie können den update-function-configurationBefehl verwenden, um den Timeout-Wert in Sekunden zu konfigurieren. Der folgende Beispielbefehl erhöht das Funktions-Timeout auf 120 Sekunden (2 Minuten).

Example

```
aws lambda update-function-configuration \
  --function-name my-function \
  --timeout 120
```

Timeout () konfigurieren AWS SAM

Sie können das verwenden AWS Serverless Application Model, um den Timeout-Wert für Ihre Funktion zu konfigurieren. Aktualisieren Sie die Timeout-Eigenschaft in Ihrer `template.yaml` Datei und führen Sie dann sam deploy aus.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      # Other function properties...
```

Verwenden Sie Lambda-Umgebungsvariablen, um Werte im Code zu konfigurieren

Sie können Umgebungsvariablen verwenden, um das Verhalten Ihrer Funktion anzupassen, ohne Code zu aktualisieren. Eine Umgebungsvariable ist ein Zeichenfolgenpaar, das in der versionsspezifischen Konfiguration einer Funktion gespeichert ist. Die Lambda-Laufzeit stellt Umgebungsvariablen für den Code zur Verfügung und legt zusätzliche Umgebungsvariablen mit Informationen über die Funktion und die Aufrufanforderung fest.

> **Note**
>
> Um die Sicherheit zu erhöhen, empfehlen wir, AWS Secrets Manager anstelle von Umgebungsvariablen Datenbankanmeldedaten und andere vertrauliche Informationen wie API-Schlüssel oder Autorisierungstoken zu speichern. Weitere Informationen finden Sie unter Geheimnisse erstellen und verwalten mit AWS Secrets Manager.

Umgebungsvariablen werden vor dem Funktionsaufruf nicht ausgewertet. Jeder von Ihnen definierte Wert wird als Literalzeichenfolge betrachtet und nicht erweitert. Führen Sie die Variablenauswertung in Ihrem Funktionscode durch.

Sie können Umgebungsvariablen in Lambda mithilfe der Lambda-Konsole, der AWS Command Line Interface (AWS CLI), AWS Serverless Application Model (AWS SAM) oder mithilfe eines AWS SDK konfigurieren.

Console

Sie definieren Umgebungsvariablen für die unveröffentlichte Version Ihrer Funktion. Wenn Sie eine Version veröffentlichen, werden die Umgebungsvariablen zusammen mit anderen versionsspezifischen Konfigurationseinstellungen für diese Version gesperrt.

Sie erstellen eine Umgebungsvariable für Ihre Funktion, indem Sie einen Schlüssel und einen Wert definieren. Ihre Funktion verwendet den Namen des Schlüssels, um den Wert der Umgebungsvariablen abzurufen.

So legen Sie Umgebungsvariablen in der Lambda-Konsole fest

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.

3. Wählen Sie Configuration (Konfiguration) und dann Environment variables (Umgebungsvariablen) aus.
4. Wählen Sie unter Environment variables (Umgebungsvariablen) die Option Edit (Bearbeiten).
5. Wählen Sie Umgebungsvariablen hinzufügen aus.
6. Geben Sie einen Schlüssel und einen Wert ein.

   Voraussetzungen

   - Schlüssel beginnen mit einem Buchstaben und bestehen aus mindestens zwei Zeichen.
   - Schlüssel enthalten nur Buchstaben, Zahlen und den Unterstrich (_).
   - Schlüssel sind nicht Lambda vorbehalten.
   - Die Gesamtgröße aller Umgebungsvariablen überschreitet nicht 4 KB.
7. Wählen Sie Save aus.

Generieren einer Liste von Umgebungsvariablen im Konsolen-Code-Editor

Sie können im Lambda-Code-Editor eine Liste von Umgebungsvariablen generieren. So können Sie beim Programmieren schnell auf Ihre Umgebungsvariablen verweisen.

1. Wählen Sie die Registerkarte Code.
2. Wählen Sie die Registerkarte Umgebungsvariablen.
3. Wählen Sie Tools, Umgebungsvariablen anzeigen.

Umgebungsvariablen bleiben verschlüsselt, wenn sie im Code-Editor der Konsole aufgeführt werden. Wenn Sie Verschlüsselungshilfen für die Verschlüsselung während der Übertragung aktiviert haben, bleiben diese Einstellungen unverändert. Weitere Informationen finden Sie unter Sicherung von Lambda-Umgebungsvariablen.

Die Liste der Umgebungsvariablen ist schreibgeschützt und nur auf der Lambda-Konsole verfügbar. Diese Datei ist nicht enthalten, wenn Sie das ZIP-Dateiarchiv der Funktion herunterladen, und Sie können keine Umgebungsvariablen hinzufügen, indem Sie diese Datei hochladen.

AWS CLI

Im folgenden Beispiel werden zwei Umgebungsvariablen für eine Funktion mit dem Namen festgeleg `my-function`.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --environment "Variables={BUCKET=DOC-EXAMPLE-BUCKET,KEY=file.txt}"
```

Wenn Sie Umgebungsvariablen mit dem `update-function-configuration`-Befehl anwenden, wird der gesamte Inhalt der `Variables`-Struktur ersetzt. Um vorhandene Umgebungsvariablen beibehalten, wenn Sie eine neue hinzufügen, schließen Sie alle vorhandenen Werte in Ihre Anforderung ein.

Mit dem `get-function-configuration`-Befehl können Sie die aktuelle Konfiguration abrufen.

```
aws lambda get-function-configuration \
  --function-name my-function
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-2:111122223333:function:my-function",
    "Runtime": "nodejs20.x",
    "Role": "arn:aws:iam::111122223333:role/lambda-role",
    "Environment": {
        "Variables": {
            "BUCKET": "DOC-EXAMPLE-BUCKET",
            "KEY": "file.txt"
        }
    },
    "RevisionId": "0894d3c1-2a3d-4d48-bf7f-abade99f3c15",
    ...
}
```

Sie können die Revisions-ID aus der Ausgabe von `get-function-configuration` als Parameter an `update-function-configuration` übergeben. Dadurch wird sichergestellt, dass sich die Werte zwischen dem Lesen und dem Aktualisieren der Konfiguration nicht ändern.

Um den Verschlüsselungsschlüssel einer Funktion zu konfigurieren, legen Sie die `KMSKeyARN`-Option fest.

```
aws lambda update-function-configuration \
  --function-name my-function \
```

```
  --kms-key-arn arn:aws:kms:us-east-2:111122223333:key/055efbb4-xmpl-4336-
ba9c-538c7d31f599
```

AWS SAM

Sie können die verwenden AWS Serverless Application Model, um Umgebungsvariablen für Ihre Funktion zu konfigurieren. Aktualisieren Sie die Eigenschaften Umgebung und Variablen in Ihrer `template.yaml` Datei und führen Sie dann sam deploy aus.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: An AWS Serverless Application Model template describing your function.
Resources:
  my-function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: .
      Description: ''
      MemorySize: 128
      Timeout: 120
      Handler: index.handler
      Runtime: nodejs18.x
      Architectures:
        - x86_64
      EphemeralStorage:
        Size: 10240
      Environment:
        Variables:
          BUCKET: DOC-EXAMPLE-BUCKET
          KEY: file.txt
      # Other function properties...
```

AWS SDKs

Verwenden Sie die folgenden API-Operationen, um Umgebungsvariablen mithilfe eines AWS SDK zu verwalten.

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Weitere Informationen finden Sie in der AWS SDK-Dokumentation für Ihre bevorzugte Programmiersprache.

Definierte Laufzeitumgebungsvariablen

Lambda Laufzeiten setzen mehrere Umgebungsvariablen während der Initialisierung. Die meisten Umgebungsvariablen stellen Informationen über die Funktion oder Laufzeit bereit. Die Schlüssel für diese Umgebungsvariablen sind reserviert und können nicht in der Funktionskonfiguration gesetzt werden.

Reservierte Umgebungsvariablen

- `_HANDLER` – Der für die Funktion konfigurierte Handler-Speicherort.
- `_X_AMZN_TRACE_ID` – Die X-Ray-Tracing-Header. Diese Umgebungsvariable ändert sich bei jedem Aufruf.
  - Diese Umgebungsvariable ist nicht für reine OS-Laufzeiten (die `provided`-Laufzeitfamilie) definiert. Sie können `_X_AMZN_TRACE_ID` für benutzerdefinierte Laufzeiten einstellen, indem Sie den Antwort-Header `Lambda-Runtime-Trace-Id` der Nächster Aufruf verwenden.
  - Für die Java-Laufzeit-Versionen 17 und höher wird diese Umgebungsvariable nicht verwendet. Stattdessen speichert Lambda Ablaufverfolgungsinformationen in der Systemeigenschaft `com.amazonaws.xray.traceHeader`.
- `AWS_DEFAULT_REGION`— Die Standardeinstellung AWS-Region , in der die Lambda-Funktion ausgeführt wird.
- `AWS_REGION`— Der AWS-Region Ort, an dem die Lambda-Funktion ausgeführt wird. Wenn eingegeben, überschreibt dieser Wert die `AWS_DEFAULT_REGION`.
  - Weitere Informationen zur Verwendung der AWS-Region Umgebungsvariablen mit AWS SDKs finden Sie unter AWS Region im Referenzhandbuch für AWS SDKs und Tools.
- `AWS_EXECUTION_ENV` – Die Laufzeit-Kennung mit dem Präfix `AWS_Lambda_` z. B. `AWS_Lambda_java8`. Diese Umgebungsvariable ist nicht für reine OS-Laufzeiten (die `provided`-Laufzeitfamilie) definiert.
- `AWS_LAMBDA_FUNCTION_NAME` – Der Name der Funktion.
- `AWS_LAMBDA_FUNCTION_MEMORY_SIZE` – Die Menge des für die Funktion verfügbaren Speichers in MB.
- `AWS_LAMBDA_FUNCTION_VERSION` – Die Version der Funktion, die gerade ausgeführt wird.

- `AWS_LAMBDA_INITIALIZATION_TYPE` – Der Initialisierungstyp der Funktion, der `on-demand`, `provisioned-concurrency` oder `snap-start` ist. Weitere Informationen finden Sie unter Konfigurieren der bereitgestellten Gleichzeitigkeit oder unter Verbesserung der Startleistung mit Lambda SnapStart.
- `AWS_LAMBDA_LOG_GROUP_NAME`, `AWS_LAMBDA_LOG_STREAM_NAME` — Der Name der Amazon CloudWatch Logs-Gruppe und des Streams für die Funktion. Die `AWS_LAMBDA_LOG_STREAM_NAME` Umgebungsvariablen `AWS_LAMBDA_LOG_GROUP_NAME` und sind in SnapStart Lambda-Funktionen nicht verfügbar.
- `AWS_ACCESS_KEY`, `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY`, `AWS_SESSION_TOKEN` – Die Zugriffsschlüssel, die über die Ausführungsrolle der Funktion bezogen wurden.
- `AWS_LAMBDA_RUNTIME_API` – (Benutzerdefinierte Laufzeit) Host und Port der Laufzeit-API.
- `LAMBDA_TASK_ROOT` – Der Pfad zu Ihrem Lambda-Funktionscode.
- `LAMBDA_RUNTIME_DIR` – Der Pfad zu Laufzeitbibliotheken.

Die folgenden zusätzlichen Umgebungsvariablen sind nicht vorbehalten und können in Ihrer Funktionskonfiguration erweitert werden.

Nicht reservierte Umgebungsvariablen

- `LANG` – Das Gebietsschema der Laufzeit (`en_US.UTF-8`).
- `PATH` – Der Ausführungspfad (`/usr/local/bin:/usr/bin/:/bin:/opt/bin`).
- `LD_LIBRARY_PATH` – Der Pfad der Systembibliothek (`/var/lang/lib:/lib64:/usr/lib64:$LAMBDA_RUNTIME_DIR:$LAMBDA_RUNTIME_DIR/lib:$LAMBDA_TASK_ROOT:$LAMBDA_TASK_ROOT/lib:/opt/lib`).
- `NODE_PATH` – (Node.js) Der Node.js-Bibliothekspfad (`/opt/nodejs/node12/node_modules/:/opt/nodejs/node_modules:$LAMBDA_RUNTIME_DIR/node_modules`).
- `PYTHONPATH` – (Python 2.7, 3.6, 3.8) Der Python-Bibliothekspfad (`$LAMBDA_RUNTIME_DIR`).
- `GEM_PATH` – (Ruby) Der Pfad der Ruby-Bibliothek (`$LAMBDA_TASK_ROOT/vendor/bundle/ruby/2.5.0:/opt/ruby/gems/2.5.0`).
- `AWS_XRAY_CONTEXT_MISSING` – Für die X-Ray-Ablaufverfolgung legt Lambda dies auf `LOG_ERROR` fest, um Laufzeitfehler aus dem X-Ray-SDK zu vermeiden.
- `AWS_XRAY_DAEMON_ADDRESS` – Die IP-Adresse und der Port des X-Ray-Daemons.
- `AWS_LAMBDA_DOTNET_PREJIT`: Legen Sie diese Variable für die .NET 6- und die .NET 7-Laufzeit fest, um .NET-spezifische Laufzeitoptimierungen zu aktivieren oder zu deaktivieren. Zu den Werten

gehören `always`, `never` und `provisioned-concurrency`. Weitere Informationen finden Sie unter Konfiguration der bereitgestellten Parallelität für eine Funktion.

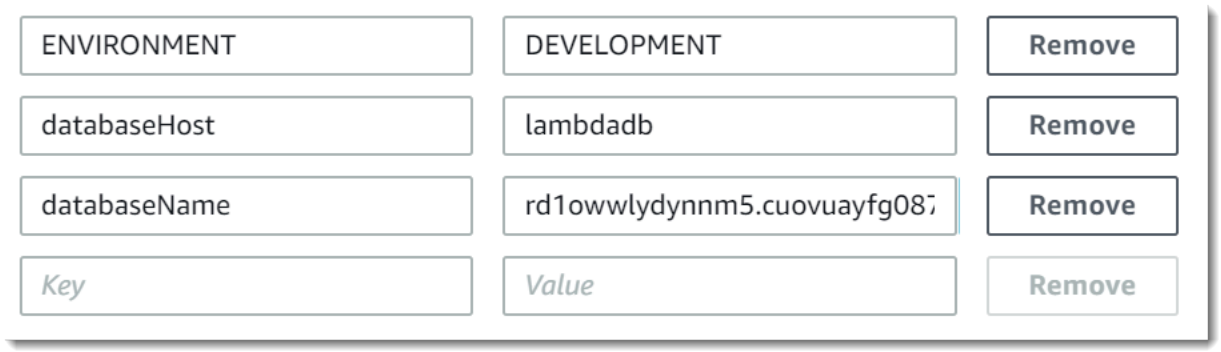
- `TZ` – Die Zeitzone der Umgebung (`UTC`). Die Ausführungsumgebung verwendet NTP, um die Systemuhr zu synchronisieren.

Die angezeigten Beispielwerte spiegeln die neuesten Laufzeiten wider. Das Vorhandensein bestimmter Variablen oder deren Werte kann je nach früheren Laufzeiten unterschiedlich sein.

Beispielszenario für Umgebungsvariablen

Sie können Umgebungsvariablen verwenden, um das Funktionsverhalten in Ihrer Testumgebung und Produktionsumgebung anzupassen. Zum Beispiel können Sie zwei Funktionen mit demselben Code aber mit unterschiedlichen Konfigurationen erstellen. Die eine Funktion stellt eine Verbindung mit einer Testdatenbank und die andere mit einer Produktionsdatenbank her. In diesem Fall verwenden Sie Umgebungsvariablen, um den Hostnamen und andere Verbindungsdetails für die Datenbank an die Funktion zu übergeben.

Das folgende Beispiel zeigt, wie der Datenbankhost und der Datenbankname als Umgebungsvariablen definiert werden.



Wenn Ihre Testumgebung mehr Debugging-Informationen generieren soll als die Produktionsumgebung, können Sie eine Umgebungsvariable festlegen, um Ihre Testumgebung so zu konfigurieren, dass eine ausführlichere Protokollierung oder eine detailliertere Ablaufverfolgung verwendet wird.

Sicherung von Lambda-Umgebungsvariablen

Sie können Ihre Umgebungsvariablen sichern, können Sie eine serverseitige Verschlüsselung nutzen, um Ihre Data-at-Rest zu schützen und eine clientseitige Verschlüsselung, um Ihre Daten während der Übertragung zu schützen.

> **Note**
>
> Um die Datenbanksicherheit zu erhöhen, empfehlen wir, AWS Secrets Manager anstelle von Umgebungsvariablen zum Speichern von Datenbankanmeldedaten zu verwenden. Weitere Informationen finden Sie unter Verwendung AWS Lambda mit Amazon RDS.

Sicherheit im Ruhezustand

Lambda bietet im Ruhezustand immer serverseitiger Verschlüsselung mit einem AWS KMS key an. Standardmäßig verwendet Lambda einen Von AWS verwalteter Schlüssel. Wenn dieses Standardverhalten Ihrem Workflow entspricht, müssen Sie nichts anderes einrichten. Lambda erstellt das Von AWS verwalteter Schlüssel in Ihrem Konto und verwaltet die Berechtigungen dafür für Sie. AWS berechnet Ihnen keine Gebühren für die Verwendung dieses Schlüssels.

Wenn Sie möchten, können Sie stattdessen einen vom AWS KMS Kunden verwalteten Schlüssel bereitstellen. Sie können dies tun, um die Drehung des KMS-Schlüssels zu steuern oder die Anforderungen Ihrer Organisation für die Verwaltung von KMS-Schlüsseln zu erfüllen. Wenn Sie einen vom Kunden verwalteten Schlüssel verwenden, können nur Benutzer in Ihrem Konto mit Zugriff auf den KMS-Schlüssel Umgebungsvariablen für die Funktion anzeigen oder verwalten.

Für vom Kunden verwaltete Schlüssel fallen AWS KMS Standardgebühren an. Weitere Informationen finden Sie unter AWS Key Management Service Preise.

Sicherheit während der Übertragung

Für zusätzliche Sicherheit können Sie Helfer für die Verschlüsselung bei der Übertragung aktivieren, wodurch sichergestellt wird, dass Ihre Umgebungsvariablen clientseitig verschlüsselt sind, um sie während der Übertragung zu schützen.

So konfigurieren Sie die Verschlüsselung für Ihre Umgebungsvariablen

1. Verwenden Sie AWS Key Management Service (AWS KMS), um vom Kunden verwaltete Schlüssel für Lambda zu erstellen, die für die serverseitige und clientseitige Verschlüsselung verwendet werden sollen. Weitere Informationen finden Sie unter Erstellen von Schlüsseln im AWS Key Management Service -Entwicklerhandbuch.
2. Navigieren Sie mithilfe der Lambda-Konsole zur Seite Umgebungsvariablen bearbeiten.
   a. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

b. Wählen Sie eine Funktion aus.

c. Wählen Sie Konfiguration und dann Umgebungsvariablen aus der linken Navigationsleiste.

d. Wählen Sie im Abschnitt Umgebungsvariablen Bearbeiten aus.

e. Erweitern Sie Encryption configuration (Verschlüsselungskonfiguration).

3. (Optional) Aktivieren Sie Konsolenverschlüsselungshelfer, um die clientseitige Verschlüsselung zu verwenden, um Ihre Daten während der Übertragung zu schützen.

   a. Wählen Sie unter Verschlüsselung während der Übertragung die Option Helfer für die Verschlüsselung während der Übertragung aktivieren aus.

   b. Wählen Sie für jede Umgebungsvariable, für die Sie Konsolenverschlüsselungshilfen aktivieren möchten, neben der Umgebungsvariablen die Option Encrypt (Verschlüsseln) aus.

   c. Wählen AWS KMS key Sie unter Verschlüsselung bei der Übertragung einen vom Kunden verwalteten Schlüssel aus, den Sie zu Beginn dieses Verfahrens erstellt haben.

   d. Wählen Sie Ausführungsrollenrichtlinie und kopieren Sie die Richtlinie. Diese Richtlinie gewährt der Ausführungsrolle Ihrer Funktion die Berechtigung zum Entschlüsseln der Umgebungsvariablen.

      Speichern Sie diese Richtlinie zur Verwendung im letzten Schritt dieses Verfahrens.

   e. Fügen Sie Ihrer Funktion Code hinzu, der die Umgebungsvariablen entschlüsselt. Wählen Sie Geheimnisausschnitt entschlüsseln, um ein Beispiel anzuzeigen.

4. (Optional) Geben Sie Ihren kundenverwalteten Schlüssel zur Verschlüsselung im Ruhezustand an.

   a. Wählen Sie Kundenmasterschlüssel verwenden aus.

   b. Wählen Sie einen vom Kunden verwalteten Schlüssel aus, den Sie zu Beginn dieses Verfahrens erstellt haben.

5. Wählen Sie Speichern.

6. Richten Sie Berechtigungen ein.

   Wenn Sie einen vom Kunden verwalteten Schlüssel mit serverseitiger Verschlüsselung verwenden, erteilen Sie allen Benutzern oder Rollen Berechtigungen zum Anzeigen oder Verwalten von Umgebungsvariablen für die Funktion. Weitere Informationen finden Sie unter Verwalten von Berechtigungen für den serverseitigen Verschlüsselungs-KMS-Schlüssel.

   Wenn Sie die clientseitige Verschlüsselung für die Sicherheit während der Übertragung aktivieren, benötigt Ihre Funktion die Berechtigung zum Aufrufen der `kms:Decrypt`-API-

Operation. Fügen Sie die Richtlinie, die Sie zuvor in diesem Verfahren gespeichert haben, zur Ausführungsrolle der Funktion hinzu.

Verwalten von Berechtigungen für den serverseitigen Verschlüsselungs-KMS-Schlüssel

Für Ihren Benutzer oder die Ausführungsrolle der Funktion sind keine AWS KMS Berechtigungen erforderlich, um den Standard-Verschlüsselungsschlüssel zu verwenden. Um einen vom kundenverwalteten Schlüssel verwenden zu können, benötigen Sie eine Berechtigungen zur Verwendung des Schlüssels. Lambda erstellt anhand Ihrer Berechtigungen eine Berechtigungserteilung für den Schlüssel. So wird es Lambda ermöglicht, diesen für die Verschlüsselung zu verwenden.

- `kms:ListAliases` – Zur Ansicht von Schlüssel in der Lambda-Konsole.
- `kms:CreateGrant`, `kms:Encrypt` – Zum Konfigurieren eines vom Kunden verwalteten Schlüssels für eine Funktion.
- `kms:Decrypt` – Zum Anzeigen und Verwalten von Umgebungsvariablen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt sind.

Sie können diese Berechtigungen über Ihre AWS-Konto oder über die ressourcenbasierte Berechtigungsrichtlinie eines Schlüssels erhalten. `ListAliases`wird durch die verwalteten Richtlinien für Lambda bereitgestellt. Schlüsselrichtlinien gewähren Benutzern in der Gruppe Key users (Schlüsselbenutzer) die verbleibenden Berechtigungen.

Benutzer ohne `Decrypt`-Berechtigungen können Funktionen weiterhin verwalten, aber sie können keine Umgebungsvariablen anzeigen oder in der Lambda-Konsole verwalten. Um zu verhindern, dass ein Benutzer Umgebungsvariablen anzeigen kann, fügen Sie den Berechtigungen des Benutzers eine Anweisung hinzu, die den Zugriff auf den Standardschlüssel, einen vom Kunden verwalteten Schlüssel oder alle Schlüssel verweigert.

Example IAM-Richtlinie – Verweigern des Zugriffs nach Schlüssel-ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
```

```
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-2:111122223333:key/3be10e2d-xmpl-4be4-
bc9d-0405a71945cc"
        }
    ]
}
```

Details zum Verwalten von Schlüsselberechtigungen finden Sie unter Key policies in AWS KMS im AWS Key Management Service -Entwicklerhandbuch.

Lambda-Umgebungsvariablen abrufen

Umgebungsvariablen in Ihrem Funktionscode können Sie mit der Standardmethode für Ihre Programmiersprache abrufen.

Node.js

```
let region = process.env.AWS_REGION
```

Python

```
import os
  region = os.environ['AWS_REGION']
```

> **Note**
>
> In einigen Fällen müssen Sie möglicherweise das folgende Format verwenden:
>
> ```
> region = os.environ.get('AWS_REGION')
> ```

Ruby

```
region = ENV["AWS_REGION"]
```

Java

```
String region = System.getenv("AWS_REGION");
```

Go

```
var region = os.Getenv("AWS_REGION")
```

C#

```
string region = Environment.GetEnvironmentVariable("AWS_REGION");
```

PowerShell

```
$region = $env:AWS_REGION
```

Lambda speichert Umgebungsvariablen sicher, indem sie im Ruhezustand verschlüsselt werden. Sie können Lambda so konfigurieren, dass es einen anderen Verschlüsselungsschlüssel verwendet, Umgebungsvariablenwerte auf der Clientseite verschlüsselt oder Umgebungsvariablen in einer AWS CloudFormation Vorlage mit festlegen. AWS Secrets Manager

Lambda-Funktionen Zugriff auf Ressourcen in einer Amazon VPC gewähren

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie private Netzwerke in Ihren AWS-Konto Host-Ressourcen wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances, Amazon Relational Database Service (Amazon RDS) -Instances und Amazon-Instances erstellen. ElastiCache Sie können Ihrer Lambda-Funktion Zugriff auf Ressourcen gewähren, die in einer Amazon-VPC gehostet werden, indem Sie Ihre Funktion über die privaten Subnetze, die die Ressourcen enthalten, an die VPC anhängen. Folgen Sie den Anweisungen in den folgenden Abschnitten, um eine Lambda-Funktion über die Lambda-Konsole, die AWS Command Line Interface (AWS CLI) oder an eine Amazon VPC anzuhängen. AWS SAM

> **Note**
>
> Jede Lambda-Funktion wird in einer VPC ausgeführt, die dem Lambda-Service gehört und von diesem verwaltet wird. Diese VPCs werden automatisch von Lambda verwaltet und sind für Kunden nicht sichtbar. Die Konfiguration Ihrer Funktion für den Zugriff auf andere AWS Ressourcen in einer Amazon VPC hat keine Auswirkungen auf die von Lambda verwaltete VPC, in der Ihre Funktion ausgeführt wird.

Sections

Erforderliche IAM-Berechtigungen

Um eine Lambda-Funktion an eine Amazon-VPC in Ihrer anzuhängen AWS-Konto, benötigt Lambda Berechtigungen zum Erstellen und Verwalten der Netzwerkschnittstellen, die es verwendet, um Ihrer Funktion Zugriff auf die Ressourcen in der VPC zu gewähren.

Die von Lambda erstellten Netzwerkschnittstellen werden als Hyperplane Elastic Network Interfaces oder Hyperplane ENIs bezeichnet. Weitere Informationen zu diesen Netzwerkschnittstellen finden Sie unter. the section called “Grundlegendes zu Hyperplane Elastic Network Interfaces (ENIs)”

Sie können Ihrer Funktion die erforderlichen Berechtigungen erteilen, indem Sie die AWS verwaltete Richtlinie der Ausführungsrolle Ihrer Funktion AWSLambdaVPCAccessExecutionRolezuordnen. Wenn Sie eine neue Funktion in der Lambda-Konsole erstellen und sie an eine VPC anhängen, fügt Lambda diese Berechtigungsrichtlinie automatisch für Sie hinzu.

Wenn Sie es vorziehen, Ihre eigene IAM-Berechtigungsrichtlinie zu erstellen, stellen Sie sicher, dass Sie alle der folgenden Berechtigungen hinzufügen:

- ec2: Schnittstelle CreateNetwork
- ec2: DescribeNetwork Interfaces — Diese Aktion funktioniert nur, wenn sie auf allen Ressourcen erlaubt ist ()`"Resource": "*"`.
- ec2: DescribeSubnets
- ec2: DeleteNetwork Interface — Wenn Sie in der Ausführungsrolle keine Ressourcen-ID für DeleteNetworkInterface angeben, kann Ihre Funktion möglicherweise nicht auf die VPC zugreifen. Geben Sie entweder eine eindeutige Ressourcen-ID an oder schließen Sie alle Ressourcen-IDs ein, z. B. `"Resource": "arn:aws:ec2:us-west-2:123456789012:*/*"`.
- ec2: AssignPrivate IpAddresses
- ec2: UnassignPrivate IpAddresses

Beachten Sie, dass die Rolle Ihrer Funktion diese Berechtigungen nur benötigt, um die Netzwerkschnittstellen zu erstellen, nicht aber, um Ihre Funktion aufzurufen. Sie können Ihre Funktion immer noch erfolgreich aufrufen, wenn sie an eine Amazon VPC angehängt ist, auch wenn Sie diese Berechtigungen aus der Ausführungsrolle Ihrer Funktion entfernen.

Um Ihre Funktion an eine VPC anzuhängen, muss Lambda auch Netzwerkressourcen mithilfe Ihrer IAM-Benutzerrolle verifizieren. Stellen Sie sicher, dass Ihre Benutzerrolle über die folgenden IAM-Berechtigungen verfügt:

- ec2: Gruppen DescribeSecurity
- ec2: DescribeSubnets
- ec2: DescribeVpcs

> **Note**
>
> Die Amazon EC2 EC2-Berechtigungen, die Sie der Ausführungsrolle Ihrer Funktion gewähren, werden vom Lambda-Service verwendet, um Ihre Funktion an eine VPC anzuhängen. Sie gewähren diese Berechtigungen jedoch auch implizit für den Code Ihrer Funktion. Das bedeutet, dass Ihr Funktionscode diese Amazon EC2 EC2-API-Aufrufe ausführen kann. Hinweise zu den folgenden bewährten Sicherheitsmethoden finden Sie unterthe section called “Bewährte Methoden für die Gewährleistung der Sicherheit”.

Hinzufügen von Lambda-Funktionen zu einer Amazon VPC in Ihrem AWS-Konto

Verbinden Sie Ihre Funktion mit einer Amazon VPC in Ihrem, AWS-Konto indem Sie die Lambda-Konsole verwenden, oder. AWS CLI AWS SAM Wenn Sie das AWS CLI oder verwenden oder AWS SAM eine bestehende Funktion mithilfe der Lambda-Konsole an eine VPC anhängen, stellen Sie sicher, dass die Ausführungsrolle Ihrer Funktion über die erforderlichen Berechtigungen verfügt, die im vorherigen Abschnitt aufgeführt sind.

Lambda-Funktionen können keine direkte Verbindung mit einer VPC mit Dedicated-Instance-Tenancy herstellen. Zum Herstellen einer Verbindung mit Ressourcen in einer dedizierten VPC verbinden Sie sie mit einer zweiten VPC mit Standard-Tenancy.

Lambda console

Um eine Funktion an eine Amazon VPC anzuhängen, wenn Sie sie erstellen

1. Öffnen Sie die Seite Functions (Funktionen) der Lambda-Konsole und wählen Sie Create function (Funktion erstellen) aus.
2. Geben Sie unter Basic information (Grundlegende Informationen) bei Function name (Funktionsname) einen Namen für Ihre Funktion ein.
3. Konfigurieren Sie die VPC-Einstellungen für die Funktion, indem Sie wie folgt vorgehen:
   a. Erweiterten Sie Advanced settings (Erweiterte Einstellungen).
   b. Wählen Sie VPC aktivieren und wählen Sie dann die VPC aus, an die Sie die Funktion anhängen möchten.

c. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.

d. Wählen Sie die Subnetze und Sicherheitsgruppen aus, für die Sie die Netzwerkschnittstelle erstellen möchten. Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

> **Note**
>
> Verbinden Sie Ihre Funktion für den Zugriff auf private Ressourcen mit privaten Subnetzen. Wenn Ihre Funktion Internetzugang benötigt, finden Sie weitere Informationen unterthe section called “Internetzugang für VPC-Funktionen”. Durch die Verbindung einer Funktion mit einem öffentlichen Subnetz erhält sie weder Internetzugang noch eine öffentliche IP-Adresse.

4. Wählen Sie Create function (Funktion erstellen).

Um eine bestehende Funktion an eine Amazon VPC anzuhängen

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie die Registerkarte Konfiguration und dann VPC.
3. Wählen Sie Bearbeiten aus.
4. Wählen Sie unter VPC die Amazon VPC aus, an die Sie Ihre Funktion anhängen möchten.
5. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.
6. Wählen Sie die Subnetze und Sicherheitsgruppen aus, für die Sie die Netzwerkschnittstelle erstellen möchten. Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

> **Note**
>
> Verbinden Sie Ihre Funktion für den Zugriff auf private Ressourcen mit privaten Subnetzen. Wenn Ihre Funktion Internetzugang benötigt, finden Sie weitere Informationen unterthe section called “Internetzugang für VPC-Funktionen”. Durch

die Verbindung einer Funktion mit einem öffentlichen Subnetz erhält sie weder Internetzugang noch eine öffentliche IP-Adresse.

7. Wählen Sie Save aus.

AWS CLI

Um eine Funktion an eine Amazon VPC anzuhängen, wenn Sie sie erstellen

- Führen Sie den folgenden `create-function` CLI-Befehl aus, um eine Lambda-Funktion zu erstellen und sie an eine VPC anzuhängen.

```
aws lambda create-function --function-name my-function \
--runtime nodejs20.x --handler index.js --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/lambda-role \
--vpc-config
 Ipv6AllowedForDualStack=true,SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a03
```

Geben Sie Ihre eigenen Subnetze und Sicherheitsgruppen an und legen Sie `Ipv6AllowedForDualStack` sie auf `true` oder `false` entsprechend Ihrem Anwendungsfall fest.

Um eine bestehende Funktion an eine Amazon VPC anzuhängen

- Führen Sie den folgenden `update-function-configuration` CLI-Befehl aus, um eine vorhandene Funktion an eine VPC anzuhängen.

```
aws lambda update-function-configuration --function-name my-function \
--vpc-config Ipv6AllowedForDualStack=true,
 SubnetIds=subnet-071f712345678e7c8,subnet-07fd123456788a036,SecurityGroupIds=sg-0859123
```

So trennen Sie Ihre Funktion von einer VPC

- Um Ihre Funktion von einer VPC zu trennen, führen Sie den folgenden `update-function-configuration` CLI-Befehl mit einer leeren Liste von VPC-Subnetzen und Sicherheitsgruppen aus.

```
aws lambda update-function-configuration --function-name my-function \
```

```
--vpc-config SubnetIds=[],SecurityGroupIds=[]
```

AWS SAM

So hängen Sie Ihre Funktion an eine VPC an

- Um eine Lambda-Funktion an eine Amazon VPC anzuhängen, fügen Sie die `VpcConfig` Eigenschaft zu Ihrer Funktionsdefinition hinzu, wie in der folgenden Beispielvorlage gezeigt. Weitere Informationen zu dieser Eigenschaft finden Sie unter AWS: :Lambda: :Function VpcConfig im AWS CloudFormation Benutzerhandbuch (die AWS SAM `VpcConfig` Eigenschaft wird direkt an die `VpcConfig` Eigenschaft einer AWS CloudFormation `AWS::Lambda::Function` Ressource übergeben).

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31

Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./lambda_function/
      Handler: lambda_function.handler
      Runtime: python3.12
      VpcConfig:
        SecurityGroupIds:
          - !Ref MySecurityGroup
        SubnetIds:
          - !Ref MySubnet1
          - !Ref MySubnet2
      Policies:
        - AWSLambdaVPCAccessExecutionRole

  MySecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Security group for Lambda function
      VpcId: !Ref MyVPC

  MySubnet1:
    Type: AWS::EC2::Subnet
    Properties:
```

```
      VpcId: !Ref MyVPC
      CidrBlock: 10.0.1.0/24

  MySubnet2:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref MyVPC
      CidrBlock: 10.0.2.0/24

  MyVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
```

Weitere Informationen zur Konfiguration Ihrer VPC in AWS SAM finden Sie unter AWS: :EC2: :VPC im Benutzerhandbuch.AWS CloudFormation

Internetzugang bei Verbindung mit einer VPC

Standardmäßig haben Lambda-Funktionen Zugriff auf das öffentliche Internet. Wenn Sie Ihre Funktion an eine VPC anhängen, kann sie nur auf Ressourcen zugreifen, die in dieser VPC verfügbar sind. Um Ihrer Funktion Zugriff auf das Internet zu gewähren, müssen Sie die VPC auch für den Internetzugang konfigurieren. Weitere Informationen hierzu finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Bewährte Methoden für die Verwendung von Lambda mit Amazon VPCs

Um sicherzustellen, dass Ihre Lambda-VPC-Konfiguration den Best-Practice-Richtlinien entspricht, befolgen Sie die Hinweise in den folgenden Abschnitten.

Bewährte Methoden für die Gewährleistung der Sicherheit

Um Ihre Lambda-Funktion an eine VPC anzuhängen, müssen Sie der Ausführungsrolle Ihrer Funktion eine Reihe von Amazon EC2 EC2-Berechtigungen erteilen. Diese Berechtigungen sind erforderlich, um die Netzwerkschnittstellen zu erstellen, die Ihre Funktion für den Zugriff auf die Ressourcen in der VPC verwendet. Diese Berechtigungen werden jedoch auch implizit für den Code Ihrer Funktion gewährt. Das bedeutet, dass Ihr Funktionscode berechtigt ist, diese Amazon EC2 EC2-API-Aufrufe zu tätigen.

Um dem Prinzip des Zugriffs mit den geringsten Rechten zu folgen, fügen Sie der Ausführungsrolle Ihrer Funktion eine Ablehnungsrichtlinie wie im folgenden Beispiel hinzu. Diese Richtlinie verhindert, dass Ihre Funktion die Amazon EC2 EC2-APIs aufruft, die der Lambda-Service verwendet, um Ihre Funktion an eine VPC anzuhängen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                 "ec2:CreateNetworkInterface",
                 "ec2:DeleteNetworkInterface",
                 "ec2:DescribeNetworkInterfaces",
                 "ec2:DetachNetworkInterface",
                 "ec2:AssignPrivateIpAddresses",
                 "ec2:UnassignPrivateIpAddresses",
            ],
            "Resource": [ "*" ],
            "Condition": {
                "ArnEquals": {
                    "lambda:SourceFunctionArn": [
                        "arn:aws:lambda:us-west-2:123456789012:function:my_function"
                    ]
                }
            }
        }
    ]
}
```

AWS bietet Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (ACLs), um die Sicherheit in Ihrer VPC zu erhöhen. Sicherheitsgruppen kontrollieren eingehenden und ausgehenden Verkehr für Ihre Ressourcen, Netzwerk-ACLs kontrollieren eingehenden und ausgehenden Zugriff für Ihre Subnetze. Sicherheitsgruppen bieten ausreichend Zugriffskontrolle für die meisten Subnetze. Sie können Netzwerk-ACLs verwenden, wenn Sie eine zusätzliche Sicherheitsebene für Ihre VPC benötigen. Allgemeine Richtlinien zu bewährten Sicherheitsmethoden bei der Verwendung von Amazon VPCs finden Sie unter Bewährte Sicherheitsmethoden für Ihre VPC im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Bewährte Methoden zur Leistungssteigerung

Wenn Sie Ihre Funktion an eine VPC anhängen, prüft Lambda, ob es eine verfügbare Netzwerkressource (Hyperplane ENI) gibt, mit der es eine Verbindung herstellen kann. Hyperplane-ENIs sind einer bestimmten Kombination von Sicherheitsgruppen und VPC-Subnetzen zugeordnet. Wenn Sie bereits eine Funktion an eine VPC angehängt haben, bedeutet die Angabe derselben Subnetze und Sicherheitsgruppen beim Anhängen einer anderen Funktion, dass Lambda die Netzwerkressourcen gemeinsam nutzen kann und die Notwendigkeit entfällt, ein neues Hyperplane-ENI zu erstellen. Weitere Informationen zu Hyperplane-ENIs und ihrem Lebenszyklus finden Sie unter. the section called “Grundlegendes zu Hyperplane Elastic Network Interfaces (ENIs)”

Grundlegendes zu Hyperplane Elastic Network Interfaces (ENIs)

Ein Hyperplane ENI ist eine verwaltete Ressource, die als Netzwerkschnittstelle zwischen Ihrer Lambda-Funktion und den Ressourcen fungiert, mit denen Ihre Funktion eine Verbindung herstellen soll. Der Lambda-Service erstellt und verwaltet diese ENIs automatisch, wenn Sie Ihre Funktion an eine VPC anhängen.

Hyperplane-ENIs sind für Sie nicht direkt sichtbar, und Sie müssen sie nicht konfigurieren oder verwalten. Wenn Sie jedoch wissen, wie sie funktionieren, können Sie besser verstehen, wie sich Ihre Funktion verhält, wenn Sie sie an eine VPC anhängen.

Wenn Sie zum ersten Mal eine Funktion mit einer bestimmten Kombination aus Subnetz und Sicherheitsgruppe an eine VPC anhängen, erstellt Lambda eine Hyperplane-ENI. Andere Funktionen in Ihrem Konto, die dieselbe Kombination aus Subnetz und Sicherheitsgruppe verwenden, können diese ENI ebenfalls verwenden. Wo immer möglich, verwendet Lambda bestehende ENIs wieder, um die Ressourcennutzung zu optimieren und die Erstellung neuer ENIs zu minimieren. Jedes Hyperplane ENI unterstützt bis zu 65.000 Verbindungen/Ports. Wenn die Anzahl der Verbindungen diesen Grenzwert überschreitet, skaliert Lambda die Anzahl der ENIs automatisch auf der Grundlage des Netzwerkverkehrs und der Parallelitätsanforderungen.

Bei neuen Funktionen bleibt Ihre Funktion, während Lambda eine Hyperplane-ENI erstellt, im Status Ausstehend und Sie können sie nicht aufrufen. Ihre Funktion wechselt erst in den Status Aktiv, wenn die Hyperplane ENI bereit ist, was mehrere Minuten dauern kann. Für bestehende Funktionen können Sie keine zusätzlichen Operationen ausführen, die auf die Funktion abzielen, wie z. B. das Erstellen von Versionen oder das Aktualisieren des Funktionscodes, aber Sie können weiterhin frühere Versionen der Funktion aufrufen.

> **Note**
>
> Wenn eine Lambda-Funktion 30 Tage lang inaktiv bleibt, fordert Lambda alle ungenutzten Hyperplane-ENIs zurück und setzt den Funktionsstatus auf inaktiv. Der nächste Aufrufversuch schlägt fehl, und die Funktion wechselt erneut in den Status Ausstehend, bis Lambda die Erstellung oder Zuweisung einer Hyperplane-ENI abgeschlossen hat. Weitere Hinweise zu den Status von Lambda-Funktionen finden Sie unterthe section called “Funktionszustände”.

Weitere Informationen zu den ENI-Lebenszyklen von Hyperplane finden Sie unter. the section called “Lambda Hyperplane ENIs”

Verwenden von IAM-Bedingungsschlüsseln für VPC-Einstellungen

Sie können Lambda-spezifische Bedingungsschlüssel für VPC-Einstellungen verwenden, um zusätzliche Berechtigungssteuerungen für Ihre Lambda-Funktionen bereitzustellen. Sie können beispielsweise festlegen, dass alle Funktionen in Ihrer Organisation mit einer VPC sein müssen. Sie können auch die Subnetze und Sicherheitsgruppen angeben, die die Benutzer der Funktion verwenden können bzw. nicht verwenden können.

Lambda unterstützt die folgenden IAM-Bedingungsschlüssel:

- lambda: VpcIds — Erlaubt oder verweigert eine oder mehrere VPCs.
- lambda: SubnetIds — Erlaubt oder verweigert ein oder mehrere Subnetze.
- lambda: SecurityGroup Ids — Erlaubt oder verweigert eine oder mehrere Sicherheitsgruppen.

Die Lambda-API-Operationen CreateFunctionund die UpdateFunctionKonfiguration unterstützen diese Bedingungsschlüssel. Weitere Informationen zur Verwendung von Bedingungsschlüsseln in IAM-Richtlinien finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

> **Tip**
>
> Wenn Ihre Funktion bereits eine VPC-Konfiguration aus einer früheren API-Anforderung enthält, können Sie eine `UpdateFunctionConfiguration`-Anforderung ohne die VPC-Konfiguration senden.

Beispielrichtlinien mit Bedingungsschlüsseln für VPC-Einstellungen

In den folgenden Beispielen wird gezeigt, wie Bedingungsschlüssel für VPC-Einstellungen verwendet werden. Nachdem Sie eine Richtlinienanweisung mit den gewünschten Einschränkungen erstellt haben, fügen Sie die Richtlinienanweisung für den -Zielbenutzer oder die Zielrolle an.

Stellen Sie sicher, dass Benutzer nur VPC-verbundene Funktionen bereitstellen

Um sicherzustellen, dass alle Benutzer nur VPC-verbundene Funktionen bereitstellen, können Sie Erstellungs- und Aktualisierungsoperationen von Funktionen verweigern, die keine gültige VPC-ID enthalten.

Beachten Sie, dass die VPC-ID kein Eingabeparameter für die `CreateFunction`- oder `UpdateFunctionConfiguration` -Anforderung ist. Lambda ruft den VPC-ID-Wert basierend auf den Subnetz- und Sicherheitsgruppenparametern ab.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceVPCFunction",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "Null": {
           "lambda:VpcIds": "true"
        }
      }
    }
  ]
}
```

Benutzern den Zugriff auf bestimmte VPCs, Subnetze oder Sicherheitsgruppen verweigern

Um Benutzern den Zugriff auf bestimmte VPCs `StringEquals` zu verweigern, überprüfen Sie den Wert der `lambda:VpcIds`-Bedingung. Im folgenden Beispiel wird Benutzern der Zugriff auf `vpc-1` und `vpc-2` verweigert.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceOutOfVPC",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "lambda:VpcIds": ["vpc-1", "vpc-2"]
        }
      }
    }
```

Um Benutzern den Zugriff auf bestimmte Subnetze zu verweigern, verwenden Sie `StringEquals`, um den Wert der `lambda:SubnetIds` Bedingung zu überprüfen. Im folgenden Beispiel wird Benutzern der Zugriff auf `subnet-1` und `subnet-2` verweigert.

```
{
      "Sid": "EnforceOutOfSubnet",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
            "lambda:SubnetIds": ["subnet-1", "subnet-2"]
        }
      }
    }
```

Um Benutzern den Zugriff auf bestimmte Sicherheitsgruppen zu verweigern, verwenden Sie `StringEquals`, um den Wert der `lambda:SecurityGroupIds`-Bedingung zu überprüfen. Im folgenden Beispiel wird Benutzern der Zugriff auf `sg-1` und `sg-2` verweigert.

```
{
      "Sid": "EnforceOutOfSecurityGroups",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
            "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
        }
      }
    }
  ]
}
```

Benutzern das Erstellen und Aktualisieren von Funktionen mit bestimmten VPC-Einstellungen ermöglichen

Um Benutzern den Zugriff auf bestimmte VPCs zu ermöglichen, verwenden Sie `StringEquals`, um den Wert der `lambda:VpcIds`-Bedingung zu überprüfen. Im folgenden Beispiel können Benutzer auf `vpc-1` und `vpc-2` zugreifen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceStayInSpecificVpc",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "lambda:VpcIds": ["vpc-1", "vpc-2"]
        }
      }
    }
```

Um Benutzern den Zugriff auf bestimmte Subnetze zu ermöglichen, verwenden Sie `StringEquals`, um den Wert der `lambda:SubnetIds`-Bedingung zu überprüfen. Im folgenden Beispiel können Benutzer auf `subnet-1` und `subnet-2` zugreifen.

```
{
      "Sid": "EnforceStayInSpecificSubnets",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
            "lambda:SubnetIds": ["subnet-1", "subnet-2"]
        }
      }
    }
```

Um Benutzern den Zugriff auf bestimmte Sicherheitsgruppen zu ermöglichen, verwenden Sie `StringEquals`, um den Wert der `lambda:SecurityGroupIds`-Bedingung zu überprüfen. Im folgenden Beispiel können Benutzer auf `sg-1` und `sg-2` zugreifen.

```
{
      "Sid": "EnforceStayInSpecificSecurityGroup",
      "Action": [
          "lambda:CreateFunction",
          "lambda:UpdateFunctionConfiguration"
       ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
        "ForAllValues:StringEquals": {
            "lambda:SecurityGroupIds": ["sg-1", "sg-2"]
        }
      }
    }
  ]
}
```

VPC-Tutorials

In den folgenden Tutorials verbinden Sie eine Lambda-Funktion mit Ressourcen in Ihrer VPC.

- Tutorial: Verwenden einer Lambda-Funktion für den Zugriff auf Amazon RDS in einer Amazon VPC
- Tutorial: Konfiguration einer Lambda-Funktion für den Zugriff auf Amazon ElastiCache in einer Amazon VPC

Aktivieren Sie den Internetzugang für mit VPN verbundene Lambda-Funktionen

Standardmäßig werden Lambda-Funktionen in einer von Lambda verwalteten VPC mit Internetzugang ausgeführt. Um auf Ressourcen in einer VPC in Ihrem Konto zuzugreifen, können Sie einer Funktion eine VPC-Konfiguration hinzufügen. Dadurch wird die Funktion auf Ressourcen innerhalb dieser VPC beschränkt, es sei denn, die VPC hat Internetzugang. Auf dieser Seite wird erklärt, wie Sie den Internetzugang für mit VPN verbundene Lambda-Funktionen bereitstellen.

Ich habe noch keine VPC

Erstellen Sie die VPC

Der Workflow Create VPC erstellt alle VPC-Ressourcen, die für eine Lambda-Funktion für den Zugriff auf das öffentliche Internet von einem privaten Subnetz aus erforderlich sind, einschließlich Subnetzen, NAT-Gateways, Internet-Gateways und Routentabelleneinträgen.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard VPC erstellen aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
4. Konfigurieren Sie die VPC
    a. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
    b. Behalten Sie für den IPv4-CIDR-Block entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein.
    c. Wenn die Anwendung über IPv6-Adressen kommuniziert, wählen Sie IPv6-CIDR-Block und Von Amazon bereitgestellter IPv6-CIDR-Block aus.
5. Konfiguration der Subnetze
    a. Wählen Sie für Anzahl der Availability Zones 2 aus. Wir empfehlen mindestens zwei AZs für hohe Verfügbarkeit.
    b. Wählen Sie für Number of public subnets (Anzahl der öffentlichen Subnetze) 2 aus.
    c. Wählen Sie für Number of private subnets (Anzahl der privaten Subnetze) 2 aus.

d. Sie können die standardmäßigen CIDR-Blöcke für die Subnetze beibehalten oder alternativ CIDR-Blöcke des Subnetzes anpassen erweitern und einen CIDR-Block eingeben. Weitere Informationen finden Sie unter Subnetz-CIDR-Blöcke.

6. Wählen Sie für NAT-Gateways 1 pro AZ aus, um die Resilienz zu verbessern.
7. Wählen Sie für ein Internet-Gateway nur für ausgehenden Datenverkehr die Option Ja aus, wenn Sie sich dafür entschieden haben, einen IPv6-CIDR-Block einzubeziehen.
8. Behalten Sie für VPC-Endpoints die Standardeinstellung (S3-Gateway) bei. Für diese Option fallen keine Kosten an. Weitere Informationen finden Sie unter Typen von VPC-Endpunkten für Amazon S3.
9. Behalten Sie für DNS-Optionen die Standardeinstellungen bei.
10. Wählen Sie VPC erstellen aus.

Konfigurieren der Lambda-Funktion

So konfigurieren Sie eine VPC bei der Funktionserstellung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Create function (Funktion erstellen).
3. Geben Sie unter Basic information (Grundlegende Informationen) bei Function name (Funktionsname) einen Namen für Ihre Funktion ein.
4. Erweiterten Sie Advanced settings (Erweiterte Einstellungen).
5. Wählen Sie VPC aktivieren und wählen Sie dann eine VPC aus.
6. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.
7. Wählen Sie für Subnetze alle privaten Subnetze aus. Die privaten Subnetze können über das NAT-Gateway auf das Internet zugreifen. Wenn eine Funktion mit einem öffentlichen Subnetz verbunden wird, erhält sie keinen Internetzugang.

> **Note**
>
> Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

8. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, die ausgehenden Datenverkehr zulässt.
9. Wählen Sie Funktion erstellen.

Lambda erstellt automatisch eine Ausführungsrolle mit der AWSLambdaVPCAccessExecutionRole AWS verwalteten Richtlinie. Die Berechtigungen in dieser Richtlinie sind nur erforderlich, um elastische Netzwerkschnittstellen für die VPC-Konfiguration zu erstellen, nicht aber, um Ihre Funktion aufzurufen. Um Berechtigungen mit den geringsten Rechten anzuwenden, können Sie die AWSLambdaVPCAccessExecutionRoleRichtlinie aus Ihrer Ausführungsrolle entfernen, nachdem Sie die Funktion und die VPC-Konfiguration erstellt haben. Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen.

So konfigurieren Sie eine VPC für eine vorhandene Funktion

Um einer vorhandenen Funktion eine VPC-Konfiguration hinzuzufügen, muss die Ausführungsrolle der Funktion über die Berechtigung verfügen, elastische Netzwerkschnittstellen zu erstellen und zu verwalten. Die AWSLambdaVPCAccessExecutionRole AWS verwaltete Richtlinie umfasst die erforderlichen Berechtigungen. Um Berechtigungen mit den geringsten Rechten anzuwenden, können Sie die AWSLambdaVPCAccessExecutionRoleRichtlinie aus Ihrer Ausführungsrolle entfernen, nachdem Sie die VPC-Konfiguration erstellt haben.

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann VPC aus.
4. Wählen Sie unter VPC die Option Edit (Bearbeiten) aus.
5. Wählen Sie die VPC aus.
6. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.
7. Wählen Sie für Subnetze alle privaten Subnetze aus. Die privaten Subnetze können über das NAT-Gateway auf das Internet zugreifen. Wenn eine Funktion mit einem öffentlichen Subnetz verbunden wird, erhält sie keinen Internetzugang.

> **Note**
>
> Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

8. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, die ausgehenden Datenverkehr zulässt.
9. Wählen Sie Speichern.

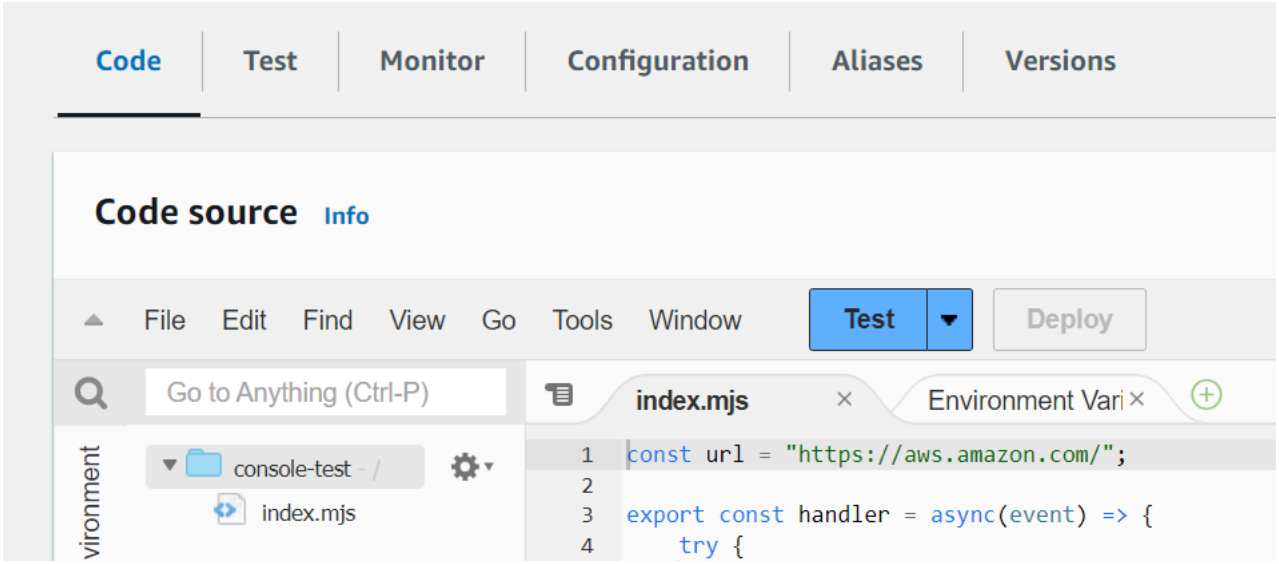
Testen der Funktion

Verwenden Sie den folgenden Beispielcode, um zu bestätigen, dass Ihre VPC-verbundene Funktion das öffentliche Internet erreichen kann. Bei Erfolg gibt der Code einen `200` Statuscode zurück. Wenn dies nicht erfolgreich ist, wird das Zeitlimit für die Funktion überschritten.

Node.js

In diesem Beispiel wird verwendet`fetch`, was in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

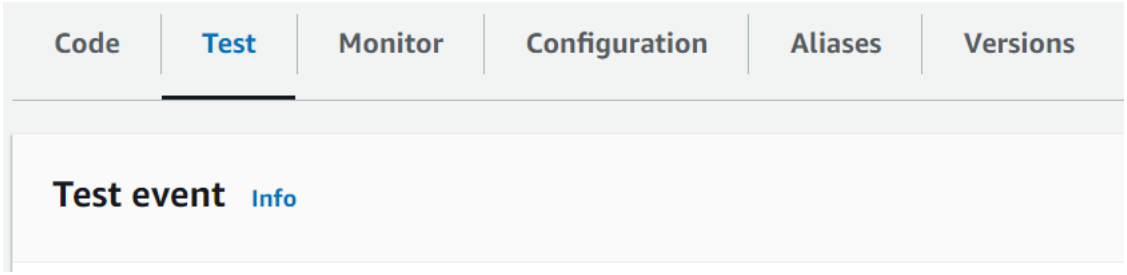
1. Fügen Sie im Bereich Codequelle der Lambda-Konsole den folgenden Code in die Datei index.mjs ein. Die Funktion sendet eine HTTP-GET-Anfrage an einen öffentlichen Endpunkt und gibt den HTTP-Antwortcode zurück, um zu testen, ob die Funktion Zugriff auf das öffentliche Internet hat.



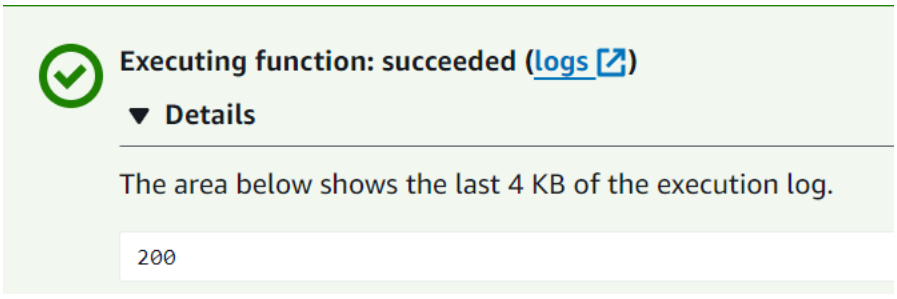
Example — HTTP-Anfrage mit async/await

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        // fetch is available with Node.js 18 and later runtimes
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

2. Wählen Sie Bereitstellen.
3. Wählen Sie die Registerkarte Test.



4. Wählen Sie Test aus.
5. Die Funktion gibt einen `200` Statuscode zurück. Das bedeutet, dass die Funktion über einen ausgehenden Internetzugang verfügt.

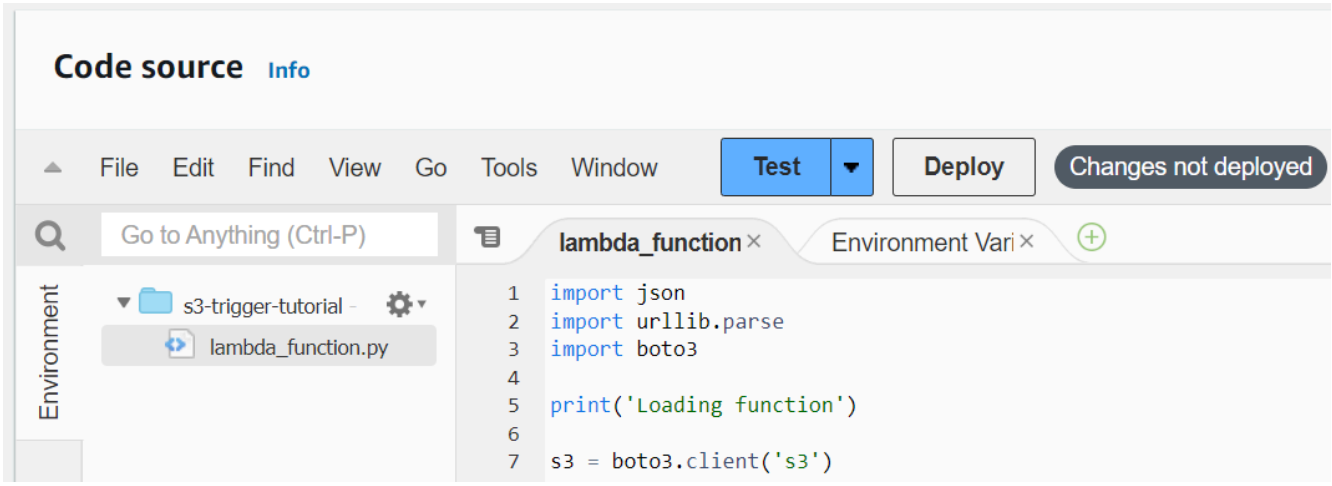


Wenn die Funktion das öffentliche Internet nicht erreichen kann, erhalten Sie eine Fehlermeldung wie diese:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

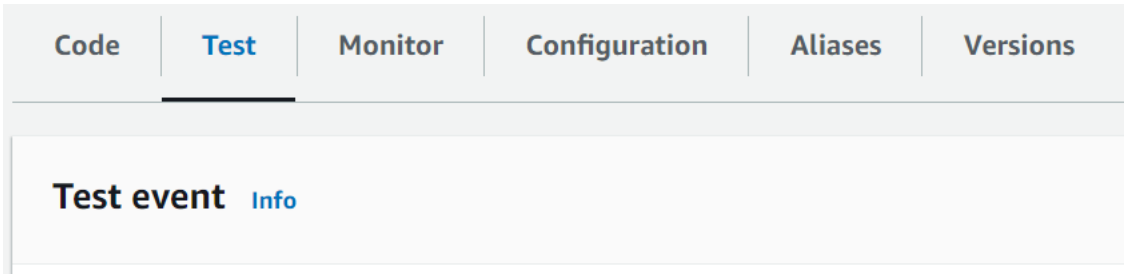
Python

1. Fügen Sie im Bereich Codequelle der Lambda-Konsole den folgenden Code in die Datei lambda_function.py ein. Die Funktion sendet eine HTTP-GET-Anfrage an einen öffentlichen Endpunkt und gibt den HTTP-Antwortcode zurück, um zu testen, ob die Funktion Zugriff auf das öffentliche Internet hat.

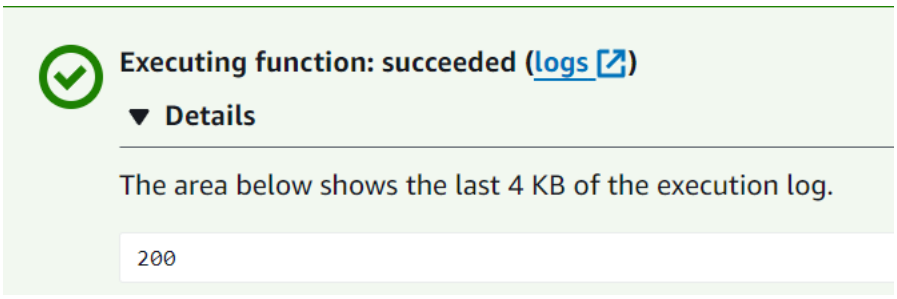



```
import urllib.request

def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e
```

2. Wählen Sie Bereitstellen.
3. Wählen Sie die Registerkarte Test.



4. Wählen Sie Test aus.
5. Die Funktion gibt einen `200` Statuscode zurück. Das bedeutet, dass die Funktion über einen ausgehenden Internetzugang verfügt.



Wenn die Funktion das öffentliche Internet nicht erreichen kann, erhalten Sie eine Fehlermeldung wie diese:

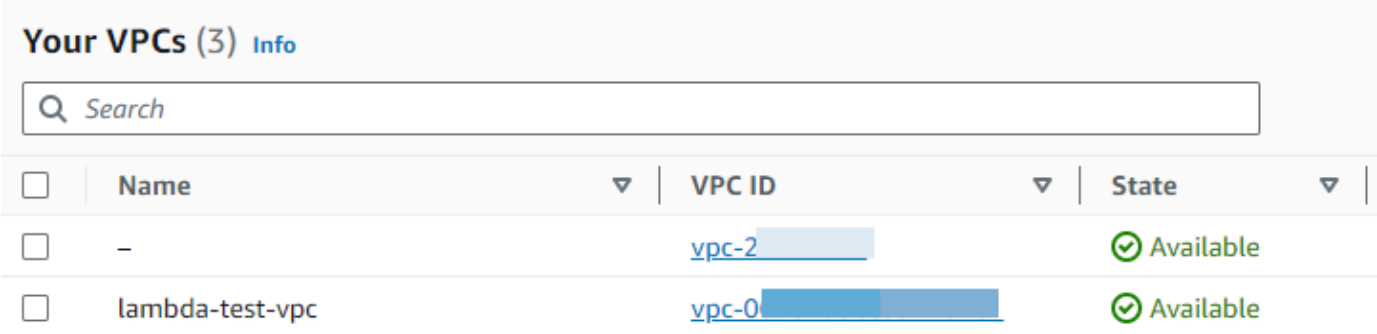
```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

Ich habe bereits eine VPC

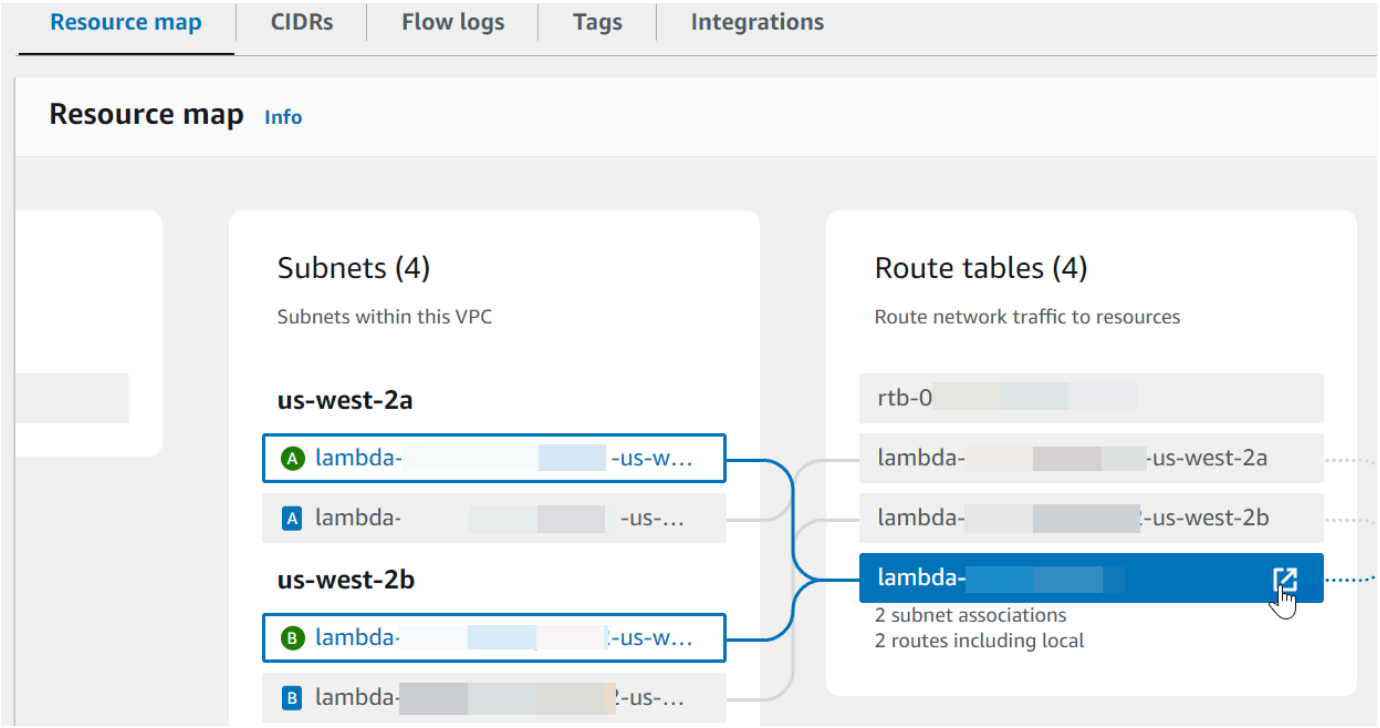
Wenn Sie bereits über eine VPC verfügen, aber den öffentlichen Internetzugang für eine Lambda-Funktion konfigurieren müssen, gehen Sie wie folgt vor. Bei diesem Verfahren wird davon ausgegangen, dass Ihre VPC über mindestens zwei Subnetze verfügt. Wenn Sie nicht über zwei Subnetze verfügen, finden Sie weitere Informationen unter Erstellen eines Subnetzes im Amazon VPC-Benutzerhandbuch.

Überprüfen Sie die Konfiguration der Routing-Tabelle

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie die VPC-ID.



3. Scrollen Sie nach unten zum Abschnitt Ressourcenübersicht. Beachten Sie die Zuordnungen der Routentabellen. Öffnen Sie jede Routing-Tabelle, die einem Subnetz zugeordnet ist.

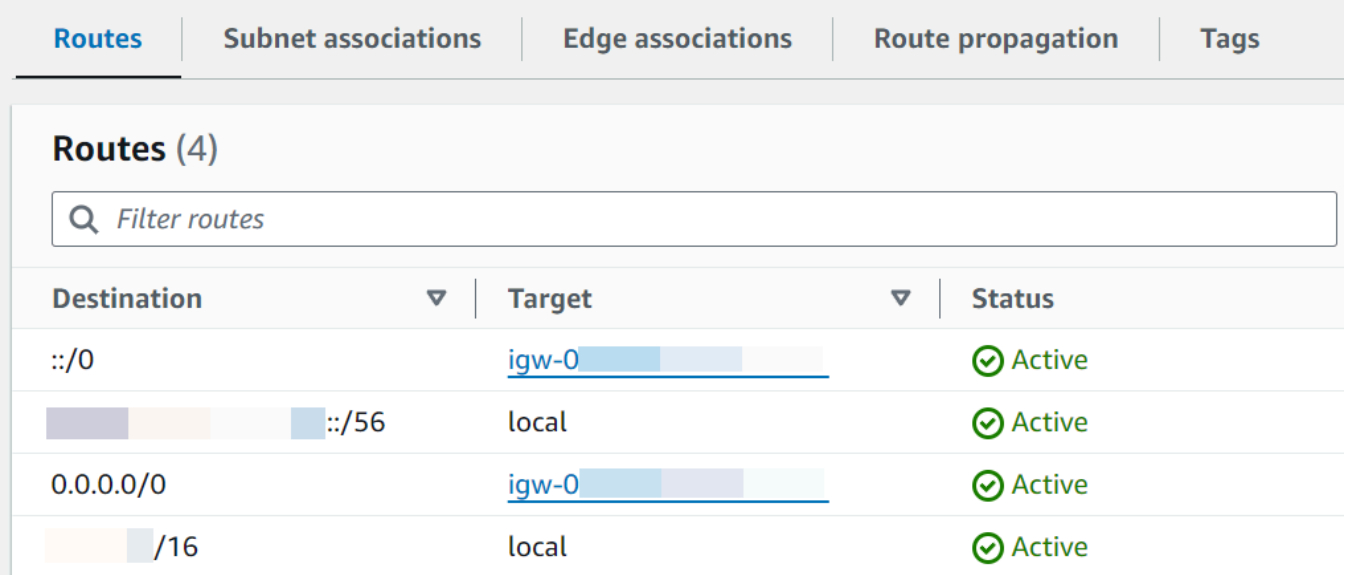


4. Scrollen Sie nach unten zur Registerkarte Routen. Überprüfen Sie die Routen, um festzustellen, ob eine der folgenden Bedingungen zutrifft. Jede dieser Anforderungen muss durch eine separate Routentabelle erfüllt werden.

   - Internetdatenverkehr (`0.0.0.0/0`für IPv4, `::/0` für IPv6) wird an ein Internet-Gateway () weitergeleitet. `igw-xxxxxxxxxx` Das bedeutet, dass das der Routing-Tabelle zugeordnete Subnetz ein öffentliches Subnetz ist.

> **Note**
>
> Wenn Ihr Subnetz keinen IPv6-CIDR-Block hat, wird Ihnen nur die IPv4-Route () angezeigt. `0.0.0.0/0`

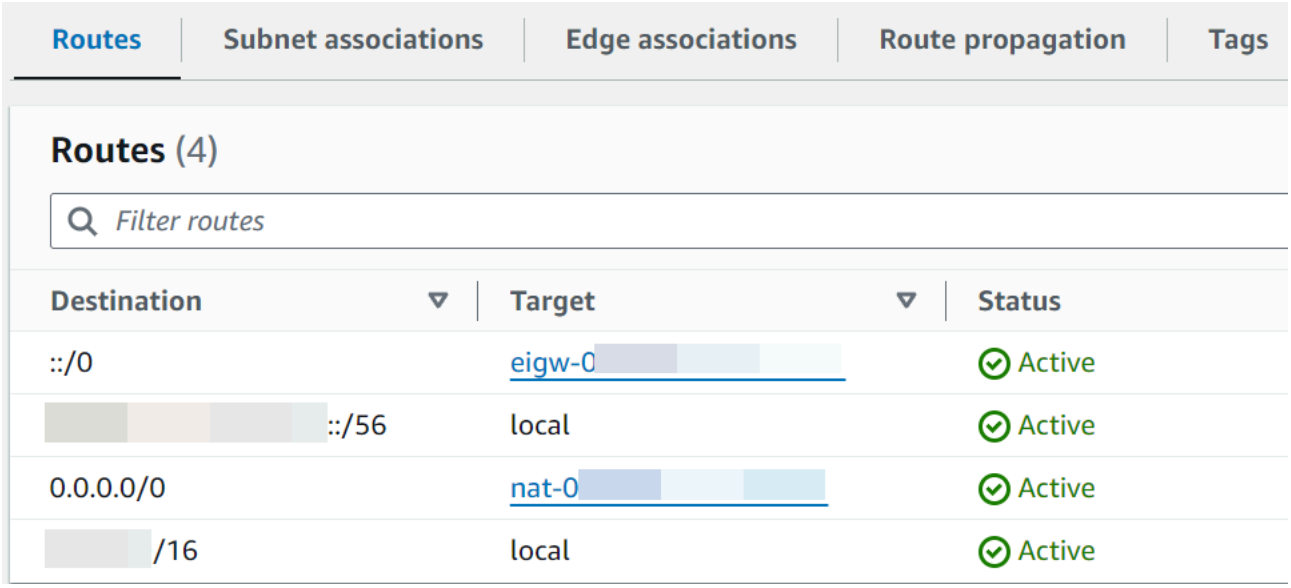
Example öffentliche Subnetz-Routentabelle



- Internetgebundener Datenverkehr für IPv4 (`0.0.0.0/0`) wird an ein NAT-Gateway (`nat-xxxxxxxxxx`) weitergeleitet, das einem öffentlichen Subnetz zugeordnet ist. Das bedeutet, dass das Subnetz ein privates Subnetz ist, das über das NAT-Gateway auf das Internet zugreifen kann.

> **Note**
>
> Wenn Ihr Subnetz über einen IPv6-CIDR-Block verfügt, muss die Routing-Tabelle auch internetgebundenen IPv6-Verkehr () an ein Internet-Gateway (`::/0`) weiterleiten, das nur für ausgehenden Datenverkehr bestimmt ist. `eigw-xxxxxxxxxx` Wenn Ihr Subnetz keinen IPv6-CIDR-Block hat, wird Ihnen nur die IPv4-Route () angezeigt. `0.0.0.0/0`

Example private Subnetz-Routentabelle



5. Wiederholen Sie den vorherigen Schritt, bis Sie alle Routing-Tabellen überprüft haben, die einem Subnetz in Ihrer VPC zugeordnet sind, und bestätigt haben, dass Sie über eine Routentabelle mit einem Internet-Gateway und eine Routing-Tabelle mit einem NAT-Gateway verfügen.

   Wenn Sie nicht über zwei Routing-Tabellen verfügen, eine mit einer Route zu einem Internet-Gateway und eine mit einer Route zu einem NAT-Gateway, gehen Sie wie folgt vor, um die fehlenden Ressourcen und Routing-Tabelleneinträge zu erstellen.

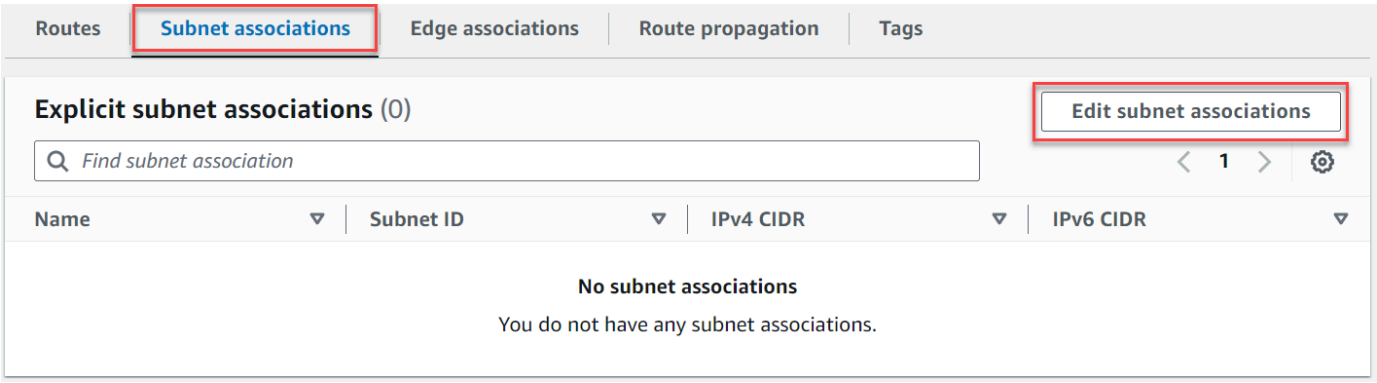
Erstellen einer Routing-Tabelle

Gehen Sie wie folgt vor, um eine Routing-Tabelle zu erstellen und sie einem Subnetz zuzuordnen.

Um eine benutzerdefinierte Routing-Tabelle mit der Amazon VPC-Konsole zu erstellen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
4. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle ein.
5. Wählen Sie unter VPC Ihre VPC aus.
6. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.

7. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
8. Wählen Sie auf der Registerkarte Subnet associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus.



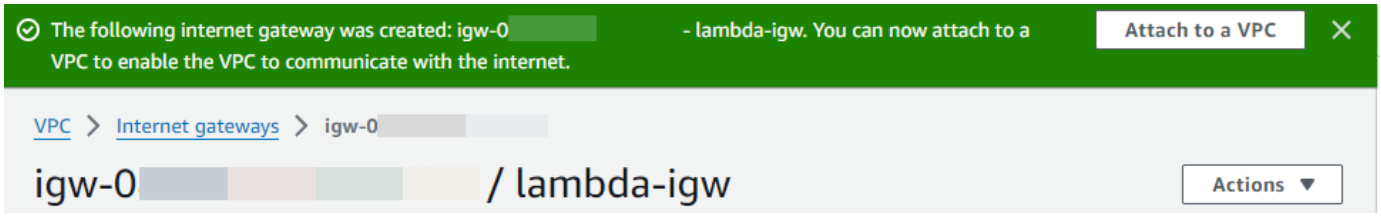
9. Aktivieren Sie das Kontrollkästchen für das Subnetz, um es der Routing-Tabelle zuzuordnen.
10. Klicken Sie auf Save associations (Zuordnungen speichern).

Ein Internet-Gateway erstellen

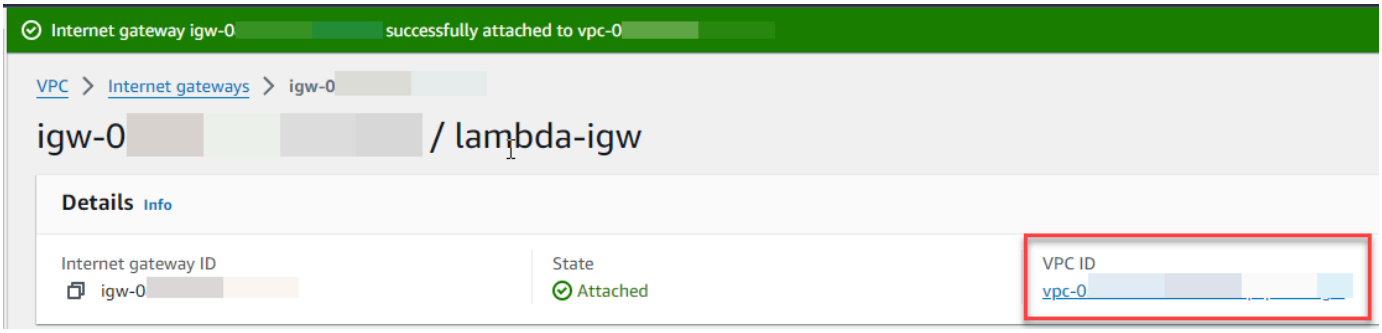
Gehen Sie wie folgt vor, um ein Internet-Gateway zu erstellen, es an Ihre VPC anzuhängen und es der Routing-Tabelle Ihres öffentlichen Subnetzes hinzuzufügen.

So erstellen Sie ein Internet-Gateway

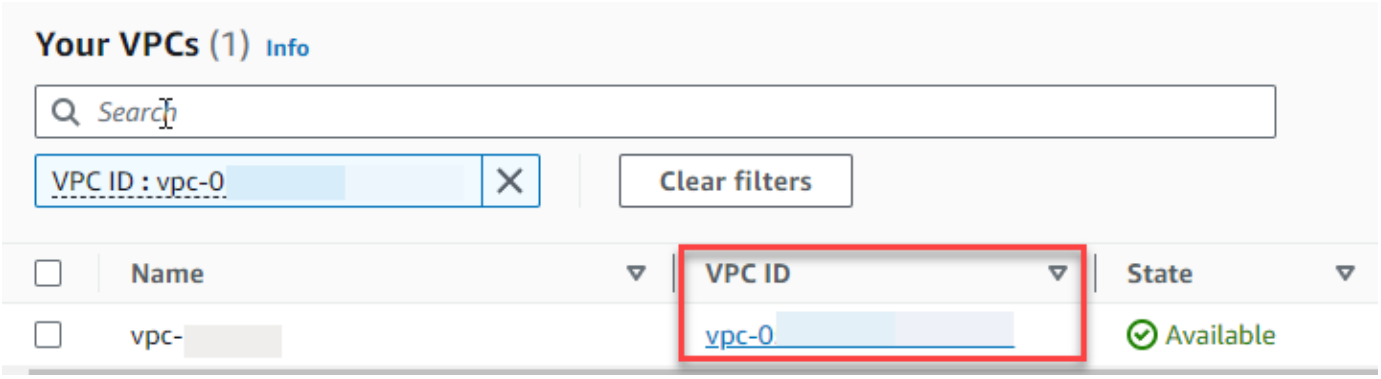
1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet Gateways (Internet-Gateways) aus.
3. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
4. (Optional) Geben Sie einen Namen für Ihr Internet-Gateway ein.
5. (Optional) Um ein Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen) aus und geben Sie den Schlüssel und den Wert für den Tag ein.
6. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
7. Wählen Sie im Banner oben auf dem Bildschirm die Option An eine VPC anhängen, wählen Sie eine verfügbare VPC aus und wählen Sie dann Internet-Gateway anhängen aus.



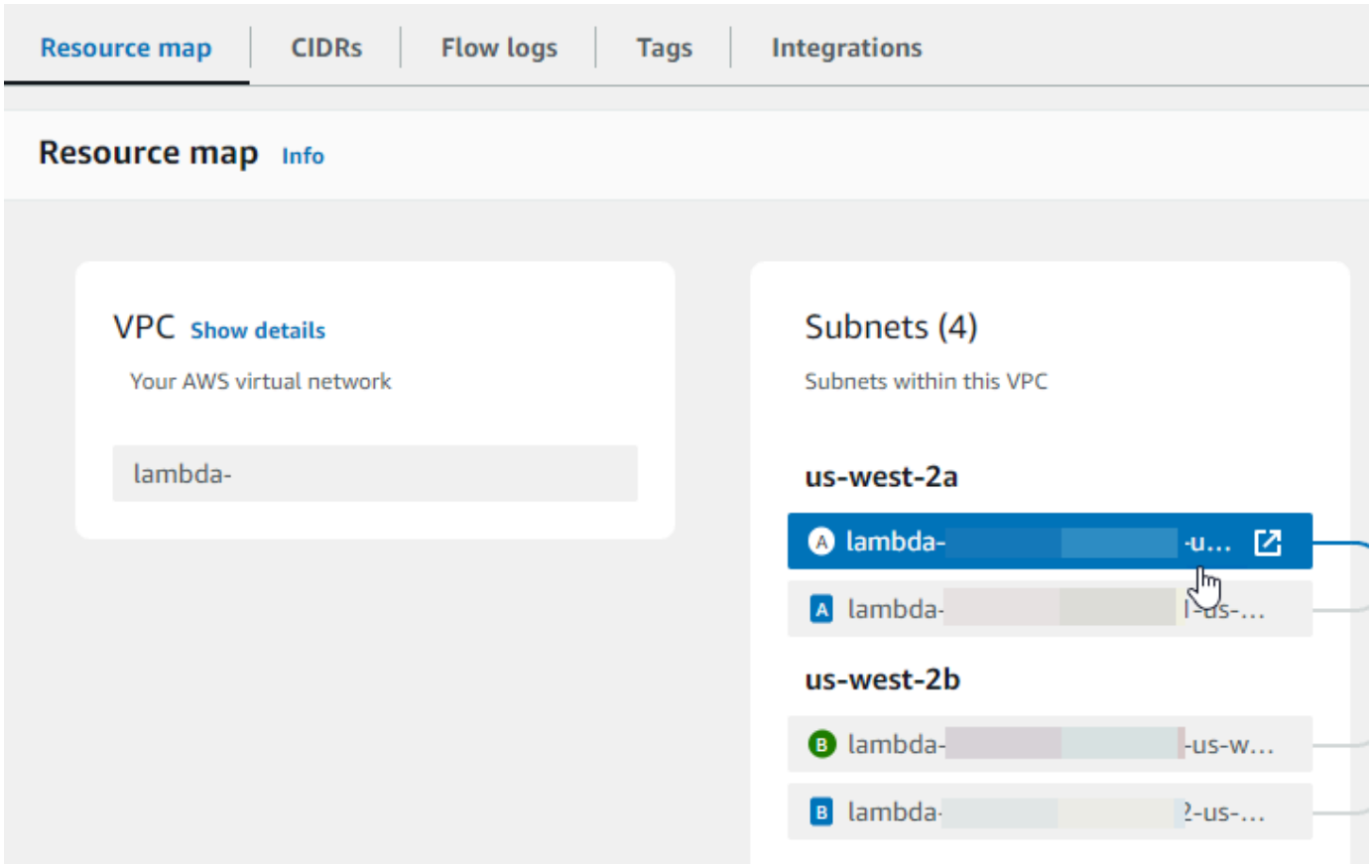
8. Wählen Sie die VPC-ID.



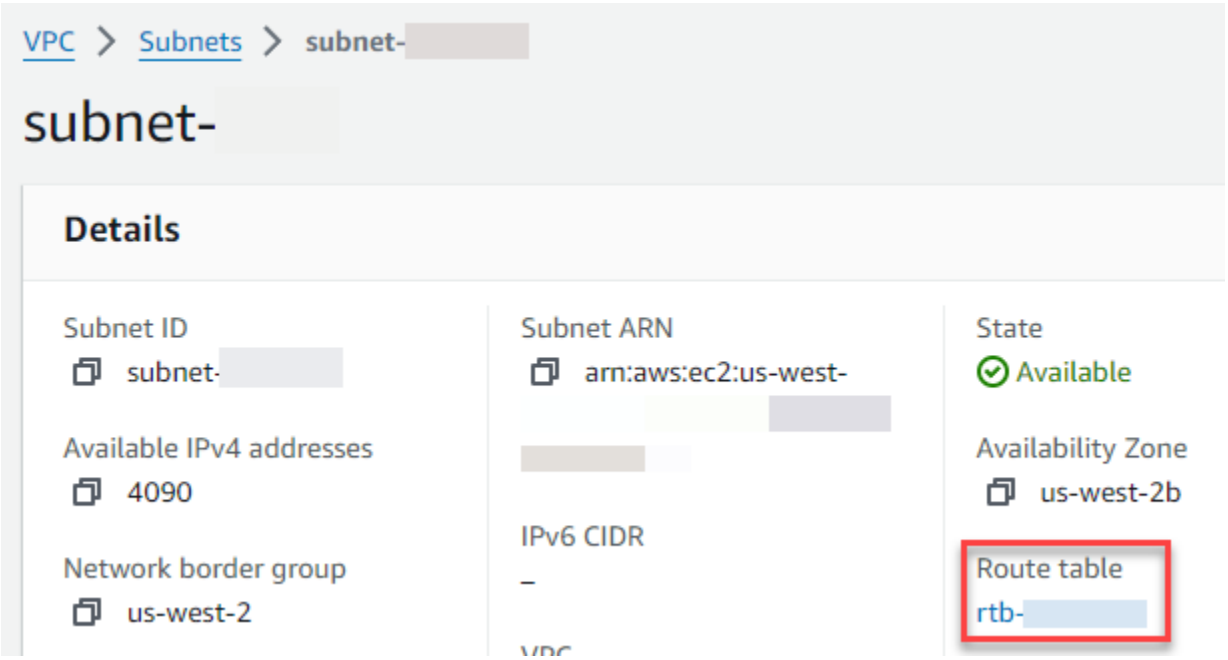
9. Wählen Sie erneut die VPC-ID aus, um die VPC-Detailseite zu öffnen.



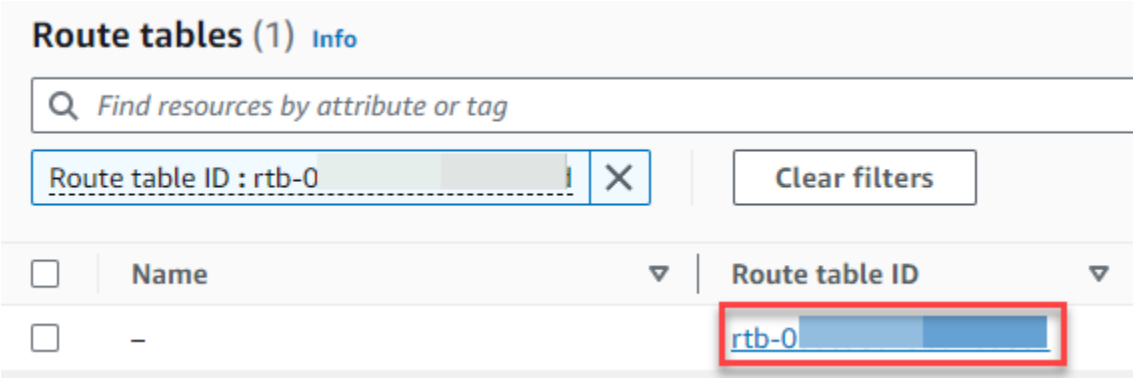
10. Scrollen Sie nach unten zum Abschnitt Ressourcenübersicht und wählen Sie dann ein Subnetz aus. Die Subnetzdetails werden auf einer neuen Registerkarte angezeigt.



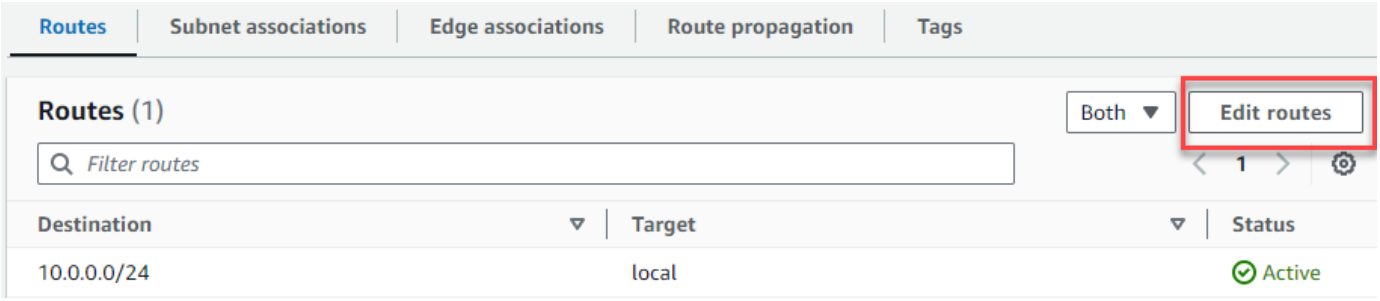
11. Wählen Sie den Link unter Routentabelle aus.



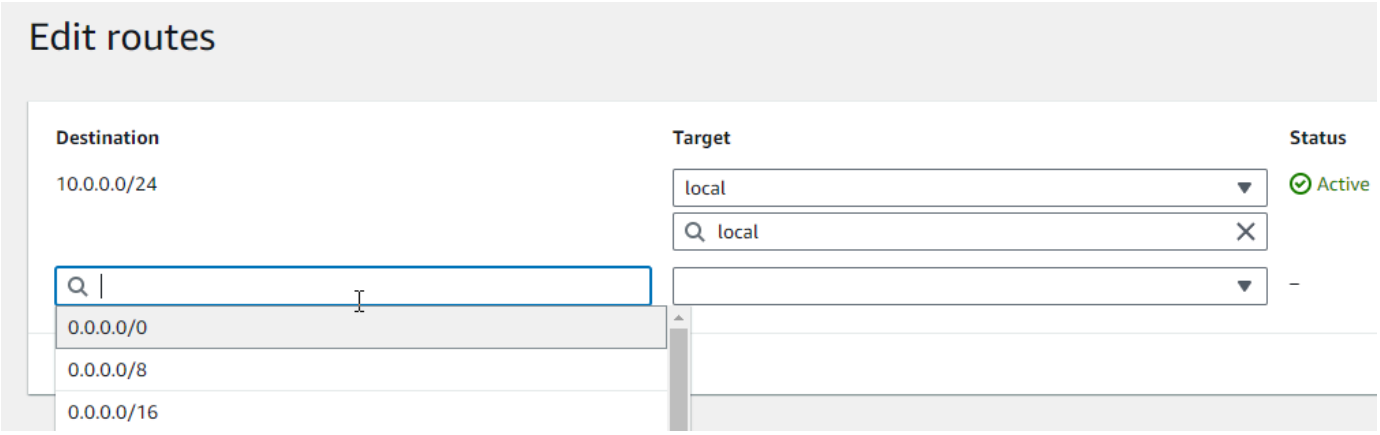
12. Wählen Sie die Routentabellen-ID, um die Detailseite der Routentabelle zu öffnen.



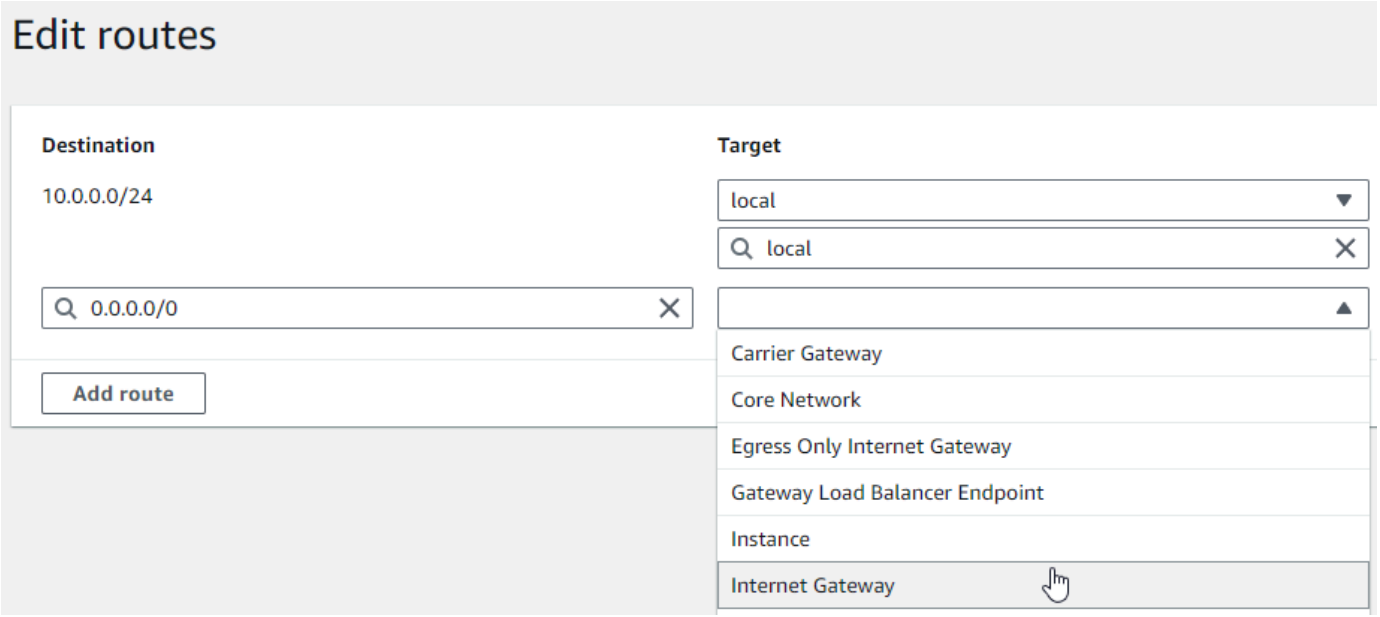
13. Wählen Sie unter Routen die Option Routen bearbeiten aus.



14. Wählen Sie Route hinzufügen und geben Sie sie dann `0.0.0.0/0` in das Feld Ziel ein.



15. Wählen Sie für Target Internet-Gateway und dann das Internet-Gateway aus, das Sie zuvor erstellt haben. Wenn Ihr Subnetz über einen IPv6-CIDR-Block verfügt, müssen Sie auch eine Route für dasselbe `::/0` Internet-Gateway hinzufügen.



16. Wählen Sie Änderungen speichern aus.

Erstellen eines NAT-Gateways

Gehen Sie wie folgt vor, um ein NAT-Gateway zu erstellen, es einem öffentlichen Subnetz zuzuordnen und es dann der Routing-Tabelle Ihres privaten Subnetzes hinzuzufügen.

Um ein NAT-Gateway zu erstellen und es einem öffentlichen Subnetz zuzuordnen

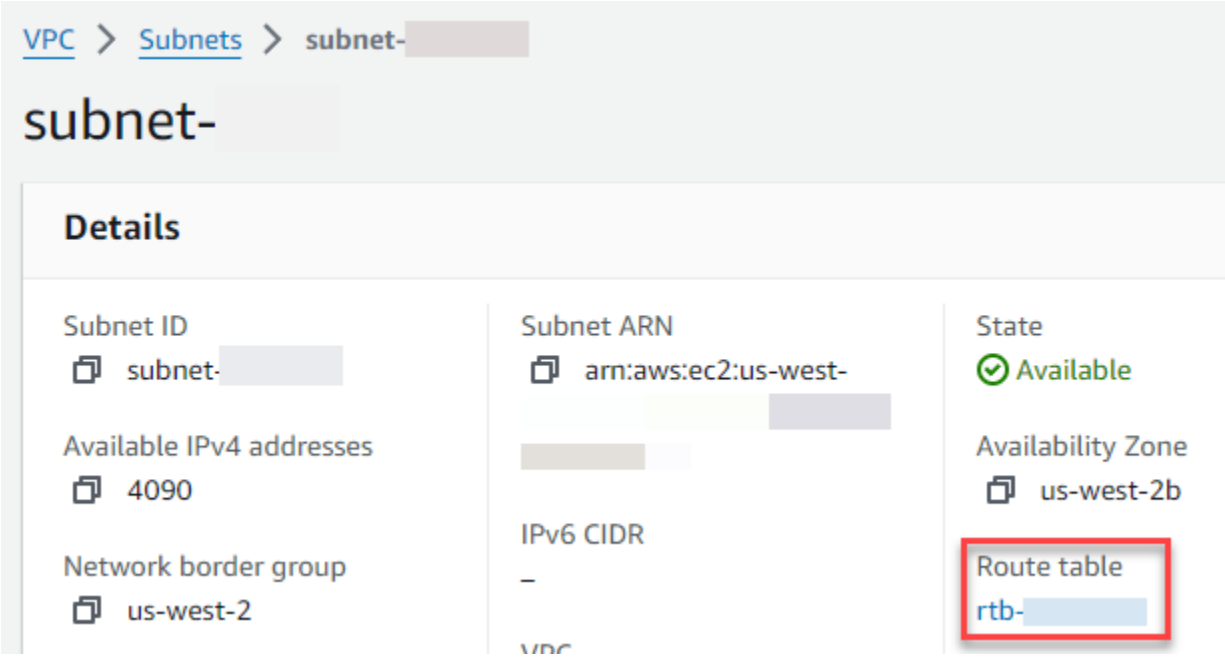
1. Klicken Sie im Navigationsbereich auf NAT-Gateways.
2. Wählen Sie NAT-Gateway erstellen aus.
3. (Optional) Geben Sie einen Namen für Ihr NAT-Gateway ein.
4. Wählen Sie für Subnetz ein öffentliches Subnetz in Ihrer VPC aus. (Ein öffentliches Subnetz ist ein Subnetz, dessen Routing-Tabelle eine direkte Route zu einem Internet-Gateway enthält.)

> **Note**
>
> NAT-Gateways sind einem öffentlichen Subnetz zugeordnet, aber der Routing-Tabelleneintrag befindet sich im privaten Subnetz.

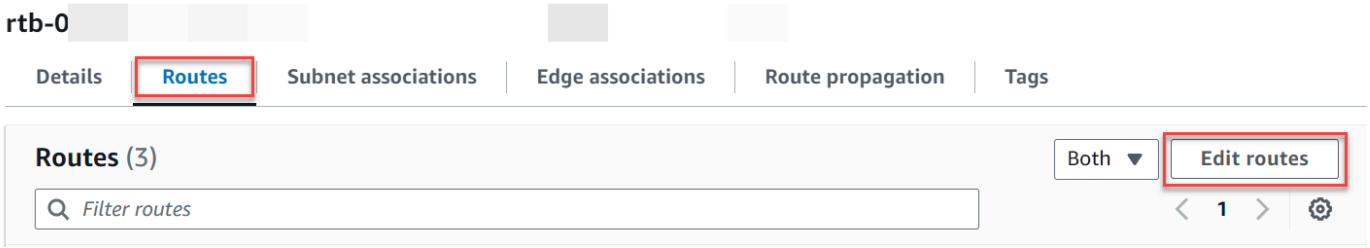
5. Wählen Sie als Elastic IP Allocation ID eine Elastic IP Address oder Allocate Elastic IP aus.
6. Wählen Sie NAT-Gateway erstellen aus.

Um eine Route zum NAT-Gateway in der Routing-Tabelle des privaten Subnetzes hinzuzufügen

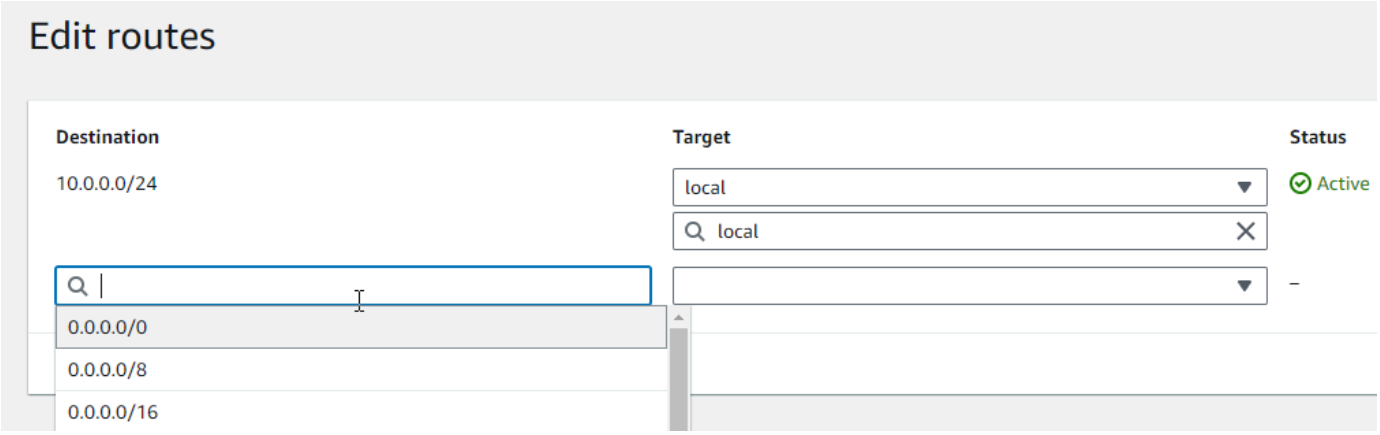
1. Wählen Sie im Navigationsbereich Subnetze aus.
2. Wählen Sie ein privates Subnetz in Ihrer VPC aus. (Ein privates Subnetz ist ein Subnetz, dessen Routing-Tabelle keine Route zu einem Internet-Gateway enthält.)
3. Wählen Sie den Link unter Routentabelle aus.



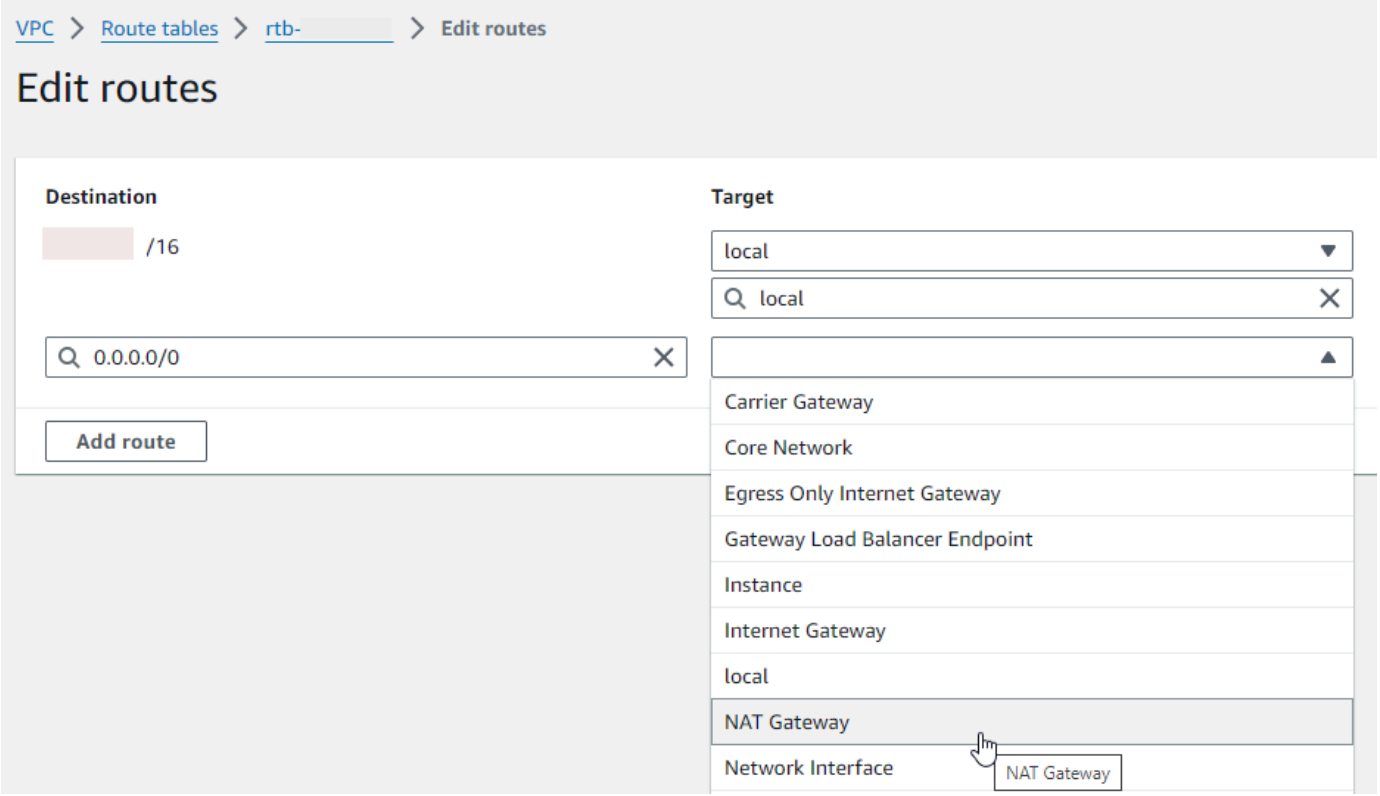
4. Scrollen Sie nach unten und wählen Sie die Registerkarte Routen und anschließend Routen bearbeiten



5. Wählen Sie Route hinzufügen und geben Sie sie dann `0.0.0.0/0` in das Feld Ziel ein.



6. Wählen Sie für Target NAT-Gateway und dann das NAT-Gateway aus, das Sie zuvor erstellt haben.



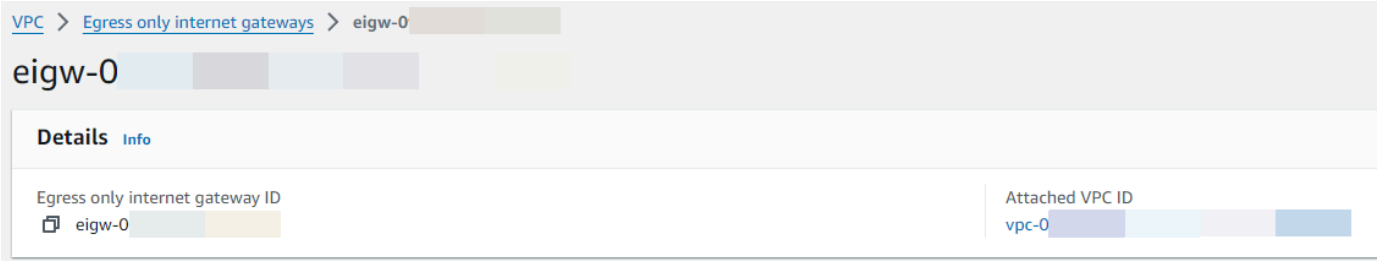
7. Wählen Sie Änderungen speichern aus.

Erstellen Sie ein Internet-Gateway nur für ausgehenden Datenverkehr (nur IPv6)

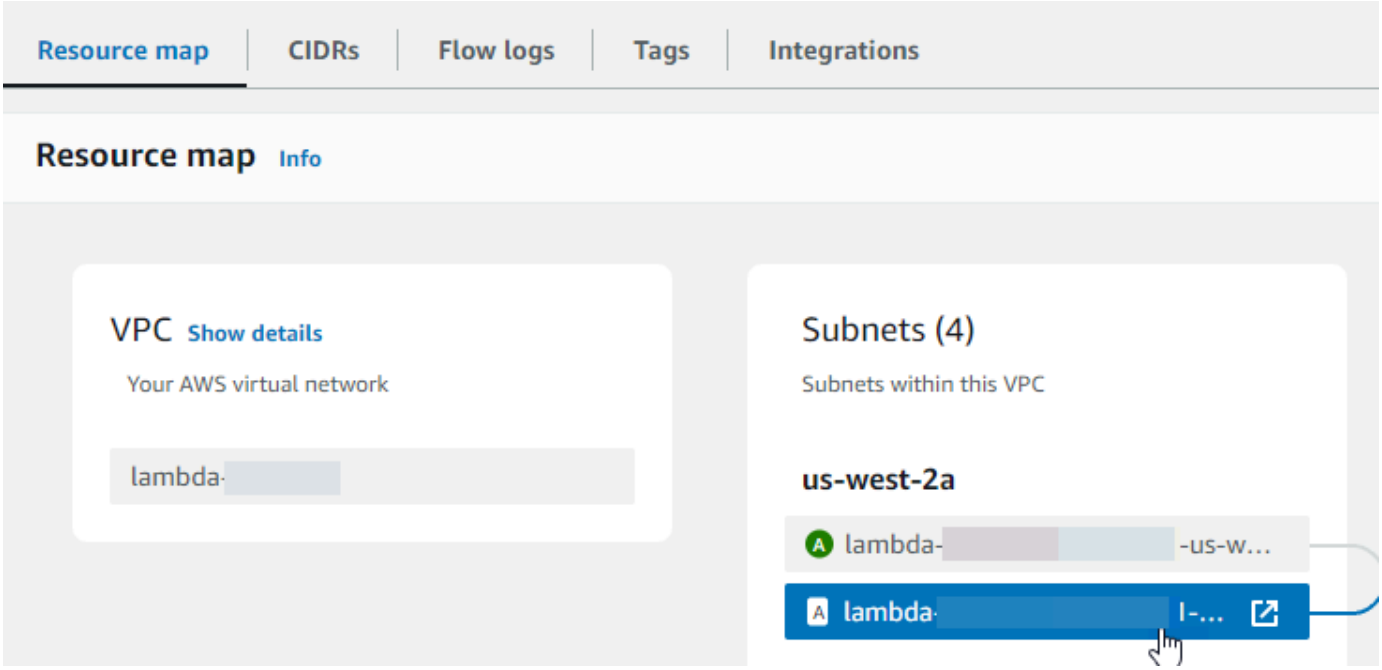
Gehen Sie wie folgt vor, um ein Internet-Gateway nur für ausgehenden Datenverkehr zu erstellen und es der Routing-Tabelle Ihres privaten Subnetzes hinzuzufügen.

So erstellen Sie ein Internet-Gateway nur für ausgehenden Verkehr

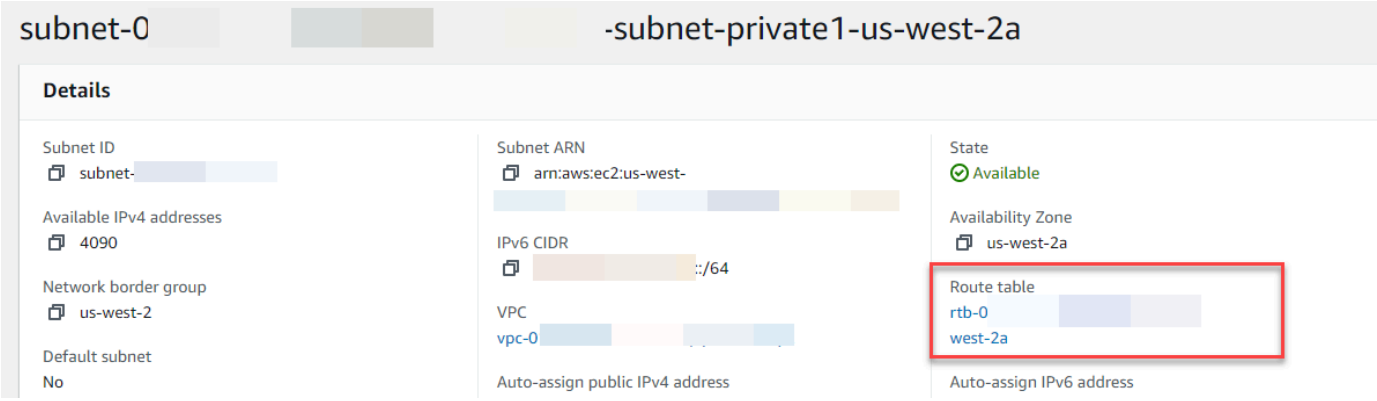
1. Wählen Sie im Navigationsbereich Internet-Gateways für ausgehenden Datenverkehr.
2. Klicken Sie auf Internet-Gateway für ausgehenden Datenverkehr erstellen.
3. (Optional) Geben Sie einen Namen ein.
4. Wählen Sie die VPC aus, in der Sie das Internet-Gateway für ausgehenden Verkehr erstellen möchten.
5. Klicken Sie auf Internet-Gateway für ausgehenden Datenverkehr erstellen.
6. Wählen Sie den Link unter Angehängte VPC-ID aus.



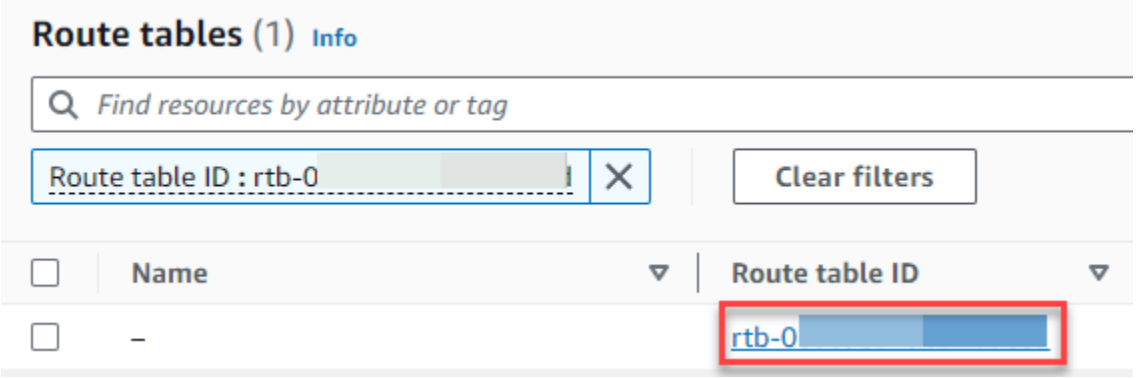
7. Wählen Sie den Link unter VPC-ID, um die VPC-Detailseite zu öffnen.
8. Scrollen Sie nach unten zum Abschnitt Ressourcenübersicht und wählen Sie dann ein privates Subnetz aus. Die Subnetzdetails werden auf einer neuen Registerkarte angezeigt.



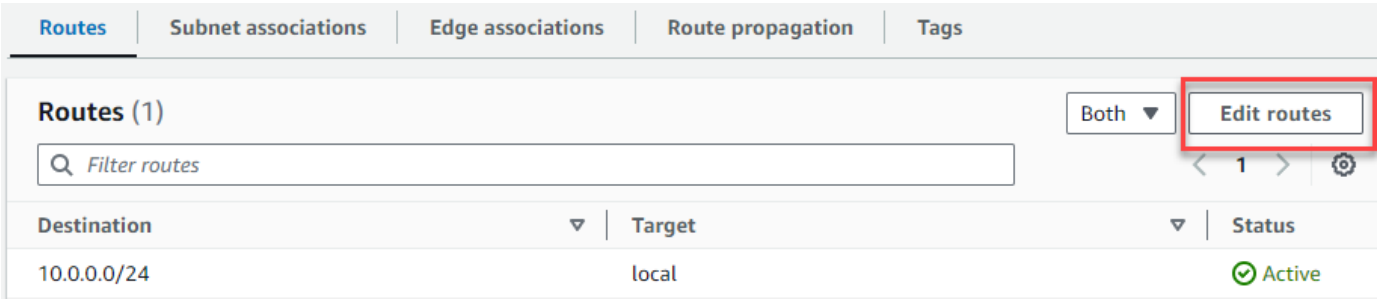
9. Wählen Sie den Link unter Routentabelle aus.



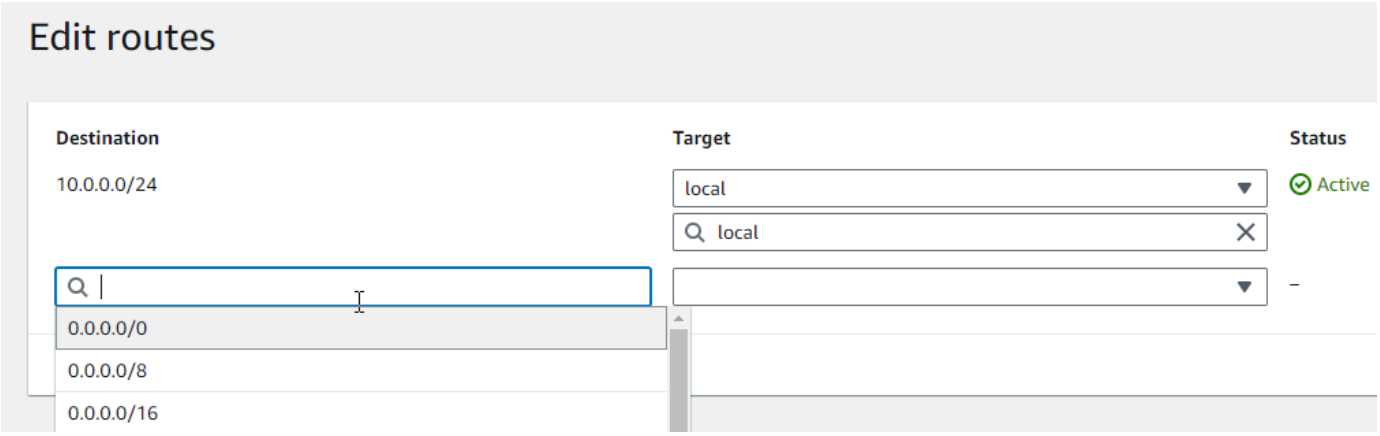
10. Wählen Sie die Routentabellen-ID, um die Detailseite der Routentabelle zu öffnen.



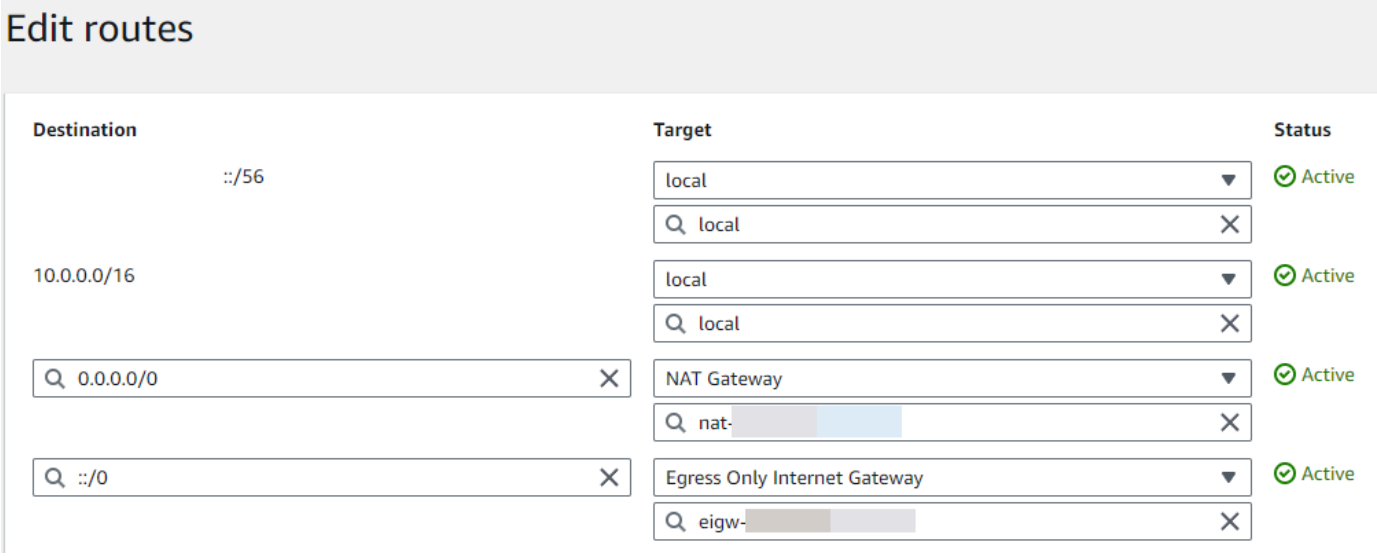
11. Wählen Sie unter Routen die Option Routen bearbeiten aus.



12. Wählen Sie Route hinzufügen und geben Sie sie dann `::/0` in das Feld Ziel ein.



13. Wählen Sie für Target die Option Internet Gateway Only Egress Only und dann das Gateway aus, das Sie zuvor erstellt haben.



14. Wählen Sie Änderungen speichern aus.

Konfigurieren der Lambda-Funktion

So konfigurieren Sie eine VPC bei der Funktionserstellung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Create function (Funktion erstellen).
3. Geben Sie unter Basic information (Grundlegende Informationen) bei Function name (Funktionsname) einen Namen für Ihre Funktion ein.
4. Erweiterten Sie Advanced settings (Erweiterte Einstellungen).
5. Wählen Sie VPC aktivieren und wählen Sie dann eine VPC aus.
6. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.
7. Wählen Sie für Subnetze alle privaten Subnetze aus. Die privaten Subnetze können über das NAT-Gateway auf das Internet zugreifen. Wenn eine Funktion mit einem öffentlichen Subnetz verbunden wird, erhält sie keinen Internetzugang.

> **Note**
>
> Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

8. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, die ausgehenden Datenverkehr zulässt.
9. Wählen Sie Funktion erstellen.

Lambda erstellt automatisch eine Ausführungsrolle mit der AWSLambdaVPCAccessExecutionRole AWS verwalteten Richtlinie. Die Berechtigungen in dieser Richtlinie sind nur erforderlich, um elastische Netzwerkschnittstellen für die VPC-Konfiguration zu erstellen, nicht aber, um Ihre Funktion aufzurufen. Um Berechtigungen mit den geringsten Rechten anzuwenden, können Sie die AWSLambdaVPCAccessExecutionRoleRichtlinie aus Ihrer Ausführungsrolle entfernen, nachdem Sie die Funktion und die VPC-Konfiguration erstellt haben. Weitere Informationen finden Sie unter Erforderliche IAM-Berechtigungen.

So konfigurieren Sie eine VPC für eine vorhandene Funktion

Um einer vorhandenen Funktion eine VPC-Konfiguration hinzuzufügen, muss die Ausführungsrolle der Funktion über die Berechtigung verfügen, elastische Netzwerkschnittstellen zu erstellen und zu verwalten. Die AWSLambdaVPCAccessExecutionRole AWS verwaltete Richtlinie umfasst die erforderlichen Berechtigungen. Um Berechtigungen mit den geringsten Rechten anzuwenden, können Sie die AWSLambdaVPCAccessExecutionRoleRichtlinie aus Ihrer Ausführungsrolle entfernen, nachdem Sie die VPC-Konfiguration erstellt haben.

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann VPC aus.
4. Wählen Sie unter VPC die Option Edit (Bearbeiten) aus.
5. Wählen Sie die VPC aus.
6. (Optional) Um ausgehenden IPv6-Verkehr zuzulassen, wählen Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) aus.

7. Wählen Sie für Subnetze alle privaten Subnetze aus. Die privaten Subnetze können über das NAT-Gateway auf das Internet zugreifen. Wenn eine Funktion mit einem öffentlichen Subnetz verbunden wird, erhält sie keinen Internetzugang.

   > **Note**
   >
   > Wenn Sie Allow IPv6 traffic for dual-stack subnets (IPv6-Verkehr für Dual-Stack-Subnetze zulassen) ausgewählt haben, müssen alle ausgewählten Subnetze einen IPv4-CIDR-Block und einen IPv6-CIDR-Block besitzen.

8. Wählen Sie unter Sicherheitsgruppen eine Sicherheitsgruppe aus, die ausgehenden Datenverkehr zulässt.
9. Wählen Sie Speichern.

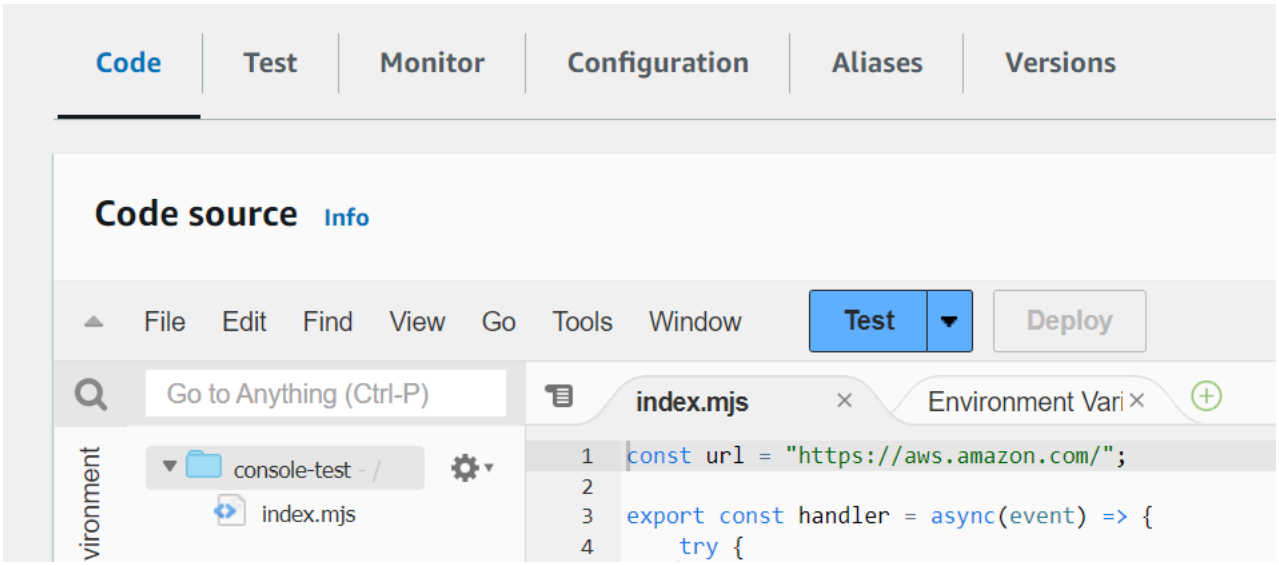
Testen der Funktion

Verwenden Sie den folgenden Beispielcode, um zu bestätigen, dass Ihre VPC-verbundene Funktion das öffentliche Internet erreichen kann. Bei Erfolg gibt der Code einen `200` Statuscode zurück. Wenn dies nicht erfolgreich ist, wird das Zeitlimit für die Funktion überschritten.

Node.js

In diesem Beispiel wird verwendet`fetch`, was in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

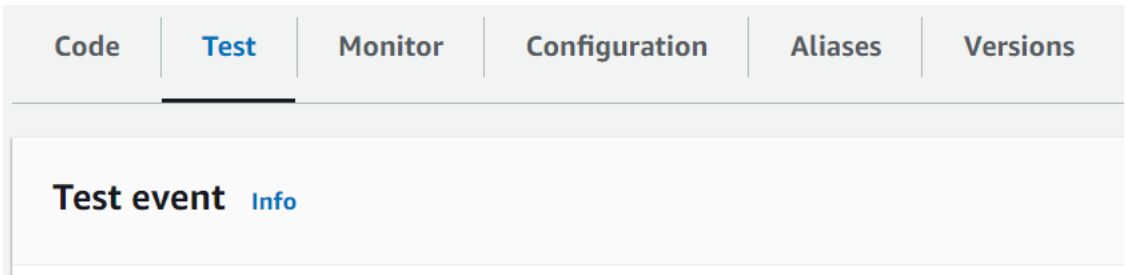
1. Fügen Sie im Bereich Codequelle der Lambda-Konsole den folgenden Code in die Datei index.mjs ein. Die Funktion sendet eine HTTP-GET-Anfrage an einen öffentlichen Endpunkt und gibt den HTTP-Antwortcode zurück, um zu testen, ob die Funktion Zugriff auf das öffentliche Internet hat.



Example — HTTP-Anfrage mit async/await

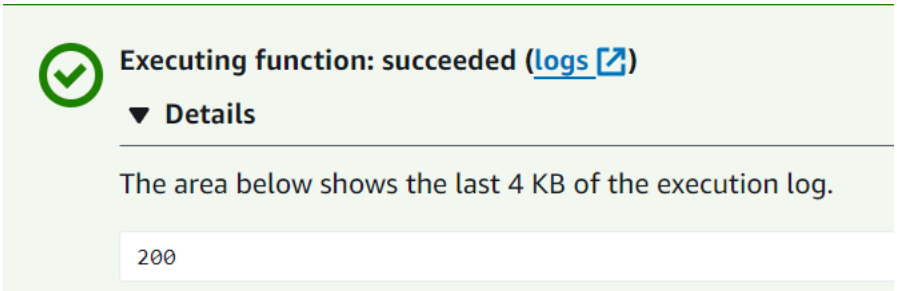
```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        // fetch is available with Node.js 18 and later runtimes
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

2. Wählen Sie Bereitstellen.
3. Wählen Sie die Registerkarte Test.



4. Wählen Sie Test aus.

5. Die Funktion gibt einen `200` Statuscode zurück. Das bedeutet, dass die Funktion über einen ausgehenden Internetzugang verfügt.

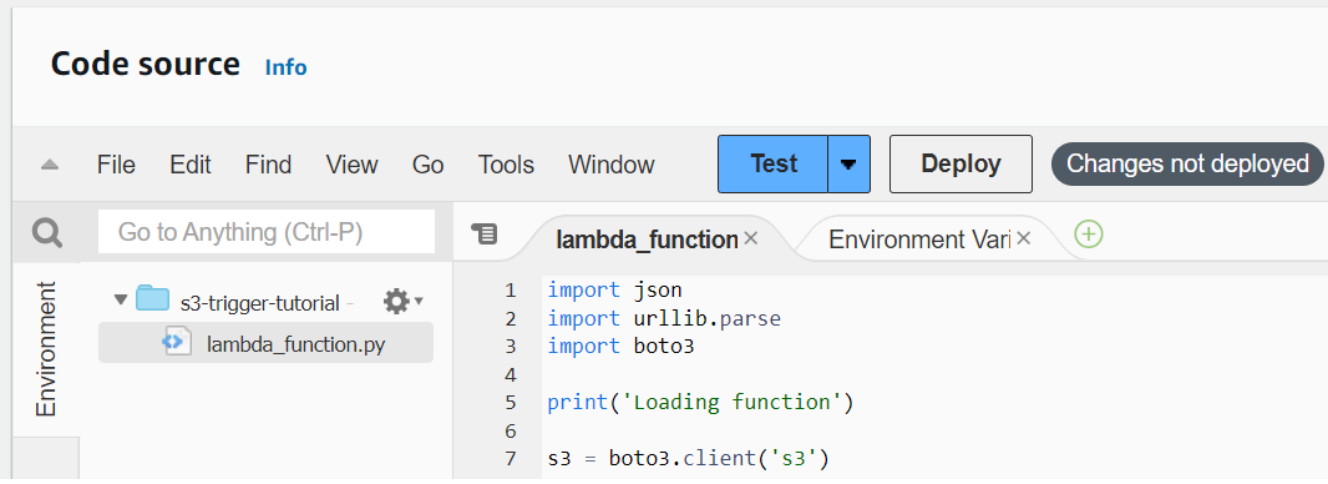


Wenn die Funktion das öffentliche Internet nicht erreichen kann, erhalten Sie eine Fehlermeldung wie diese:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

Python

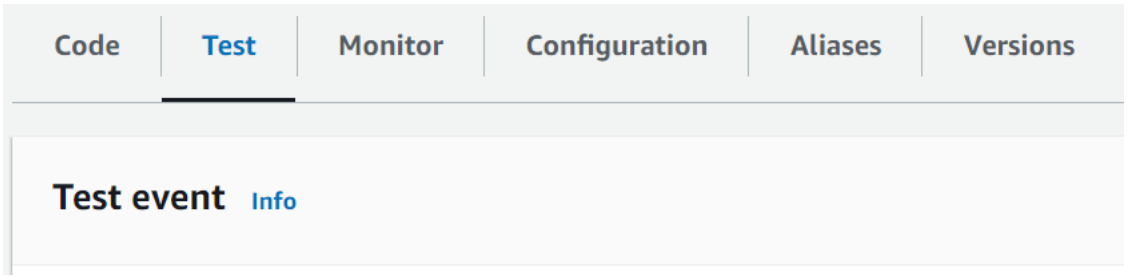
1. Fügen Sie im Bereich Codequelle der Lambda-Konsole den folgenden Code in die Datei lambda_function.py ein. Die Funktion sendet eine HTTP-GET-Anfrage an einen öffentlichen Endpunkt und gibt den HTTP-Antwortcode zurück, um zu testen, ob die Funktion Zugriff auf das öffentliche Internet hat.



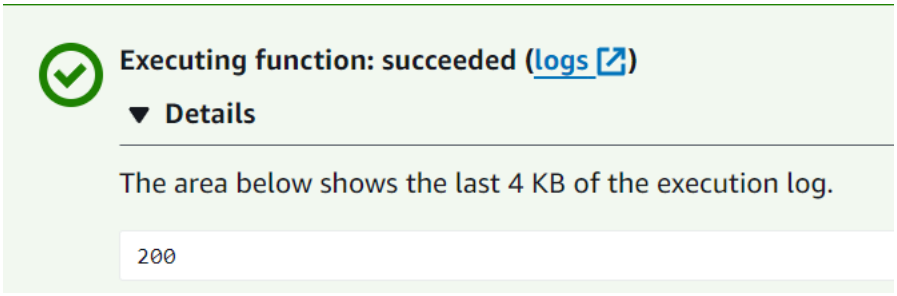

```
import urllib.request
```

```
def lambda_handler(event, context):
    try:
        response = urllib.request.urlopen('https://aws.amazon.com')
        status_code = response.getcode()
        print('Response Code:', status_code)
        return status_code
    except Exception as e:
        print('Error:', e)
        raise e
```

2. Wählen Sie Bereitstellen.
3. Wählen Sie die Registerkarte Test.



4. Wählen Sie Test aus.
5. Die Funktion gibt einen `200` Statuscode zurück. Das bedeutet, dass die Funktion über einen ausgehenden Internetzugang verfügt.



Wenn die Funktion das öffentliche Internet nicht erreichen kann, erhalten Sie eine Fehlermeldung wie diese:

```
{
  "errorMessage": "2024-04-11T17:22:20.857Z abe12jlc-640a-8157-0249-9be825c2y110
 Task timed out after 3.01 seconds"
}
```

Verbinden von VPC-Endpunkten von eingehenden Schnittstellen für Lambda

Wenn Sie Amazon Virtual Private Cloud (Amazon VPC) zum Hosten Ihrer AWS Ressourcen verwenden, können Sie eine Verbindung zwischen Ihrer VPC und Lambda herstellen. Sie können mit dieser Verbindung Ihre Lambda-Funktion aufrufen, ohne das öffentliche Internet überqueren.

Um eine private Verbindung zwischen Ihrer VPC und Lambda herzustellen, erstellen Sie einen Schnittstellen-VPC-Endpunkt. Schnittstellenendpunkte werden von betrieben AWS PrivateLink, sodass Sie privat auf Lambda-APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung erforderlich ist. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Lambda-APIs keine öffentlichen IP-Adressen. Datenverkehr zwischen Ihrer VPC und Lambda verlässt das AWS -Netzwerk nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Eine Netzwerkschnittstelle stellt eine private IP-Adresse bereit, die als Einstiegspunkt für den Datenverkehr zu Lambda dient.

Abschnitte

- Überlegungen für Lambda-Schnittstellenendpunkte
- Erstellen eines Schnittstellenendpunkts für Lambda
- Erstellen einer Richtlinie des Schnittstellenendpunkts für Lambda

Überlegungen für Lambda-Schnittstellenendpunkte

Bevor Sie einen Schnittstellenendpunkt für Lambda einrichten, lesen Sie unbedingt die Eigenschaften und Einschränkungen des Schnittstellenendpunkts im Amazon-VPC-Benutzerhandbuch.

Sie können alle Lambda-API-Operationen von Ihrer VPC aus aufrufen. Sie können die Lambda-Funktion beispielsweise aufrufen, indem Sie die `Invoke`-API aus Ihrer VPC aufrufen. Die vollständige Liste der Lambda-APIs finden Sie unter Aktionen in der Lambda-API-Referenz.

`use1-az3` ist eine Region mit begrenzter Kapazität für Lambda-VPC-Funktionen. Sie sollten in dieser Availability Zone keine Subnetze für Ihre Lambda-Funktionen verwenden, da dies im Falle eines Ausfalls zu einer verringerten zonalen Redundanz führen kann.

Keep-Alive für persistente Verbindungen

Lambda löscht Leerlaufverbindungen im Laufe der Zeit. Daher müssen Sie eine Keep-Alive-Direktive verwenden, um dauerhafte Verbindungen zu pflegen. Der Versuch, eine Leerlaufverbindung beim Aufruf einer Funktion wiederzuverwenden, führt zu einem Verbindungsfehler. Um Ihre persistente Verbindung aufrechtzuerhalten, verwenden Sie die Keep-Alive-Direktive, die Ihrer Laufzeit zugeordnet ist. Ein Beispiel finden Sie unter Wiederverwenden von Verbindungen mit Keep-Alive in Node.js im AWS SDK for JavaScript -Entwicklerhandbuch.

Überlegungen zur Abrechnung

Es fallen keine zusätzlichen Kosten für den Zugriff auf eine Lambda-Funktion über einen Schnittstellen-Endpunkt an. Weitere Informationen über Lambda-Preise finden Sie unter AWS Lambda -Preise.

Die Standardpreise für AWS PrivateLink gelten für Schnittstellenendpunkte für Lambda. Ihrem AWS Konto wird jede Stunde, in der ein Schnittstellenendpunkt in jeder Availability Zone bereitgestellt wird, sowie für Daten, die über den Schnittstellenendpunkt verarbeitet werden, in Rechnung gestellt. Weitere Informationen zu Preisen für Schnittstellenendpunkte finden Sie unter AWS PrivateLink - Preise.

Überlegungen zu VPC Peering

Sie können andere VPCs mit Schnittstellenendpunkten über VPC-Peering mit der VPC verbinden. VPC-Peering ist eine Netzwerkverbindung zwischen zwei VPCs. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen beiden VPCs oder mit einer VPC in einem anderen AWS -Konto herstellen. Die VPCs können sich auch in zwei verschiedenen Regionen befinden. AWS

Der Verkehr zwischen Peer-VPCs verbleibt im AWS Netzwerk und durchquert nicht das öffentliche Internet. Sobald VPCs per Peering verbunden sind, können Ressourcen wie Amazon-Elastic-Compute-Cloud-(Amazon-EC2)-Instances, Amazon-Relational-Database-Service-(Amazon-RDS)-Instances oder VPC-fähige Lambda-Funktionen in beiden VPCs über Schnittstellenendpunkte, die in einem der VPCs erstellt wurden, auf die Lambda-API zugreifen.

Erstellen eines Schnittstellenendpunkts für Lambda

Sie können einen Schnittstellenendpunkt für Lambda entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

So erstellen Sie einen Schnittstellenendpunkt für Lambda (Konsole)

1. Öffnen Sie die Seite Endpunkte der Amazon-VPC-Konsole.
2. Klicken Sie auf Create Endpoint.
3. Stellen Sie sicher, dass für Service-Kategorie die Option AWS -Services ausgewählt ist.
4. Wählen Sie als Service Name (Servicename) com.amazonaws.***region***.lambda aus. Stellen Sie sicher, dass als Typ die Option Schnittstelle gewählt ist.
5. Auswählen von VPC und Subnetzen
6. Um ein privates DNS für den Schnittstellenendpunkt zu aktivieren, aktivieren Sie das Kontrollkästchen für Name eines DNS aktivieren. Wir empfehlen Ihnen, private DNS-Namen für Ihre VPC-Endpunkte für zu aktivieren. AWS-Services Dadurch wird sichergestellt, dass Anfragen, die die Endpunkte des öffentlichen Dienstes verwenden, z. B. Anfragen, die über ein AWS SDK gestellt wurden, an Ihren VPC-Endpunkt weitergeleitet werden.
7. Wählen Sie unter Security group (Sicherheitsgruppe) eine oder mehrere Sicherheitsgruppen aus.
8. Wählen Sie Endpunkt erstellen aus.

Um die private DNS-Option verwenden zu können, müssen Sie `enableDnsHostnames` und `enableDnsSupportattributes` Ihrer VPC festlegen. Weitere Informationen finden Sie unter Anzeigen und Aktualisieren der DNS-Unterstützung für Ihre VPC im Amazon-VPC-Benutzerhandbuch. Wenn Sie einen privaten DNS für den Schnittstellenendpunkt aktivieren, können Sie mittels seines standardmäßigen DNS-Namen für die Region, beispielsweise `lambda.us-east-1.amazonaws.com`, API-Anforderungen an Lambda senden. Weitere Service-Endpunkte finden Sie unter Service-Endpunkte und Kontingente im Allgemeine AWS-Referenz.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Informationen zum Erstellen und Konfigurieren eines Endpunkts mithilfe AWS CloudFormation von finden Sie in der Ressource AWS: :EC2: :VpcEndpoint im Benutzerhandbuch.AWS CloudFormation

So erstellen Sie einen Schnittstellen-Endpunkt für Lambda (AWS CLI)

Verwenden Sie den `create-vpc-endpoint`-Befehl und geben Sie die VPC-ID an, den VPC-Endpunkttyp (Schnittstelle), den Servicenamen, die Subnetze, die den Endpunkt verwenden sollen, sowie die Sicherheitsgruppen, die den Endpunktnetzwerkschnittstellen zugeordnet werden sollen. Zum Beispiel:

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface --
service-name \
   com.amazonaws.us-east-1.lambda --subnet-id subnet-abababab --security-group-id
 sg-1a2b3c4d
```

Erstellen einer Richtlinie des Schnittstellenendpunkts für Lambda

Wenn Sie steuern möchten, wer Ihren Schnittstellenendpunkt verwenden kann und auf welche Lambda-Funktionen der Benutzer zugreifen kann, können Sie eine Endpunktrichtlinie an Ihren Endpunkt anfügen. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann
- Die Aktionen, die der Prinzipal ausführen kann.
- Die Ressourcen, auf denen der Prinzipal Aktionen ausführen kann.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon VPC Benutzerhandbuch.

Beispiel: Schnittstellenendpunktrichtlinie für Lambda-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für Lambda. Bei Anfügung an einen Endpunkt ermöglicht diese Richtlinie dem Benutzer `MyUser` die Funktion `my-function` aufzurufen.

> **Note**
>
> Sie müssen sowohl den qualifizierten als auch den nicht qualifizierten Funktions-ARN in die Ressource aufnehmen.

```
{
   "Statement":[
      {
         "Principal":
         {
             "AWS": "arn:aws:iam::111122223333:user/MyUser"
         },
         "Effect":"Allow",
```

```
         "Action":[
            "lambda:InvokeFunction"
         ],
         "Resource": [
               "arn:aws:lambda:us-east-2:123456789012:function:my-function",
               "arn:aws:lambda:us-east-2:123456789012:function:my-function:*"
            ]
      }
   ]
}
```

Konfigurieren des Dateisystemzugriffs für Lambda-Funktionen

Sie können eine Funktion konfigurieren, um eine Bindungsbereitstellung für ein Amazon-Elastic-File-System-(Amazon-EFS)-Dateisystem in einem lokalen Verzeichnis zu erstellen. Mit Amazon EFS kann Ihr Funktionscode auf freigegebene Ressourcen sicher und mit hoher Nebenläufigkeit zugreifen und diese ändern.

Sections

Ausführungsrolle und Benutzerberechtigungen

Wenn das Dateisystem nicht über eine vom Benutzer konfigurierte Richtlinie AWS Identity and Access Management (IAM) verfügt, verwendet EFS eine Standardrichtlinie, die jedem Client, der über ein Dateisystem-Mount-Ziel eine Verbindung zum Dateisystem herstellen kann, vollen Zugriff gewährt. Wenn das Dateisystem eine benutzerkonfigurierte IAM-Richtlinie hat, muss die Ausführungsrolle Ihrer Funktion die richtigen `elasticfilesystem`-Berechtigungen besitzen.

Berechtigungen für die Ausführungsrolle

- elastisches Dateisystem: ClientMount
- elastisches Dateisystem: ClientWrite (nicht erforderlich für schreibgeschützte Verbindungen)

Diese Berechtigungen sind in der verwalteten Richtlinie enthalten. AmazonElasticFileSystemClientReadWriteAccess Darüber hinaus muss Ihre Ausführungsrolle die Berechtigungen, die für die Verbindung mit der VPC des Dateisystems erforderlich sind, besitzen.

Wenn Sie ein Dateisystem konfigurieren, werden Ihre Berechtigungen von Lambda verwendet, um Bindungsbereitstellung-Ziele zu überprüfen. Um eine Funktion für die Herstellung von Verbindungen mit einer VPC zu konfigurieren, benötigt Ihr Benutzer die folgenden Berechtigungen:

Benutzerberechtigungen

- elasticfilesystem: Ziele DescribeMount

Konfigurieren eines Dateisystems und eines Zugriffspunkts

Erstellen Sie ein Dateisystem in Amazon EFS mit einem Bindungsbereitstellung-Ziel in jeder Availability Zone, zu der Ihre Funktion eine Verbindung herstellt. Verwenden Sie für Leistung und Ausfallsicherheit mindestens zwei Availability Zones. In einer einfachen Konfiguration könnten Sie beispielsweise eine VPC mit zwei privaten Subnetzen in separaten Availability Zones haben. Die Funktion verbindet sich mit beiden Subnetzen und ein Mount-Ziel ist in jedem verfügbar. Stellen Sie sicher, dass NFS-Datenverkehr (Port 2049) von den Sicherheitsgruppen erlaubt ist, die von den Funktionen und Mount-Zielen verwendet werden.

> **Note**
>
> Wenn Sie ein Dateisystem erstellen, wählen Sie einen Leistungsmodus, der später nicht geändert werden kann. Der Allzweckmodus hat eine geringere Latenz, und der Max I/O-Modus unterstützt einen höheren maximalen Durchsatz und IOPS. Hilfe bei der Auswahl finden Sie unter Amazon-EFS-Leistung im Amazon-Elastic-File-System-Benutzerhandbuch.

Ein Zugriffspunkt verbindet jede Instance der Funktion mit dem richtigen Mount-Ziel für die Availability Zone, mit der sie eine Verbindung herstellt. Um eine optimale Leistung zu erzielen, erstellen Sie einen Zugriffspunkt mit einem Nicht-Stammpfad und beschränken Sie die Anzahl der Dateien, die Sie in jedem Verzeichnis erstellen. Im folgenden Beispiel wird ein Verzeichnis mit dem Namen `my-function` auf dem Dateisystem erstellt und die Besitzer-ID auf 1001 mit Standardverzeichnisberechtigungen (755) festgelegt.

Example Konfiguration von Zugriffspunkten

- Name (Name – `files`
- Benutzer-ID – `1001`
- Gruppen-ID – `1001`
- Pfad – `/my-function`
- Berechtigungen – `755`
- Benutzer-ID des Eigentümers – `1001`

- Gruppen-Benutzer-ID – `1001`

Wenn eine Funktion den Zugriffspunkt verwendet, erhält sie die Benutzer-ID 1001 und hat vollen Zugriff auf das Verzeichnis.

Weitere Informationen finden Sie in den folgenden Themen im Amazon-Elastic-File-System-Benutzerhandbuch:

- Erstellen von Ressourcen für Amazon EFS
- Arbeiten mit Benutzern, Gruppen und Berechtigungen

Herstellen einer Verbindung mit einem Dateisystem (Konsole)

Eine Funktion stellt eine Verbindung mit einem Dateisystem über das lokale Netzwerk in einer VPC her. Die Subnetze, mit denen Ihre Funktion eine Verbindung herstellt, können dieselben Subnetze sein, die Mounting-Punkte für Ihr Dateisystem enthalten, oder Subnetze in derselben Availability Zone, die NFS-Datenverkehr (Port 2049) an das Dateisystem weiterleiten kann.

> **Note**
>
> Wenn Ihre Funktion noch nicht mit einer VPC verbunden ist, finden Sie weitere Informationen unter Lambda-Funktionen Zugriff auf Ressourcen in einer Amazon VPC gewähren.

So konfigurieren Sie den Zugriff auf Dateisysteme

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Konfiguration und dann Dateisysteme.
4. Wählen Sie unter Dateisystem die Option Dateisystem hinzufügen.
5. Konfigurieren Sie die folgenden Eigenschaften:
   - EFS-Dateisystem – Der Zugriffspunkt für ein Dateisystem in derselben VPC.
   - Lokaler Bindungsbereitstellungspfad – Der Speicherort, an dem das Dateisystem für die Lambda-Funktion gemountet ist, beginnend mit `/mnt/`.

> **Preisgestaltung**
>
> Amazon EFS erhebt Gebühren für Speicher und Durchsatz, mit Raten, die je nach Speicherklasse variieren. Details dazu finden Sie unter Amazon-EFS-Preise.
> Lambda erhebt Gebühren für die Datenübertragung zwischen VPCs. Dies gilt nur, wenn die VPC Ihrer Funktion auf eine andere VPC mit einem Dateisystem gepeered wird. Die Preise sind die gleichen wie für die Amazon-EC2-Datenübertragung zwischen VPCs in derselben Region. Einzelheiten finden Sie unter Lambda – Preise.

Weitere Informationen zur Lambda-Integration in Amazon EFS finden Sie unter Verwenden von Amazon EFS mit Lambda.

Verwenden eines Amazon EFS-Dateisystems in einem anderen AWS-Konto für eine Lambda-Funktion

Sie können eine Funktion konfigurieren, um ein Amazon EFS-Dateisystem in einem anderen zu mounten AWS-Konto. Bevor Sie das Dateisystem einbinden, müssen Sie Folgendes sicherstellen:

- VPC-Peering muss konfiguriert werden und den Routentabellen in jeder VPC müssen entsprechende Routen hinzugefügt werden.
- Die Sicherheitsgruppe für das Amazon-EFS-Dateisystem, das Sie einbinden möchten, muss so konfiguriert sein, dass der eingehende Zugriff von der Sicherheitsgruppe, die Ihrer Lambda-Funktion zugeordnet ist, zugelassen wird.
- In jeder VPC müssen Subnetze mit passenden Availability Zone (AZ)-IDs erstellt werden.
- In beiden VPCs müssen DNS-Hostnamen aktiviert sein.

Damit Ihre Lambda-Funktion auf ein Amazon EFS-Dateisystem in einem anderen zugreifen kann AWS-Konto, muss dieses Dateisystem auch über eine Dateisystemrichtlinie verfügen, die Ihrer Funktion Berechtigungen erteilt. Informationen zum Erstellen einer Dateisystemrichtlinie finden Sie unter Erstellen von Dateisystemrichtlinien im Benutzerhandbuch zu Amazon Elastic File System.

Im Folgenden wird eine Beispielrichtlinie gezeigt, die Lambda-Funktionen in einem angegebenen Konto die Berechtigung gewährt, alle API-Aktionen in einem Dateisystem auszuführen.

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

```
    "Id": "efs-lambda-policy",
    "Statement": [
        {
            "Sid": "efs-lambda-statement",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{LAMBDA-ACCOUNT-ID}:root"
            },
            "Action": "*",
            "Resource": "arn:aws:elasticfilesystem:{REGION}:{ACCOUNT-ID}:file-
system/{FILE SYSTEM ID}"
        }
    ]
}
```

> **Note**
>
> Die gezeigte Beispielrichtlinie verwendet das Platzhalterzeichen („*“), um Lambda-Funktionen in der angegebenen Liste Berechtigungen zur Ausführung beliebiger API-Operationen im Dateisystem AWS-Konto zu gewähren. Dies beinhaltet das Löschen des Dateisystems. Um die Operationen einzuschränken, die andere an Ihrem Dateisystem ausführen AWS-Konten können, geben Sie die Aktionen an, die Sie explizit zulassen möchten. Eine Liste möglicher API-Operationen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Elastic File System.

Um das kontenübergreifende Dateisystem-Mounten zu konfigurieren, verwenden Sie die Operation AWS Command Line Interface (AWS CLI)`update-function-configuration`.

Um ein Dateisystem in einem anderen zu mounten AWS-Konto, führen Sie den folgenden Befehl aus. Verwenden Sie Ihren eigenen Funktionsnamen und ersetzen Sie den Amazon-Ressourcenname (ARN) durch den ARN des Amazon-EFS-Zugangspunkts für das Dateisystem, das Sie einbinden möchten. `LocalMountPath` ist der Pfad, über dem die Funktion auf das Dateisystem zugreifen kann, beginnend mit `/mnt/`. Stellen Sie sicher, dass der Lambda-Einbindungspfad mit dem Zugangspunktpfad für das Dateisystem übereinstimmt. Wenn der Zugangspunkt beispielsweise `/efs` ist, muss der Lambda-Einbindungspfad `/mnt/efs` sein.

```
aws lambda update-function-configuration --function-name MyFunction \
--file-system-configs Arn=arn:aws:elasticfilesystem:us-east-1:222222222222:access-
point/fsap-01234567,LocalMountPath=/mnt/test
```

Erstellen Sie einen Alias für eine Lambda-Funktion

Sie können für Ihre Lambda-Funktion Aliasse erstellen. Ein Lambda-Alias ist ein Zeiger auf eine Version einer Funktion, der aktualisiert werden kann. Die Benutzer der Funktion können über den Amazon-Ressourcennamen (ARN) des Alias auf die Funktionsversion zugreifen. Wenn Sie eine neue Version bereitstellen, können Sie den Alias aktualisieren, um ihn auf die neue Version umzustellen oder den Datenverkehr zwischen zwei Versionen aufzuteilen.

Sections

Erstellen eines Funktionsalias (Konsole)

Sie können einen Funktionsalias mit der Lambda-Konsole erstellen.

Erstellen eines Alias

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Aliasse und dann Alias erstellen aus.
4. Führen Sie auf der Seite Alias erstellen die folgenden Schritte aus:
    a. Machen Sie für den Alias eine Angabe unter Name.
    b. (Optional) Geben Sie eine Beschreibung für den Alias ein.
    c. Wählen Sie unter Version, eine Funktionsversion aus, auf die der Alias verweisen soll.
    d. (Optional) Um das Routing für den Alias zu konfigurieren, erweitern Sie den Eintrag Gewichteter Alias. Weitere Informationen finden Sie unter Alias-Weiterleitungskonfiguration.
    e. Wählen Sie Save (Speichern) aus.

Verwalten von Aliassen mit der Lambda-API

Verwenden Sie den `create-alias`Befehl, um einen Alias mit AWS Command Line Interface (AWS CLI) zu erstellen.

```
aws lambda create-alias --function-name my-function --name alias-name --function-version version-number --description " "
```

Verwenden Sie den Befehl `update-alias`, um einen Alias so zu ändern, dass er auf eine neue Version der Funktion verweist.

```
aws lambda update-alias --function-name my-function --name alias-name --function-version version-number
```

Verwenden Sie den Befehl `delete-alias`, um einen Alias zu löschen.

```
aws lambda delete-alias --function-name my-function --name alias-name
```

Die AWS CLI Befehle in den vorherigen Schritten entsprechen den folgenden Lambda-API-Operationen:

- CreateAlias
- UpdateAlias
- DeleteAlias

Verwaltung von Aliasen mit und AWS SAMAWS CloudFormation

Sie können Funktionsaliase mit AWS Serverless Application Model (AWS SAM) und erstellen und verwalten. AWS CloudFormation

Informationen zur Deklaration eines Funktionsalias in einer AWS SAM Vorlage finden Sie auf der Seite AWS: :Serverless: :Function im Developer Guide. AWS SAM Informationen zum Erstellen und Konfigurieren von Aliasen mithilfe AWS CloudFormation von finden Sie unter AWS: :Lambda: :Alias im Benutzerhandbuch. AWS CloudFormation

Verwenden von Aliassen

Jeder Alias hat einen eindeutigen ARN. Ein Alias kann nur auf eine Funktionsversion verweisen, nicht auf einen anderen Alias. Sie können einen Alias aktualisieren, um auf eine neue Version der Funktion zu verweisen.

Ereignisquellen wie Amazon Simple Storage Service (Amazon S3) rufen Ihre Lambda-Funktion auf. Diese Ereignisquellen pflegen eine Zuweisung, die die Funktion identifiziert, die beim Auftreten von Ereignissen aufgerufen werden soll. Wenn Sie in der Mappingkonfiguration einen Lambda-Funktionsalias angeben, müssen Sie das Mapping nicht aktualisieren, wenn sich die Funktionsversion ändert. Weitere Informationen finden Sie unter Wie Lambda Datensätze aus Stream- und warteschlangenbasierten Ereignisquellen verarbeitet.

In einer Ressourcenrichtlinie können Sie Berechtigungen für Ereignisquellen zur Verwendung Ihrer Lambda-Funktion erteilen. Wenn Sie in der Richtlinie einen Alias-ARN angeben, müssen Sie die Richtlinie nicht aktualisieren, wenn sich die Funktionsversion ändert.

Ressourcenrichtlinien

Sie können eine ressourcenbasierte Richtlinie verwenden, um einem Dienst, einer Ressource oder einem Konto Zugriff auf Ihre Funktion zu gewähren. Der Umfang dieser Berechtigung hängt davon ab, ob Sie sie auf einen Alias, eine Version oder die gesamte Funktion anwenden. Wenn Sie beispielsweise einen Aliasnamen verwenden (z. B. `helloworld:PROD`), gewährt Ihnen die Berechtigung, die Funktion `helloworld` mithilfe des ARN des Alias (`helloworld:PROD`) aufzurufen.

Wenn Sie versuchen, die Funktion ohne Alias oder eine bestimmte Version aufzurufen, erhalten Sie einen Berechtigungsfehler. Dieser Berechtigungsfehler tritt weiterhin auf, selbst wenn Sie versuchen, die dem Alias zugeordnete Funktionsversion direkt aufzurufen.

Der folgende AWS CLI Befehl erteilt Amazon S3 beispielsweise die Berechtigung, den PROD-Alias der `helloworld` Funktion aufzurufen, wenn Amazon S3 im Namen von handelt. `DOC-EXAMPLE-BUCKET`

```
aws lambda add-permission --function-name helloworld \
--qualifier PROD --statement-id 1 --principal s3.amazonaws.com --action
 lambda:InvokeFunction \
--source-arn arn:aws:s3:::DOC-EXAMPLE-BUCKET --source-account 123456789012
```

Weitere Hinweise zum Verwenden von Ressourcennamen in Richtlinien finden Sie unter Feinabstimmung der Abschnitte „Ressourcen“ und „Bedingungen“ der Richtlinien.

Alias-Weiterleitungskonfiguration

Verwenden Sie die Weiterleitungskonfiguration für einen Alias, um einen Teil des Datenverkehrs an eine zweite Funktionsversion zu senden. Beispielsweise können Sie das Risiko der Bereitstellung einer neuen Version verringern, indem Sie den Alias so konfigurieren, dass der größte Teil des Datenverkehrs an die vorhandene Version gesendet wird, und nur ein geringer Prozentsatz des Datenverkehrs an die neue Version.

Beachten Sie, dass Lambda ein einfaches probabilistisches Modell verwendet, um den Datenverkehr zwischen den beiden Funktionsversionen zu verteilen. Bei niedrigem Datenverkehr sehen Sie möglicherweise eine hohe Abweichung zwischen dem konfigurierten und dem tatsächlichen Prozentsatz des Datenverkehrs für jede Version. Wenn Ihre Funktion bereitgestellte Parallelität verwendet, können Sie Überlaufaufrufe durch Konfigurieren einer höheren Anzahl von bereitgestellten Parallelitätsinstances während des aktiven Alias-Routings vermeiden.

Sie können ein Alias auf maximal zwei Lambda-Funktionsversionen verweisen lassen. Die Versionen müssen folgende Kriterien erfüllen:

- Beide Versionen müssen die gleiche Ausführungsrolle haben.
- Beide Versionen müssen die gleiche Warteschlangenkonfiguration für unzustellbare Nachrichten oder keine Warteschlangenkonfiguration für unzustellbare Nachrichten haben.
- Beide Versionen müssen veröffentlicht werden. Der Alias darf nicht auf verweise `$LATEST`.

Konfigurieren des Routings für einen Alias

> **Note**
>
> Stellen Sie sicher, dass die Funktion über mindestens zwei veröffentlichte Versionen verfügt. Um weitere Versionen zu erstellen, folgen Sie den Anweisungen unter Versionen der Lambda-Funktion.

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.

3. Wählen Sie Aliasse und dann Alias erstellen aus.
4. Führen Sie auf der Seite Alias erstellen die folgenden Schritte aus:

   a. Machen Sie für den Alias eine Angabe unter Name.
   b. (Optional) Geben Sie eine Beschreibung für den Alias ein.
   c. Wählen Sie unter Version die erste Funktionsversion aus, auf die der Alias verweisen soll.
   d. Erweitern Sie Gewichteter Alias.
   e. Wählen Sie unter Zusätzliche Version die zweite Funktionsversion aus, auf die der Alias verweisen soll.
   f. Geben Sie unter Gewicht (%) einen Gewichtungswert für die Funktion ein. Die Gewichtung ist der Prozentsatz des Datenverkehrs, der beim Aufruf des Alias dieser Version zugewiesen wird. Die erste Version erhält den Datenverkehr mit der verbleibenden Gewichtung. Wenn Sie beispielsweise 10 Prozent für die Additional version (Zusätzliche Version) angeben, werden der ersten Version automatisch 90 Prozent zugewiesen.
   g. Wählen Sie Save aus.

Konfigurieren des Alias-Routings mithilfe der CLI

Verwenden Sie die Befehle `update-alias` AWS CLI und `create-alias`, um die Datenverkehrsgewichtungen zwischen zwei Funktionsversionen zu konfigurieren. Wenn Sie den Alias erstellen oder aktualisieren, geben Sie die Datenverkehrsgewichtung im `routing-config`-Parameter an.

Im folgenden Beispiel wird ein Lambda-Funktionsalias namens routing-alias erstellt, der auf Version 1 der Funktion verweist. Version 2 der Funktion erhält 3 Prozent des Datenverkehrs. Die verbleibenden 97 Prozent des Datenverkehrs werden zu Version 1 weitergeleitet.

```
aws lambda create-alias --name routing-alias --function-name my-function --function-
version 1  \
--routing-config AdditionalVersionWeights={"2"=0.03}
```

Verwenden Sie den `update-alias`-Befehl, um den Prozentsatz des eingehenden Datenverkehrs an Version 2 zu erhöhen. Im folgenden Beispiel erhöhen Sie den Datenverkehr auf 5 Prozent.

```
aws lambda update-alias --name routing-alias --function-name my-function  \
--routing-config AdditionalVersionWeights={"2"=0.05}
```

Um den gesamten Datenverkehr an Version 2 weiterzuleiten, ändern Sie den Befehl `update-alias`, um die Eigenschaft `function-version` so zu ändern, dass der Alias auf Version 2 verweist. Der Befehl setzt auch die Weiterleitungskonfiguration zurück.

```
aws lambda update-alias --name routing-alias --function-name my-function  \
--function-version 2 --routing-config AdditionalVersionWeights={}
```

Die AWS CLI Befehle in den vorherigen Schritten entsprechen den folgenden Lambda-API-Operationen:

- CreateAlias
- UpdateAlias

Feststellen, welche Version aufgerufen wurde

Wenn Sie Datenverkehrsgewichtungen zwischen zwei Funktionsversionen konfigurieren, gibt es zwei Möglichkeiten, die aufgerufene Lambda-Funktionsversion zu bestimmen:

- CloudWatch Logs — Lambda gibt bei jedem Funktionsaufruf automatisch einen `START` Protokolleintrag, der die aufgerufene Versions-ID enthält, an Amazon CloudWatch Logs aus. Im Folgenden wird ein Beispiel gezeigt:

  ```
  19:44:37 START RequestId: request id Version: $version
  ```

  Für Aliasaufrufe verwendet Lambda die Dimension `Executed Version` zum Filtern der Metrikdaten nach aufgerufener Version. Weitere Informationen finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.
- Antwortnutzlast (synchrone Aufrufe) – Antworten auf synchrone Funktionsaufrufe enthalten einen `x-amz-executed-version`-Header, der angibt, welche Funktionsversion aufgerufen wurde.

Versionen der Lambda-Funktion

Sie können Versionen verwenden, um die Bereitstellung Ihrer Funktionen zu verwalten. Beispielsweise können Sie eine neue Version einer Funktion für Beta-Tests veröffentlichen, ohne dass Benutzer der stabilen Produktionsversion betroffen sind. Lambda erstellt jedes Mal, wenn Sie die Funktion veröffentlichen, eine neue Version Ihrer Funktion. Die neue Version ist eine Kopie der unveröffentlichten Version der Funktion. Die unveröffentlichte Version heißt $LATEST.

> **Note**
>
> Um eine neue Version Ihrer Funktion zu erstellen, müssen Sie zunächst Änderungen an der unveröffentlichten Version ($LATEST) vornehmen. Diese Änderungen können das Aktualisieren des Codes oder das Ändern der Konfigurationseinstellungen beinhalten. Wenn $LATEST mit einer zuvor veröffentlichten Version identisch ist, können Sie keine neue Version erstellen, bis Sie Änderungen an $LATEST bereitstellen.

Nachdem Sie eine Funktionsversion veröffentlicht haben, sind der Code, die Laufzeit, die Architektur, der Arbeitsspeicher, die Ebenen und die meisten anderen Konfigurationseinstellungen unveränderlich. Das bedeutet, dass Sie diese Einstellungen nicht ändern können, ohne eine neue Version von $LATEST zu veröffentlichen. Sie können die folgenden Elemente für eine veröffentlichte Funktionsversion konfigurieren:

- Auslöser
- Ziele
- Bereitgestellte Gleichzeitigkeit
- Asynchroner Aufruf
- Datenbankverbindungen und Proxys

> **Note**
>
> Bei Verwendung von Laufzeitverwaltungskontrollen im Auto-Modus wird die von der Funktionsversion verwendete Laufzeitversion automatisch aktualisiert. Bei Verwendung des Modus Function update (Funktionsaktualisierung) oder Manual (Manuell) wird die Laufzeitversion nicht aktualisiert. Weitere Informationen finden Sie unter the section called “Laufzeitaktualisierungen”.

Sections

Erstellen von Funktionsversionen

Sie können den Funktionscode und die Einstellungen nur in der nicht veröffentlichten Version einer Funktion ändern. Wenn Sie eine Version veröffentlichen, sperrt Lambda den Code und die meisten Einstellungen, um eine konsistente Erfahrung für Benutzer dieser Version zu gewährleisten.

Sie können eine Funktionsversion mit der Lambda-Konsole erstellen.

So erstellen Sie eine neue Funktionsversion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus und dann Versionen.
3. Wählen Sie auf der Versionskonfigurationsseite die Option Neue Version veröffentlichen aus.
4. (Optional) Geben Sie eine Versionsbeschreibung ein.
5. Wählen Sie Publish.

Alternativ können Sie eine Version einer Funktion mithilfe der PublishVersion -API-Operation veröffentlichen.

Der folgende AWS CLI Befehl veröffentlicht eine neue Version einer Funktion. In der Antwort werden die Konfigurationsinformationen der neuen Version zurückgegeben, einschließlich der Versionsnummer und des Funktion-ARN mit dem Versionssuffix.

```
aws lambda publish-version --function-name my-function
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
  "FunctionName": "my-function",
  "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:1",
  "Version": "1",
  "Role": "arn:aws:iam::123456789012:role/lambda-role",
```

```
  "Handler": "function.handler",
  "Runtime": "nodejs20.x",
  ...
}
```

> **Note**
>
> Lambda weist monoton steigende Sequenznummern für die Versionsverwaltung zu. Lambda verwendet niemals Versionsnummern wieder, auch nicht nachdem Sie eine Funktion gelöscht und neu erstellt haben.

Verwenden von Versionen

Sie können Ihre Lambda-Funktion entweder mit einem qualifizierten ARN oder einem nicht qualifizierten ARN referenzieren.

- Qualifizierter ARN – Hierbei handelt es sich um den ARN der Funktion mit einem Versionssuffix. Das folgende Beispiel bezieht sich auf Version 42 der Funktion `helloworld`.

  ```
  arn:aws:lambda:aws-region:acct-id:function:helloworld:42
  ```

- Unqualifizierter ARN – Hierbei handelt es sich um den ARN der Funktion ohne ein Versionssuffix.

  ```
  arn:aws:lambda:aws-region:acct-id:function:helloworld
  ```

Sie können in allen relevanten API-Operationen einen qualifizierten oder einen nicht qualifizierten ARN verwenden. Sie können jedoch keinen unqualifizierten ARN verwenden, um einen Alias zu erstellen.

Wenn Sie sich entscheiden, Funktionsversionen nicht zu veröffentlichen, können Sie entweder den qualifizierten oder den nicht qualifizierten ARN in Ihrer Ereignisquellen-Zuweisung verwenden, um die Funktion aufzurufen. Wenn Sie eine Funktion mit einem unqualifizierten ARN aufrufen, ruft Lambda implizit $LATEST auf.

Lambda veröffentlicht eine neue Funktionsversion nur, wenn der Code noch nie veröffentlicht wurde oder wenn sich der Code gegenüber der zuletzt veröffentlichten Version geändert hat. Wenn keine Änderung vorliegt, bleibt die Funktionsversion die zuletzt veröffentlichte Version.

Der qualifizierte ARN für jede Lambda-Funktionsversion ist eindeutig. Nachdem Sie eine Version veröffentlicht haben, können Sie den ARN oder den Funktionscode nicht ändern.

Gewähren von Berechtigungen

Sie können eine ressourcenbasierte Richtlinie oder eine identitätsbasierte Richtlinie verwenden, um Zugriff auf Ihre Funktion zu gewähren. Der Umfang der Berechtigung hängt davon ab, ob Sie die Richtlinie auf eine Funktion oder auf eine Version einer Funktion anwenden. Weitere Hinweise zu Funktionsressourcennamen in Richtlinien finden Sie unter Feinabstimmung der Abschnitte „Ressourcen“ und „Bedingungen“ der Richtlinien.

Sie können die Verwaltung von Ereignisquellen und AWS Identity and Access Management (IAM)-Richtlinien mithilfe von Funktionsaliasnamen vereinfachen. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für eine Lambda-Funktion.

Konfigurieren einer Lambda-Funktion zum Streamen von Antworten

Sie können Ihre Lambda-Funktions-URLs so konfigurieren, dass sie Antwort-Nutzlasten zurück an Clients streamen. Antwort-Streaming kann für latenzempfindliche Anwendungen von Vorteil sein, da es die Leistung in der Zeit bis zum ersten Byte (TTFB) verbessert. Dies liegt daran, dass Sie Teilantworten an den Client zurücksenden können, sobald sie verfügbar sind. Darüber hinaus können Sie Response-Streaming verwenden, um Funktionen zu erstellen, die größere Nutzlasten zurückgeben. Die Nutzlasten von Antwortstreams haben ein Soft-Limit von 20 MB im Vergleich zu den 6 MB für gepufferte Antworten. Das Streameng einer Antwort bedeutet auch, dass Ihre Funktion nicht die gesamte Antwort im Speicher unterbringen muss. Bei sehr großen Antworten kann dies die Menge des Speichers reduzieren, die Sie für Ihre Funktion konfigurieren müssen.

Die Geschwindigkeit, mit der Lambda Ihre Antworten streamt, hängt von der Größe der Antwort ab. Die Streaming-Rate für die ersten 6 MB der Antwort Ihrer Funktion ist nicht begrenzt. Bei Antworten, die größer als 6 MB sind, gilt für den Rest der Antwort eine Bandbreitenbegrenzung. Weitere Informationen zur Streaming-Bandbreite finden Sie unter Bandbreitenbegrenzung für Antwort-Streaming.

Das Streamen von Antworten ist mit Kosten verbunden. Weitere Informationen finden Sie unter AWS Lambda-Preisgestaltung.

Lambda unterstützt Antwortstreaming auf verwalteten Laufzeiten von Node.js. Für andere Sprachen können Sie eine benutzerdefinierte Laufzeit auch mit einer benutzerdefinierten Laufzeit-API-Integration verwenden, um Antworten zu streamen, oder den Lambda Web Adapter verwenden. Sie können Antworten über Lambda-Funktions-URLs, das SDK AWS oder mithilfe der Lambda-InvokeWithResponseStreamAPI streamen.

> **Note**
>
> Wenn Sie Ihre Funktion über die Lambda-Konsole testen, werden die Antworten immer gepuffert angezeigt.

Schreiben von Antwort-Streaming-fähigen Funktionen

Das Schreiben des Handlers für Antwort-Streaming-Funktionen unterscheidet sich von typischen Handler-Mustern. Wenn Sie Streaming-Funktionen schreiben, sollten Sie Folgendes beachten:

- Verpacken Sie Ihre Funktion mit dem `awslambda.streamifyResponse()`-Decorator, den die nativen Laufzeiten von Node.js zur Verfügung stellen..
- Beenden Sie den Stream ordnungsgemäß, um sicherzustellen, dass die Datenverarbeitung abgeschlossen ist.

Konfigurieren einer Handler-Funktion zum Streamen von Antworten

Um der Laufzeit zu signalisieren, dass Lambda die Antworten Ihrer Funktion streamen soll, müssen Sie Ihre Funktion mit dem `streamifyResponse()`-Decorator wrappen. Dadurch wird die Laufzeit angewiesen, den richtigen Logikpfad für Streaming-Antworten zu verwenden, und ermöglicht es der Funktion, Antworten zu streamen.

Der `streamifyResponse()`-Decorator akzeptiert eine Funktion, die die folgenden Parameter akzeptiert:

- `event` – Stellt Informationen über das Aufrufereignis der Funktions-URL bereit, z. B. die HTTP-Methode, Abfrageparameter und den Anforderungskörper.
- `responseStream` – Stellt einen schreibbaren Stream bereit.
- `context` – Stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Das `responseStream`-Objekt ist ein Node.js `writableStream`. Wie bei jedem solchen Stream sollten Sie die `pipeline()`-Methode verwenden.

Example Handler mit aktiviertem Antwort-Streaming

```
const pipeline = require("util").promisify(require("stream").pipeline);
const { Readable } = require('stream');

exports.echo = awslambda.streamifyResponse(async (event, responseStream, _context) => {
  // As an example, convert event to a readable stream.
  const requestStream = Readable.from(Buffer.from(JSON.stringify(event)));

  await pipeline(requestStream, responseStream);
});
```

Obwohl `responseStream` die `write()`-Methode bietet, in den Stream zu schreiben, empfehlen wir Ihnen, wo immer möglich, `pipeline()` zu verwenden. Die Verwendung von `pipeline()` stellt sicher, dass der schreibbare Stream nicht von einem schneller lesbaren Stream überfordert wird.

Den Stream beenden

Stellen Sie sicher, dass Sie den Stream ordnungsgemäß beenden, bevor der Handler zurückkehrt. Die `pipeline()`-Methode verarbeitet dies automatisch.

Für andere Anwendungsfälle rufen Sie die `responseStream.end()`-Methode auf, um einen Stream ordnungsgemäß zu beenden. Diese Methode signalisiert, dass keine Daten mehr in den Stream geschrieben werden sollen. Diese Methode ist nicht erforderlich, wenn Sie mit `pipeline()` oder `pipe()` in den Stream schreiben.

Example Beispiel für das Beenden eines Streams mit Pipeline ()

```
const pipeline = require("util").promisify(require("stream").pipeline);

exports.handler = awslambda.streamifyResponse(async (event, responseStream, _context)
 => {
  await pipeline(requestStream, responseStream);
});
```

Example Beispiel für das Beenden eines Streams ohne Pipeline ()

```
exports.handler = awslambda.streamifyResponse(async (event, responseStream, _context)
 => {
  responseStream.write("Hello ");
  responseStream.write("world ");
  responseStream.write("from ");
  responseStream.write("Lambda!");
  responseStream.end();
});
```

Aufrufen einer Antwort-Streaming-fähigen Funktion mit Lambda-Funktions-URLs

> **Note**
>
> Sie müssen Ihre Funktion mit einer Funktions-URL aufrufen, um die Antworten zu streamen.

Sie können Funktionen mit aktiviertem Antwort-Streaming aufrufen, indem Sie den Aufrufmodus der URL Ihrer Funktion ändern. Der Aufrufmodus bestimmt, welche API-Operation Lambda verwendet, um Ihre Funktion aufzurufen. Die verfügbaren Aufrufmodi sind:

- `BUFFERED` – Dies ist die Standardoption. Lambda ruft Ihre Funktion mithilfe der `Invoke`-API-Operation auf. Die Aufrufergebnisse sind verfügbar, wenn die Nutzlast abgeschlossen ist. Die maximale Nutzlastgröße beträgt 6 MB.
- `RESPONSE_STREAM` – Ermöglicht es Ihrer Funktion, die Ergebnisse der Nutzlasten zu streamen, sobald sie verfügbar sind. Lambda ruft Ihre Funktion mithilfe der `InvokeWithResponseStream`-API-Operation auf. Die maximale Nutzlastgröße beträgt 20 MB. Sie können allerdings eine Kontingenterhöhung beantragen.

Sie können Ihre Funktion auch ohne Antwort-Streaming aufrufen, indem Sie die `Invoke`-API-Operation direkt aufrufen. Lambda streamt jedoch alle Antwort-Nutzlasten für Aufrufe, die über die URL der Funktion erfolgen, bis Sie den Aufrufmodus auf `BUFFERED` ändern.

Um den Aufrufmodus einer Funktions-URL (Konsole) festzulegen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen der Funktion, für die Sie den Aufrufmodus festlegen möchten.
3. Wählen Sie die Registerkarte Konfiguration und dann Funktions-URL.
4. Wählen Sie Bearbeiten und dann Zusätzliche Einstellungen.
5. Wählen Sie unter Aufrufmodus den gewünschten Aufrufmodus aus.
6. Wählen Sie Speichern.

Um den Aufrufmodus einer Funktions-URL (AWS CLI) festzulegen

```
aws lambda update-function-url-config --function-name my-function --invoke-mode
 RESPONSE_STREAM
```

Um den Aufrufmodus einer Funktions-URL (AWS CloudFormation) festzulegen

```
MyFunctionUrl:
  Type: AWS::Lambda::Url
  Properties:
    AuthType: AWS_IAM
```

```
    InvokeMode: RESPONSE_STREAM
```

Weitere Hinweise zum Konfigurieren von Funktions-URLs finden Sie unter Lambda-Funktions-URLs.

Bandbreitenbegrenzung für Antwort-Streaming

Für die ersten 6 MB der Nutzlast Ihrer Funktion gibt es keine Bandbreitenbegrenzung. Nach diesem ersten Burst streamt Lambda Ihre Antwort mit einer maximalen Rate von 2 MB/s. Wenn Ihre Funktionsantworten nie größer als 6 MB sind, gilt diese Bandbreitenbegrenzung nicht.

> **Note**
>
> Bandbreitenbegrenzungen gelten nur für die Antwortnutzlast Ihrer Funktion und nicht für den Netzwerkzugriff durch Ihre Funktion.

Die Rate der unbegrenzten Bandbreite hängt von einer Reihe von Faktoren ab, einschließlich der Verarbeitungsgeschwindigkeit Ihrer Funktion. Normalerweise können Sie für die ersten 6 MB der Antwort Ihrer Funktion eine Rate von mehr als 2 MB/s erwarten. Wenn Ihre Funktion eine Antwort an ein Ziel außerhalb von AWS streamt, hängt die Streaming-Rate auch von der Geschwindigkeit der externen Internetverbindung ab.

Tutorial: Erstellen einer Lambda-Funktion zum Streamen von Antworten mit einer Funktions-URL

In diesem Tutorial erstellen Sie eine Lambda-Funktion, die als ZIP-Dateiarchiv mit einem Funktions-URL-Endpunkt definiert ist, der einen Antwort-Stream zurückgibt. Weitere Hinweise zum Konfigurieren von Funktions-URLs finden Sie unter Erstellen und Verwalten von Funktions-URLs.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen einer Ausführungsrolle

Erstellen Sie die Ausführungsrolle die Ihrer Lambda-Funktion die Berechtigung für den Zugriff auf AWS -Ressourcen erteilt.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Rollen der AWS Identity and Access Management (IAM)-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften:
   - Vertrauenswürdiger Entitätstyp – AWS -Service
   - Anwendungsfall – Lambda
   - Berechtigungen — AWSLambdaBasicExecutionRole
   - Role name (Name der Rolle – **`response-streaming-role`**

Die AWSLambdaBasicExecutionRoleRichtlinie verfügt über die Berechtigungen, die die Funktion benötigt, um Protokolle in Amazon CloudWatch Logs zu schreiben. Nachdem Sie die Rolle erstellt haben, notieren Sie sich den Amazon-Ressourcennamen (ARN). Sie benötigen ihn im nächsten Schritt.

Erstellen Sie eine Antwort-Streaming-Funktion (AWS CLI)

Erstellen Sie eine Antwort-Streaming-Lambda-Funktion mit einem Funktions-URL-Endpunkt unter Verwendung der AWS Command Line Interface (AWS CLI).

Um eine Funktion zu erstellen, die Antworten streamen kann

1. Kopieren Sie das folgende Codebeispiel in eine Datei mit dem Namen `index.mjs`.

```
import util from 'util';
import stream from 'stream';
const { Readable } = stream;
const pipeline = util.promisify(stream.pipeline);

/* global awslambda */
export const handler = awslambda.streamifyResponse(async (event, responseStream,
 _context) => {
  const requestStream = Readable.from(Buffer.from(JSON.stringify(event)));
  await pipeline(requestStream, responseStream);
});
```

2. Erstellen Sie ein Bereitstellungspaket.

```
zip function.zip index.mjs
```

3. Erstellen Sie eine Lambda-Funktion mit dem Befehl `create-function`. Ersetzen Sie den Wert von `--role` durch den Rollen-ARN aus dem vorherigen Schritt.

```
aws lambda create-function \
  --function-name my-streaming-function \
  --runtime nodejs16.x \
  --zip-file fileb://function.zip \
  --handler index.handler \
  --role arn:aws:iam::123456789012:role/response-streaming-role
```

Um eine Funktions-URL zu erstellen

1. Fügen Sie Ihrer Funktion eine ressourcenbasierte Richtlinie hinzu, um den Zugriff auf Ihre Funktions-URL zu ermöglichen. Ersetzen Sie den Wert von `--principal` durch Ihre AWS-Konto ID.

```
aws lambda add-permission \
  --function-name my-streaming-function \
  --action lambda:InvokeFunctionUrl \
  --statement-id 12345 \
  --principal 123456789012 \
  --function-url-auth-type AWS_IAM \
  --statement-id url
```

2. Erstellen Sie einen URL-Endpunkt für die Funktion mit dem Befehl `create-function-url-config`.

```
aws lambda create-function-url-config \
  --function-name my-streaming-function \
  --auth-type AWS_IAM \
  --invoke-mode RESPONSE_STREAM
```

Testen des Funktions-URL-Endpunkts

Testen Sie Ihre Integration, indem Sie Ihre Funktion aufrufen. Sie können die URL Ihrer Funktion in einem Browser öffnen oder curl verwenden.

```
curl --request GET "<function_url>" --user "<key:token>" --aws-sigv4 "aws:amz:us-east-1:lambda" --no-buffer
```

Unsere Funktions-URL nutzt den Authentifizierungstyp `IAM_AUTH`. Das bedeutet, dass Sie Anfragen sowohl mit Ihrem AWS Zugriffsschlüssel als auch mit Ihrem geheimen Schlüssel signieren müssen. Ersetzen Sie dies im vorherigen Befehl `<key:token>` durch die AWS Zugriffsschlüssel-ID. Geben Sie Ihren AWS geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden. Wenn Sie Ihren AWS geheimen Schlüssel nicht haben, können Sie stattdessen temporäre AWS Anmeldeinformationen verwenden.

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

Bereitstellen von Lambda-Funktionen

Sie können Code für Ihre Lambda-Funktion bereitstellen, indem Sie ein ZIP-Dateiarchiv hochladen oder ein Container-Image erstellen und hochladen.

Themen

ZIP-Dateiarchive

Ein ZIP-Dateiarchiv enthält Ihren Anwendungscode und seine Abhängigkeiten. Wenn Sie Funktionen mit der Lambda-Konsole oder einem Toolkit erstellen, erstellt Lambda automatisch ein ZIP-Dateiarchiv Ihres Codes.

Wenn Sie Funktionen mit der Lambda-API, Befehlszeilentools oder den AWS SDKs erstellen, müssen Sie ein Bereitstellungspaket erstellen. Sie müssen außerdem ein Bereitstellungspaket erstellen, wenn Ihre Funktion eine kompilierte Sprache verwendet oder Ihrer Funktion Abhängigkeiten hinzufügt. Um den Code Ihrer Funktion bereitzustellen, laden Sie das Bereitstellungspaket von Amazon Simple Storage Service (Amazon S3) oder Ihrem lokalen Computer hoch.

Sie können mit der Lambda-Konsole AWS Command Line Interface (AWS CLI) eine ZIP-Datei als Bereitstellungspaket oder in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochladen.

Berechtigungen für Bereitstellungspaketdateien

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Linux-Notation der Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen (rwxr-xr-x) für Verzeichnisse und ausführbare Dateien.

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Container-Images

Sie können Ihren Code und Ihre Abhängigkeiten als Container-Image mit Tools wie der Command Line Interface (CLI) verpacken. Sie können das Image dann in Ihre Container-Registry uploaden, die auf Amazon Elastic Container Registry (Amazon ECR) gehostet wird.

Wenn Sie die Funktion aufrufen, stellt Lambda das Container-Image in einer Ausführungsumgebung bereit. Lambda initialisiert alle Erweiterungen und führt dann den Initialisierungscode der Funktion aus (der Code außerhalb des Haupt-Handlers). Beachten Sie, dass die Dauer der Funktionsinitialisierung in der abgerechneten Ausführungszeit enthalten ist.

Lambda führt dann die Funktion aus, indem es den in der Funktionskonfiguration angegebenen Codeeingabepunkt aufruft (die ENTRYPOINT - und CMD-Container-Image-Einstellungen).

AWS stellt eine Reihe von Open-Source-Basis-Images bereit, mit denen Sie das Container-Image für Ihren Funktionscode erstellen können. Sie können auch alternative Basis-Images aus anderen Container-Registern verwenden. AWS bietet auch einen Open-Source-Runtime-Client, den Sie zu Ihrem alternativen Basis-Image hinzufügen, um es mit dem Lambda-Service kompatibel zu machen.

Darüber hinaus AWS bietet es einen Runtime-Schnittstellen-Emulator, mit dem Sie Ihre Funktionen lokal mit Tools wie der Docker-CLI testen können.

> **Note**
>
> Sie erstellen jedes Container-Image, um mit einer der von Lambda unterstützten Befehlssatz-Architekturen kompatibel zu sein. Lambda stellt Basis-Images für jede der Befehlssatzarchitekturen bereit und Lambda bietet auch Basis-Images, die beide Architekturen unterstützen.
> Das Image, das Sie für Ihre Funktion erstellen, muss nur auf eine der Architekturen abzielen.

Für die Paketierung und Bereitstellung von Funktionen als Container-Images fallen keine zusätzlichen Kosten an. Wenn eine Funktion aufgerufen wird, die als Container-Image bereitgestellt wird, zahlen

Sie für Aufrufanforderungen und die Ausführungsdauer. Es fallen Gebühren für die Speicherung Ihrer Container-Images in Amazon ECR an. Weitere Informationen finden Sie unter Amazon ECR-Preise.

Image-Sicherheit

Wenn Lambda das Container-Image zum ersten Mal von seiner ursprünglichen Quelle (Amazon ECR) herunterlädt, wird das Container-Image mit authentifizierten konvergenten Verschlüsselungsmethoden optimiert, verschlüsselt und gespeichert. Alle Schlüssel, die zur Entschlüsselung von Kundendaten erforderlich sind, werden durch vom AWS KMS Kunden verwaltete Schlüssel geschützt. Um die Nutzung der von Kunden verwalteten Schlüssel von Lambda zu verfolgen und zu prüfen, können Sie die AWS CloudTrail -Protokolle anzeigen.

Bereitstellen von Lambda-Funktionen als ZIP-Dateiarchive

Wenn Sie eine Lambda-Funktion erstellen, verpacken Sie Ihren Funktionscode in einem Bereitstellungspaket. Lambda unterstützt zwei Arten von Bereitstellungspaketen: Container-Images und .zip-Archive. Der Workflow zum Erstellen einer Funktion hängt vom Typ des Bereitstellungspakets ab. Zur Konfiguration einer Funktion, die als Container-Image definiert ist, siehe the section called “Container-Images”.

Sie können die Lambda-Konsole und die Lambda-API verwenden, um eine mit einem ZIP-Dateiarchiv definierte Funktion zu erstellen. Sie können auch eine aktualisierte ZIP-Datei uploaden, um den Funktionscode zu ändern.

> **Note**
>
> Sie können den Bereitstellungspakettyp (ZIP- oder Container-Image) für eine vorhandene Funktion nicht ändern. Beispielsweise können Sie eine Container-Image-Funktion nicht konvertieren, um ein ZIP-Dateiarchiv zu verwenden. Sie müssen eine neue Funktion erstellen.

Themen

Erstellen der Funktion

Wenn Sie eine Funktion erstellen, die mit einem ZIP-Dateiarchiv definiert ist, wählen Sie eine Codevorlage, die Sprachversion und die Ausführungsrolle für die Funktion aus. Sie fügen Ihren Funktionscode hinzu, nachdem Lambda die Funktion erstellt hat.

So erstellen Sie die Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Wählen Sie Von Grund auf neu erstellen oder Vorlage verwenden, um Ihre Funktion zu erstellen.
4. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie für Funktionsname den Funktionsnamen ein. Funktionsnamen sind auf eine Länge von 64 Zeichen beschränkt.
   b. Wählen Sie für Laufzeit die Sprachversion aus, die für Ihre Funktion verwendet werden soll.
   c. (Optional) Für-Architekturwählen Sie die Befehlssatz-Architektur aus, die für Ihre Funktion verwendet werden soll. Die Standardarchitektur ist x86_64. Stellen Sie beim Erstellen des Bereitstellungspakets für Ihre Funktion sicher, dass es damit kompatibel istBefehlssatz-Architekturaus.
5. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
6. (Optional) Erweitern Sie den Abschnitt Advanced Settings (Erweiterte Einstellungen). Sie können eine Codesignatur-Konfiguration für die Funktion wählen. Sie können auch eine (Amazon VPC) für die Funktion konfigurieren, auf die zugegriffen werden soll.
7. Wählen Sie Funktion erstellen.

Lambda erstellt die neue Funktion. Sie können nun die Konsole verwenden, um den Funktionscode hinzuzufügen und andere Funktionsparameter und -funktionen zu konfigurieren. Anweisungen zur Codebereitstellung finden Sie auf der Handler-Seite für die Laufzeit, die Ihre Funktion verwendet.

Node.js

Bereitstellen von Node.js Lambda-Funktionen mit ZIP-Dateiarchiven

Python

Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen

Ruby

Arbeiten mit ZIP-Dateiarchiven für Ruby-Lambda-Funktionen

Java

Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven

Go

Bereitstellen von Lambda-Go-Funktionen mit ZIP-Dateiarchiven

C#

Erstellen und Bereitstellen von C#-Lambda-Funktionen mit ZIP-Dateiarchiven

PowerShell

Bereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven

Verwenden des Konsolencode-Editors

Die Konsole erstellt eine Lambda-Funktion mit einer einzigen Quelldatei. Bei Skriptsprachen können Sie diese Datei bearbeiten und mit dem integrierten Code-Editor weitere Dateien hinzufügen. Klicken Sie auf Save (Speichern), um die Änderungen zu speichern. Um Ihren Code auszuführen, wählen Sie Test.

> **Note**
>
> Die Lambda-Konsole verwendet AWS Cloud9 , um eine integrierte Entwicklungsumgebung im Browser bereitzustellen. Sie können auch verwenden AWS Cloud9 , um Lambda-Funktionen in Ihrer eigenen Umgebung zu entwickeln. Weitere Informationen finden Sie unter Arbeiten mit - AWS Lambda Funktionen mithilfe der AWS Toolkit im AWS Cloud9 -Benutzerhandbuch.

Wenn Sie Ihren Funktionscode speichern, erstellt die Lambda-Konsole ein Bereitstellungspaket für das ZIP-Dateiarchiv. Wenn Sie Ihren Funktionscode außerhalb der Konsole (mit einer IDE) entwickeln, müssen Sie ein Bereitstellungspaket erstellen, um Ihren Code in die Lambda-Funktion hochzuladen.

Aktualisieren des Funktionscodes

Bei Skriptsprachen (Node.js, Python und Ruby) können Sie Ihren Funktionscode im eingebetteten Code-Editor bearbeiten. Wenn der Code größer als 3 MB ist, oder wenn Sie Bibliotheken hinzufügen müssen, oder für Sprachen, die der Editor nicht unterstützt (Java, Go, C#), müssen Sie Ihren Funktionscode als .zip-Archiv uploaden. Wenn das ZIP-Dateiarchiv kleiner als 50 MB ist, können Sie das ZIP-Dateiarchiv von Ihrem lokalen Computer uploaden. Wenn die Datei größer als 50 MB ist, müssen Sie die Datei aus einem Amazon S3-Bucket in die Funktion uploaden.

So können Sie den Funktionscode als .zip-Archiv uploaden

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die zu aktualisierende Funktion aus und wählen Sie die Code-Registerkarte.
3. Wählen Sie unter Codequelle die Option Upload von aus.
4. Wählen Sie .zip-Datei und dann Hochladen.
   - Wählen Sie in der Dateiauswahl die neue Image-Version aus, wählen Sie Öffnen und dann Speichern.
5. (Alternative zu Schritt 4) Wählen Sie den Amazon-S3-Standort.
   - Geben Sie in das Textfeld die S3-Link-URL des ZIP-Dateiarchivs ein und wählen Sie dann Speichern.

Ändern der Laufzeit

Wenn Sie die Funktionskonfiguration aktualisieren, um eine neue Laufzeit zu verwenden, müssen Sie möglicherweise den Funktionscode aktualisieren, damit dieser mit der neuen Laufzeit kompatibel ist. Wenn Sie die Funktionskonfiguration aktualisieren, um eine andere Laufzeit zu verwenden,mussstellen Sie neuen Funktionscode bereit, der mit Laufzeit und Architektur kompatibel ist. Anweisungen zum Erstellen eines Bereitstellungspakets für den Funktionscode finden Sie auf der Handler-Seite für die Laufzeit, die die Funktion verwendet.

So ändern Sie die Laufzeit

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die zu aktualisierende Funktion aus und wählen Sie die Code-Registerkarte.
3. Blättern Sie nach unten bis zum Abschnitt Laufzeiteinstellungen, der sich unter dem Code-Editor befindet.
4. Wählen Sie Bearbeiten aus.
   a. Wählen Sie für Runtime (Laufzeit) die Laufzeit-ID aus.
   b. Geben Sie im Feld Handler den Dateinamen und en Handler für die Funktion ein.
   c. Für-Architekturwählen Sie die Befehlssatz-Architektur aus, die für Ihre Funktion verwendet werden soll.
5. Wählen Sie Speichern.

Ändern der Architektur

Bevor Sie die Befehlssatzarchitektur ändern können, müssen Sie sicherstellen, dass der Code Ihrer Funktion mit der Zielarchitektur kompatibel ist.

Wenn Sie Node.js, Python oder Ruby verwenden und Ihren Funktionscode im eingebettetenEditorkann der vorhandene Code ohne Änderung ausgeführt werden.

Wenn Sie jedoch Ihren Funktionscode mithilfe eines Bereitstellungspakets im ZIP-Dateiarchiv angeben, müssen Sie ein neues ZIP-Dateiarchiv vorbereiten, das korrekt für die Ziel-Laufzeit- und Anleitungssatz-Architektur kompiliert und erstellt wird. Anweisungen dazu finden Sie auf der Handler-Seite für Ihre Funktions-Laufzeit.

So ändern Sie die Befehlssatz-Architektur

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die zu aktualisierende Funktion aus und wählen Sie die Code-Registerkarte.
3. Wählen Sie unter Laufzeiteinstellungen die Option Bearbeiten.
4. Für-Architekturwählen Sie die Befehlssatz-Architektur aus, die für Ihre Funktion verwendet werden soll.
5. Wählen Sie Save aus.

Verwenden der Lambda-API

Um eine Funktion zu erstellen und zu konfigurieren, die ein ZIP-Dateiarchiv verwendet, verwenden Sie die folgenden API-Operationen:

- CreateFunction
- UpdateFunctionCode
- UpdateFunctionConfiguration

AWS CloudFormation

Sie können verwenden AWS CloudFormation , um eine Lambda-Funktion zu erstellen, die ein ZIP-Dateiarchiv verwendet. In Ihrer AWS CloudFormation Vorlage gibt die `AWS::Lambda::Function` Ressource die Lambda-Funktion an. Beschreibungen der Eigenschaften

in der `AWS::Lambda::Function` Ressource finden Sie unter AWS::Lambda::Function im AWS CloudFormation -Benutzerhandbuch.

Legen Sie in der `AWS::Lambda::Function`-Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als Zip-Datei-Archiv definiert ist:

- AWS::Lambda::Function
  - PackageType – Setzen Sie auf `Zip`.
  - Code – Geben Sie den Namen des Amazon-S3-Buckets und den ZIP-Dateinamen in die Textfelder `S3Bucket` und `S3Key`. Für Node.js oder Python können Sie Inline-Quellcode Ihrer Lambda-Funktion bereitstellen.
  - Laufzeit – Legt den Laufzeitwert fest.
  - Architektur – Legen Sie den Architekturwert auf fest`arm64`, um den AWS Graviton2-Prozessor zu verwenden. Der Standardwert ist`x86_64`aus.

Erstellen Sie eine Lambda-Funktion mit einem Container-Image

Der Code Ihrer AWS Lambda Funktion besteht aus Skripten oder kompilierten Programmen und deren Abhängigkeiten. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Lambda unterstützt zwei Arten von Bereitstellungspaketen: Container-Images und ZIP-Dateiarchiven.

Es gibt drei Möglichkeiten, ein Container-Image für eine Lambda-Funktion zu erstellen:

- Verwenden eines AWS Basis-Images für Lambda

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.

- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ihre Sprache in das Image aufnehmen.

- Verwenden Sie ein Nicht-Base-Image AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ihre Sprache in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Um eine Lambda-Funktion aus einem Container-Image zu erstellen, erstellen Sie Ihr Image lokal und laden es in ein Amazon Elastic Container Registry (Amazon ECR)-Repository hoch. Geben Sie dann den Repository-URI an, wenn Sie die Funktion erstellen. Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden. Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

Auf dieser Seite werden die Basis-Image-Typen und Anforderungen für die Erstellung von Lambda-kompatiblen Container-Images erläutert.

> **Note**
>
> Sie können den Bereitstellungspakettyp (.zip oder Container-Image) für eine bestehende Funktion nicht ändern. Sie können beispielsweise eine Container-Image-Funktion nicht so konvertieren, dass sie ein ZIP-Dateiarchiv verwendet. Sie müssen eine neue Funktion erstellen.

Themen

Voraussetzungen

Installieren Sie die AWS Command Line Interface (AWS CLI) Version 2 und die Docker-CLI. Beachten Sie außerdem die folgenden Anforderungen:

- Das Container-Image muss die Lambda-Laufzeiten-API implementieren. Die AWS Open-Source-Laufzeitschnittstellen-Clients implementieren die API. Sie können Ihrem bevorzugten Basis-Image einen Laufzeitschnittstellen-Client hinzufügen, damit es mit Lambda kompatibel ist.

- Das Container-Image muss auf einem schreibgeschützten Dateisystem laufen können. Ihr Funktionscode kann auf ein beschreibbares `/tmp`-Verzeichnis mit einem Speicherplatz zwischen 512 MB bis 10 240 MB, in 1-MB-Schritten, zugreifen.
- Der Lambda-Standardbenutzer muss in der Lage sein, alle Dateien zu lesen, die zum Ausführen Ihres Funktionscodes erforderlich sind. Lambda folgt den bewährten Methoden für die Sicherheit, indem es einen Standard-Linux-Benutzer mit den geringsten Berechtigungen definiert. Stellen Sie sicher, dass Ihr Anwendungscode nicht auf Dateien angewiesen ist, von denen andere Linux-Benutzer nicht ausgeführt werden können.
- Lambda unterstützt nur Linux-basierte Container-Images.
- Lambda bietet Multi-Architektur-Basis-Images. Das Image, das Sie für Ihre Funktion erstellen, muss jedoch nur auf eine der Architekturen abzielen. Lambda unterstützt keine Funktionen, die Container-Images mit mehreren Architekturen verwenden.

Verwenden eines AWS Basis-Images für Lambda

Sie können eines der AWS -Basis-Images für Lambda verwenden, um das Container-Image für Ihren Funktionscode zu erstellen. Die Basis-Images sind mit einer Sprachlaufzeit und anderen Komponenten vorgeladen, die zum Ausführen eines Container-Images in Lambda erforderlich sind. Sie fügen Ihren Funktionscode und Ihre Abhängigkeiten dem Basis-Image hinzu und verpacken es dann als Container-Image.

AWS stellt regelmäßig Updates für die AWS Basis-Images für Lambda bereit. Wenn Ihr Dockerfile den Image-Namen in der FROM-Eigenschaft enthält, ruft Ihr Docker-Client die aktuelle Version des Images aus dem Amazon-ECR-Repository ab.. Um das aktualisierte Basis-Image verwenden zu können, müssen Sie Ihr Container-Image neu erstellen und den Funktionscode aktualisieren.

Die Basis-Images Node.js 20, Python 3.12, Java 21, AL2023 und höher basieren auf dem minimalen Container-Image von Amazon Linux 2023. Frühere Basis-Images verwenden Amazon Linux 2. AL2023 bietet mehrere Vorteile gegenüber Amazon Linux 2, darunter einen geringeren Bereitstellungsaufwand und aktualisierte Versionen von Bibliotheken wie `glibc`.

AL2023-basierte Images verwenden `microdnf` (symbolisiert als`dnf`) als Paketmanager anstelle von`yum`, dem Standard-Paketmanager in Amazon Linux 2. `microdnf`ist eine eigenständige Implementierung von. `dnf` Eine Liste der Pakete, die in AL2023-basierten Images enthalten sind, finden Sie in den Spalten Minimal Container unter Comparing packages installed on Amazon Linux 2023 Container Images. Weitere Informationen zu den Unterschieden zwischen AL2023 und Amazon

Linux 2 finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.

> **Note**
>
> Um AL2023-basierte Images lokal auszuführen, auch mit AWS Serverless Application Model (AWS SAM), müssen Sie Docker-Version 20.10.10 oder höher verwenden.

Um ein Container-Image mit einem AWS Basis-Image zu erstellen, wählen Sie die Anweisungen für Ihre bevorzugte Sprache aus:

- Node.js
- TypeScript(verwendet ein Node.js -Basisimage)
- Python
- Java
- Go
- .NET
- Ruby

Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ihre Sprache in das Image aufnehmen.

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
al2023	Reine OS-Laufzeit	Amazon Linux 2023	Dockerfile für reine Betriebssystem-Runtime on GitHub	

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
al2	Reine OS-Laufzeit	Amazon Linux 2	Dockerfile für Runtime nur für Betriebssystem aktiviert GitHub	

Öffentliche Galerie der Registry von Amazon Elastic Container: gallery.ecr.aws/lambda/provided

Verwenden Sie ein Nicht-Base-Image AWS

Lambda unterstützt jedes Image, das einem der folgenden Image-Manifestformate entspricht:

- Docker Image Manifest V2 Schema 2 (mit Docker-Version 1.10 und neuer)
- Open Container Initiative (OCI)-Spezifikationen (v1.0.0 und höher)

Lambda unterstützt eine maximale unkomprimierte Image-Größe von 10 GB, einschließlich aller Ebenen.

> **Note**
>
> Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ihre Sprache in das Image aufnehmen.

Laufzeitschnittstellen-Clients

Wenn Sie ein reines OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Runtime-Schnittstellenclient muss den erweiternLambda-Laufzeiten-API, der die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet. AWS stellt Open-Source-Runtime-Interface-Clients für die folgenden Sprachen bereit:

- Node.js
- Python
- Java
- .NET

- Go
- Ruby
- Rust – Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Wenn Sie eine Sprache verwenden, für die kein AWS Runtime-Interface-Client zur Verfügung steht, müssen Sie Ihren eigenen erstellen.

Amazon-ECR-Berechtigungen

Bevor Sie eine Lambda-Funktion aus einem Container-Image erstellen, müssen Sie das Image lokal erstellen und es in ein Amazon-ECR-Repository hochladen. Geben Sie beim Erstellen der Funktion den URI des Amazon-ECR-Repositorys an.

Stellen Sie sicher, dass die Berechtigungen für den Benutzer oder die Rolle, die die Funktion erstellt, `GetRepositoryPolicy` und `SetRepositoryPolicy` enthalten.

Verwenden Sie beispielsweise die IAM-Konsole, um eine Rolle mit der folgenden Richtlinie zu erstellen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
      ],
      "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world"
    }
  ]
}
```

Richtlinien für das Amazon-ECR-Repository

Für eine Funktion im selben Konto wie das Container-Image in Amazon ECR können Sie Ihrem Amazon-ECR-Repository die Berechtigungen `ecr:BatchGetImage` und `ecr:GetDownloadUrlForLayer` hinzufügen. Das folgende Beispiel zeigt die Mindestrichtlinie:

```
{
        "Sid": "LambdaECRImageRetrievalPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lambda.amazonaws.com"
        },
        "Action": [
          "ecr:BatchGetImage",
          "ecr:GetDownloadUrlForLayer"
        ]
    }
```

Weitere Informationen zu Amazon-ECR-Repository-Berechtigungen finden Sie unter Private Repository-Richtlinien im Benutzerhandbuch zu Amazon Elastic Container Registry.

Wenn das Amazon ECR-Repository diese Berechtigungen nicht enthält, fügt Lambda `ecr:BatchGetImage` und `ecr:GetDownloadUrlForLayer` zu den Berechtigungen des Container-Image-Repositorys hinzu. Lambda kann diese Berechtigungen nur hinzufügen, wenn der Lambda aufrufende Prinzipal über `ecr:getRepositoryPolicy`- und `ecr:setRepositoryPolicy`-Berechtigungen verfügt.

Um Ihre Repository-Berechtigungen für Amazon ECR anzuzeigen oder zu bearbeiten, befolgen Sie die Anweisungen unter Festlegung einer privaten Repository-Richtlinienanweisung im Benutzerhandbuch zu Amazon Elastic Container Registry.

Kontoübergreifende Berechtigungen von Amazon ECR

Ein anderes Konto in derselben Region kann eine Funktion erstellen, die ein Container-Image verwendet, das Ihrem Konto gehört. Im folgenden Beispiel benötigt die Berechtigungsrichtlinie Ihres Amazon-ECR-Repository die folgenden Anweisungen, um den Zugriff auf Kontonummer 123456789012 zu gewähren.

- CrossAccountBerechtigung — Ermöglicht dem Konto 123456789012 das Erstellen und Aktualisieren von Lambda-Funktionen, die Bilder aus diesem ECR-Repository verwenden.
- ImageCrossAccountRetrievalLambdaECR-Richtlinie — Lambda setzt den Status einer Funktion irgendwann auf inaktiv, wenn sie über einen längeren Zeitraum nicht aufgerufen wird. Diese Anweisung ist erforderlich, damit Lambda das Container-Image zur Optimierung und Zwischenspeicherung im Namen der Funktion abrufen kann, die 123456789012 besitzt.

Example – Ihrem Repository kontoübergreifende Berechtigungen hinzufügen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountPermission",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      }
    },
    {
      "Sid": "LambdaECRImageCrossAccountRetrievalPolicy",
      "Effect": "Allow",
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ],
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Condition": {
        "StringLike": {
          "aws:sourceARN": "arn:aws:lambda:us-east-1:123456789012:function:*"
        }
      }
    }
  ]
}
```

Um den Zugriff auf mehrere Konten zu gewähren, fügen Sie die Konto-IDs der Liste der Prinzipalen in der `CrossAccountPermission`-Richtlinie hinzu sowie zur Bedingungs-Auswertungsliste der Bedingung in `LambdaECRImageCrossAccountRetrievalPolicy`.

Wenn Sie mit mehreren Konten in einer AWS Organisation arbeiten, empfehlen wir, dass Sie jede Konto-ID in der ECR-Berechtigungsrichtlinie auflisten. Dieser Ansatz entspricht der bewährten AWS Sicherheitsmethode, enge Berechtigungen in IAM-Richtlinien festzulegen.

Zusätzlich zu den Lambda-Berechtigungen muss der Benutzer oder die Rolle, die die Funktion erstellt, auch über `GetDownloadUrlForLayer` Berechtigungen verfügen`BatchGetImage`.

Lebenszyklus der Funktion

Nachdem Sie ein neues oder aktualisiertes Container-Image hochgeladen haben, optimiert Lambda das Image, bevor die Funktion Aufrufe verarbeiten kann. Der Optimierungsprozess kann einige Sekunden dauern. Die Funktion bleibt bis zum Abschluss des Vorgangs im `Pending`-Zustand. Die Funktion wechselt dann in den `Active`-Zustand. Während der Zustand `Pending` ist, können Sie die Funktion zwar aufrufen, allerdings schlagen andere Operationen für die Funktion fehl. Aufrufe, die auftreten, während eine Image-Aktualisierung läuft, führen den Code aus dem vorherigen Image aus.

Wenn eine Funktion mehrere Wochen lang nicht aufgerufen wird, gewinnt Lambda seine optimierte Version zurück und die Funktion wechselt in den `Inactive`-Zustand. Um die Funktion wieder zu aktivieren, müssen Sie sie aufrufen. Lambda lehnt den ersten Aufruf ab und die Funktion tritt in den `Pending`-Zustand, bis Lambda das Image neu optimiert. Die Funktion kehrt dann zum `Active`-Zustand zurück.

Lambda ruft regelmäßig das zugehörige Container-Image aus dem Amazon ECR-Repository ab. Wenn das entsprechende Container-Image in Amazon ECR nicht mehr vorhanden ist oder Berechtigungen widerrufen werden, wechselt die Funktion in den `Failed`-Zustand und Lambda gibt einen Fehler für alle Funktionsaufrufe zurück.

Sie können die Lambda-API verwenden, um Informationen über den Zustand einer Funktion abzurufen. Weitere Informationen finden Sie unter Lambda-Funktionszustände.

Grundlegendes zu Methoden zum Aufrufen von Lambda-Funktionen

Nachdem Sie Ihre Lambda-Funktion bereitgestellt haben, können Sie sie auf verschiedene Arten aufrufen:

- Die Lambda-Konsole — Verwenden Sie die Lambda-Konsole, um schnell ein Testereignis zu erstellen, um Ihre Funktion aufzurufen.
- Das AWS SDK — Verwenden Sie das AWS SDK, um Ihre Funktion programmgesteuert aufzurufen.
- Die Invoke API — Verwenden Sie die Lambda Invoke-API, um Ihre Funktion direkt aufzurufen.
- The AWS Command Line Interface (AWS CLI) — Verwenden Sie den `aws lambda invoke` AWS CLI Befehl, um Ihre Funktion direkt von der Befehlszeile aus aufzurufen.
- Ein Funktions-URL-HTTP (S) -Endpunkt — Verwenden Sie Funktions-URLs, um einen dedizierten HTTP (S) -Endpunkt zu erstellen, mit dem Sie Ihre Funktion aufrufen können.

All diese Methoden sind direkte Möglichkeiten, Ihre Funktion aufzurufen. In Lambda besteht ein häufiger Anwendungsfall darin, Ihre Funktion auf der Grundlage eines Ereignisses aufzurufen, das an anderer Stelle in Ihrer Anwendung auftritt. Einige Dienste können bei jedem neuen Ereignis eine Lambda-Funktion aufrufen. Dies wird als Trigger bezeichnet. Für stream- und warteschlangenbasierte Dienste ruft Lambda die Funktion mit Batches von Datensätzen auf. Dies wird als Ereignisquellen-Mapping bezeichnet.

Wenn Sie eine Funktion aufrufen, können Sie bestimmen, ob sie synchron oder asynchron aufgerufen wird. Bei einem synchronen Aufruf warten Sie, bis die Funktion das Ereignis verarbeitet und eine Antwort zurückgegeben hat. Bei einem asynchronen Aufruf stellt Lambda das Ereignis für die Verarbeitung in eine Warteschlangen und gibt umgehend eine Antwort zurück. Der `InvocationType`Anforderungsparameter in der Invoke-API bestimmt, wie Lambda Ihre Funktion aufruft. Der Wert von `RequestResponse` steht für einen synchronen Aufruf und der Wert von steht für einen asynchronen Aufruf. `Event`

Wenn der Funktionsaufruf zu einem Fehler führt, sehen Sie sich bei synchronen Aufrufen die Fehlermeldung in der Antwort an und wiederholen Sie den Aufruf manuell. Bei asynchronen Aufrufen verarbeitet Lambda Wiederholungsversuche automatisch und kann Aufrufdatensätze an ein Ziel senden.

Synchroner Aufruf

Wenn Sie eine Funktion synchron aufrufen, führt Lambda die Funktion aus und wartet auf eine Antwort. Wenn der Funktionsaufruf beendet ist, gibt Lambda die Antwort aus dem Funktionscode mit zusätzlichen Daten, wie z. B. der Version der aufgerufenen Funktion, zurück. Wenn Sie eine Funktion mithilfe der AWS CLI synchron ausführen möchten, verwenden Sie den Befehl `invoke`.

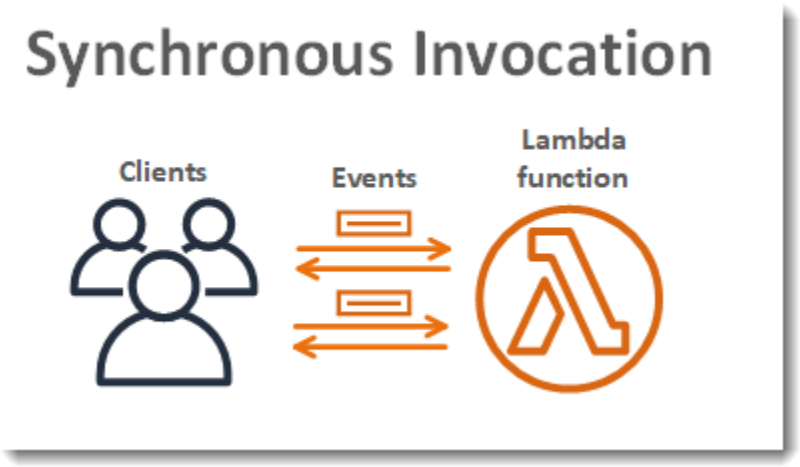
```
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{ "key": "value" }' response.json
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "ExecutedVersion": "$LATEST",
    "StatusCode": 200
}
```

Das folgende Diagramm zeigt Clients, die eine Lambda-Funktion synchron aufrufen. Lambda sendet die Ereignisse direkt an die Funktion und sendet die Antwort der Funktion zurück an den Aufrufer.



`payload` ist eine Zeichenfolge, die ein Ereignis im JSON-Format enthält. Der Name der Datei, in die die AWS CLI die Antwort von der Funktion schreibt, lautet `response.json`. Wenn die Funktion ein

Objekt oder einen Fehler zurückgibt, ist der Antworttext das Objekt oder der Fehler im JSON-Format. Wenn die Funktion fehlerfrei beendet wird, lautet der Antworttext `null`.

> **Note**
>
> Lambda wartet nicht, bis externe Erweiterungen abgeschlossen sind, bevor die Antwort gesendet wird. Externe Erweiterungen werden als unabhängige Prozesse in der Ausführungsumgebung ausgeführt und laufen auch nach Abschluss des Funktionsaufrufs weiter. Weitere Informationen finden Sie unter Erweitern Sie Lambda-Funktionen mithilfe von Lambda-Erweiterungen.

Die Ausgabe des Befehls, die im Terminal angezeigt wird, enthält Informationen aus Headern in der Antwort von Lambda. Dies umfasst die Version, von der das Ereignis verarbeitet wurde (nützlich bei der Verwendung von Aliassen) und den von Lambda zurückgegebenen Statuscode. Wenn Lambda die Funktion ausführen konnte, lautet der Statuscode 200, auch wenn die Funktion einen Fehler zurückgegeben hat.

> **Note**
>
> Bei Funktionen mit einem langen Timeout wird Ihr Client während eines synchronen Aufrufs möglicherweise getrennt, während er auf eine Antwort wartet. Konfigurieren Sie HTTP-Client, SDK, Firewall, Proxy oder Betriebssystem so, dass lange Verbindungen mit Timeout- oder Keepalive-Einstellungen möglich sind.

Wenn Lambda die Funktion nicht ausführen kann, wird der Fehler in der Ausgabe angezeigt.

```
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload value response.json
```

Die Ausgabe sollte folgendermaßen aussehen:

```
An error occurred (InvalidRequestContentException) when calling the Invoke operation:
 Could not parse request body into json: Unrecognized token 'value': was expecting
 ('true', 'false' or 'null')
 at [Source: (byte[])"value"; line: 1, column: 11]
```

Die AWS CLI ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit den AWS-Services interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI – Schnellkonfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-`

`in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Weitere Informationen über die `Invoke`-API, einschließlich einer vollständigen Liste von Parametern, Kopfzeilen und Fehlern, finden Sie unter Aufrufen.

Wenn Sie eine Funktion direkt aufrufen, können Sie die Antwort auf Fehler überprüfen und es erneut versuchen. Die AWS CLI- und das AWS SDK unternehmen zudem automatisch einen Wiederholversuch bei Client-Zeitbeschränkungen, Drosselung und Service-Fehlern. Weitere Informationen finden Sie unter Grundlegendes zum Wiederholungsverhalten in Lambda.

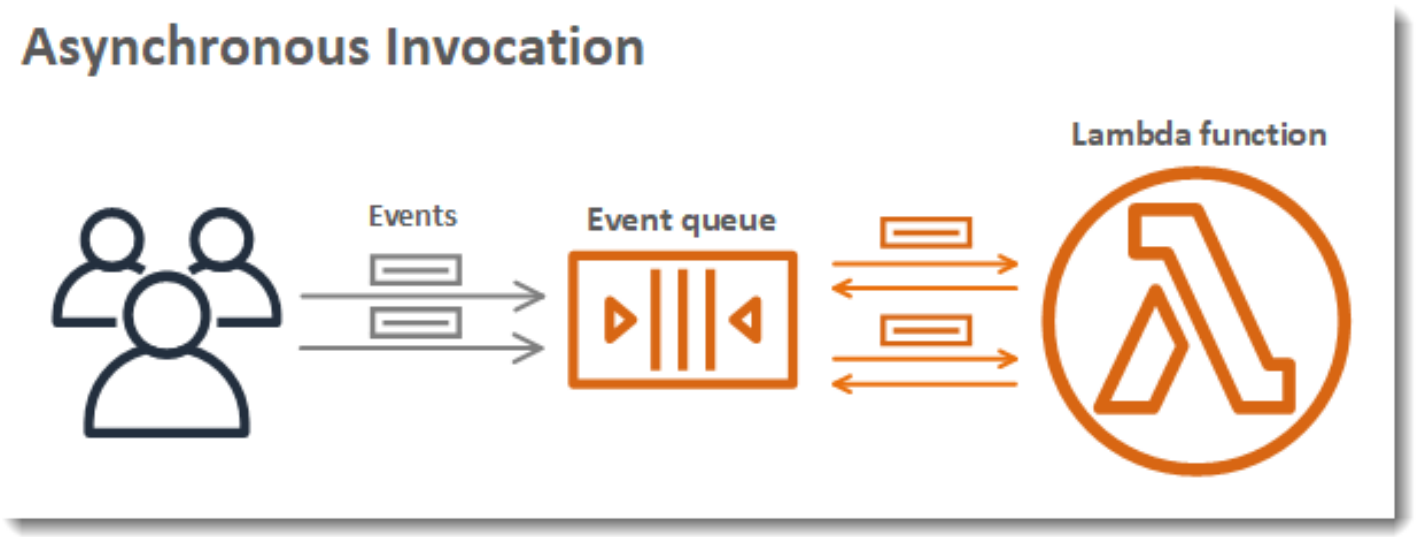
Asynchroner Aufruf

Einige AWS-Services, wie Amazon Simple Storage Service (Amazon S3) und Amazon Simple Notification Service (Amazon SNS), rufen Funktionen asynchron auf, um Ereignisse zu verarbeiten. Wenn Sie eine Funktion asynchron aufrufen, warten Sie nicht auf eine Antwort aus dem Funktionscode. Sie übergeben das Ereignis an Lambda und Lambda erledigt den Rest. Sie können konfigurieren, wie Lambda mit Fehlern umgeht, und Aufrufdatensätze an eine nachgelagerte Ressource wie Amazon Simple Queue Service (Amazon SQS) oder Amazon EventBridge (EventBridge) senden, um Komponenten Ihrer Anwendung miteinander zu verketten.

Sections

Wie Lambda asynchrone Aufrufe verarbeitet

Das folgende Diagramm zeigt Clients, die eine Lambda-Funktion asynchron aufrufen. Lambda stellt die Ereignisse in eine Warteschlange, bevor sie an die Funktion gesendet werden.



Lambda platziert das Ereignis bei asynchronem Aufruf in eine Warteschlange und gibt eine Erfolgsantwort ohne zusätzliche Informationen zurück. Ein separater Prozess liest Ereignisse aus der

Warteschlange und senden sie zu Ihrer Funktion. Um eine Funktion asynchron aufzurufen, stellen Sie den Parameter des Aufrufstyps auf ei `Event`.

```
aws lambda invoke \
  --function-name my-function  \
  --invocation-type Event \
  --cli-binary-format raw-in-base64-out \
  --payload '{ "key": "value" }' response.json
```

Die cli-binary-format Option ist erforderlich, wenn Sie Version 2 verwenden AWS CLI . Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
{
    "StatusCode": 202
}
```

Die Ausgabedatei (`response.json`) enthält keine Informationen, wird bei der Ausführung dieses Befehls aber dennoch erstellt. Wenn Lambda das Ereignis nicht zur Warteschlange hinzufügen kann, erscheint in der Befehlsausgabe eine Fehlermeldung.

Lambda verwaltet die asynchrone Ereigniswarteschlange der Funktion und unternimmt bei Fehlern Wiederholungsversuche. Wenn die Funktion einen Fehler zurückgibt, versucht Lambda zwei weitere Male, sie auszuführen. Dabei wird eine Minute lang zwischen den ersten zwei Versuchen und zwei Minuten lang zwischen dem zweiten und dem dritten Versuch gewartet. Zu Funktionsfehlern gehören Fehler, die vom Code der Funktion zurückgegeben werden, sowie Fehler, die von der Laufzeit des Fehlers zurückgegeben werden, wie z. B. Timeouts.

Wenn für die Funktion nicht genügend Gleichzeitigkeit für die Verarbeitung aller Ereignisse verfügbar ist, werden weitere Anforderungen gedrosselt. Bei Drosselungsfehlern (429) und Systemfehlern (500-Serie) sendet Lambda das Ereignis zur Warteschlange zurück und versucht bis zu 6 Stunden lang, die Funktion erneut auszuführen. Das Wiederholungsintervall erhöht sich exponentiell von 1 Sekunde nach dem ersten Versuch auf maximal 5 Minuten. Lambda stellt viele Einträge in die Warteschlange, erhöht das Wiederholungsintervall und reduziert die Rate, mit der es Ereignisse aus der Warteschlange liest.

Selbst wenn Ihre Funktion keinen Fehler zurückgibt, ist es möglich, dass sie dasselbe Ereignis mehrmals von Lambda erhält, da die Warteschlange selbst „letztendliche Konsistenz“ ist. Wenn die

Funktion mit eingehenden Ereignissen nicht Schritt halten kann, kann es auch vorkommen, dass Ereignisse aus der Warteschlange gelöscht werden, ohne zur Funktion gesendet zu werden. Stellen Sie sicher, dass Ihr Funktionscode doppelte Ereignisse ordnungsgemäß verarbeitet und dass Sie über genügend Gleichzeitigkeit zur Verarbeitung aller Aufrufe verfügen.

Wenn die Warteschlange sehr lang ist, können neue Ereignisse veraltet sein, bevor Lambda sie an Ihre Funktion senden kann. Wenn ein Ereignis abläuft oder bei ihm alle Verarbeitungsversuche fehlschlagen, wird es von Lambda verworfen. Sie können die Fehlerbehandlung für eine Funktion konfigurieren, um die Anzahl der Wiederholungsversuche zu reduzieren, die Lambda durchführt, oder um unverarbeitete Ereignisse schneller zu verwerfen.

Sie können Lambda auch so konfigurieren, dass ein Aufrufdatensatz an einen anderen Service gesendet wird. Lambda unterstützt die folgenden Ziele für den asynchronen Aufruf. Beachten Sie, dass SQS-FIFO-Warteschlangen und SNS-FIFO-Themen nicht unterstützt werden.

- Amazon SQS – Eine standardmäßige SQS-Warteschlange.
- Amazon SNS – Ein SNS-Standardthema.
- AWS Lambda – Eine Lambda-Funktion.
- Amazon EventBridge — Ein EventBridge Eventbus.

Der Aufrufdatensatz enthält Details zur Anforderung und Antwort im JSON-Format. Sie können separate Ziele für Ereignisse konfigurieren, die erfolgreich verarbeitet werden, und für Ereignisse, bei denen alle Verarbeitungsversuche fehlschlagen. Alternativ können Sie eine Amazon-SQS-Standardwarteschlange oder ein Amazon-SNS-Standardthema als Warteschlange für unzustellbare Nachrichten für verworfene Ereignisse konfigurieren. Für Warteschlangen für unzustellbare Nachrichten sendet Lambda nur den Inhalt des Ereignisses ohne Details zur Antwort.

Wenn Lambda einen Datensatz nicht an ein von Ihnen konfiguriertes Ziel senden kann, sendet es eine `DestinationDeliveryFailures` Metrik an Amazon CloudWatch. Dies kann passieren, wenn Ihre Konfiguration einen nicht unterstützten Zieltyp enthält, z. B. eine Amazon-SQS-FIFO-Warteschlange oder ein Amazon-SNS-FIFO-Thema. Zustellungsfehler können auch aufgrund von Berechtigungsfehlern und Größenbeschränkungen auftreten. Weitere Informationen zu Lambda-Aufrufmetriken finden Sie unter Aufrufmetriken.

> **Note**
>
> Um zu verhindern, dass eine Funktion ausgelöst wird, können Sie die reservierte Parallelität der Funktion auf Null setzen. Wenn Sie die reservierte Parallelität für eine

asynchron aufgerufene Funktion auf Null setzen, sendet Lambda sofort und ohne Wiederholungsversuche alle Ereignisse ohne erneute Versuche an die konfigurierte Warteschlange für unzustellbare Nachrichten oder an das Ereignisziel bei Fehlern. Um Ereignisse zu verarbeiten, die gesendet wurden, während die reservierte Parallelität auf Null gesetzt war, müssen Sie die Ereignisse aus der Warteschlange für unzustellbare Nachrichten oder dem Ereignisziel bei Fehlern verarbeiten.

Konfigurieren der Fehlerbehandlung für den asynchronen Aufruf

Verwenden Sie die Lambda-Konsole, um Einstellungen für die Fehlerbehandlung für eine Funktion, eine Version oder einen Alias zu konfigurieren.

So konfigurieren Sie die Fehlerbehandlung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie „Konfiguration“ und dann „Asynchroner Aufruf“ aus.
4. Wählen Sie unter Asynchronous invocation (Asynchroner Aufruf) die Option Edit (Bearbeiten).
5. Konfigurieren Sie die folgenden Einstellungen.
   - Maximales Alter des Ereignisses – Die maximale Zeitspanne, die Lambda ein Ereignis in der Warteschlange für asynchrone Ereignisse behält (bis zu 6 Stunden).
   - Wiederholversuche – Die Anzahl der Wiederholungen, die Lambda es erneut versucht, wenn die Funktion einen Fehler zurückgibt (zwischen 0 und 2).
6. Wählen Sie Save aus.

Wenn ein Aufrufereignis das maximale Alter überschreitet oder alle Wiederholversuche fehlschlagen, wird es von Lambda verworfen. Um eine Kopie der verworfenen Ereignisse beizubehalten, konfigurieren Sie ein Ziel für fehlgeschlagene Ereignisse.

Konfigurieren von Zielen für den asynchronen Aufruf

Um Datensätze der asynchronen Aufrufe beizubehalten, fügen Sie Ihrer Funktion ein Ziel hinzu. Sie können wählen, ob erfolgreiche Aufrufe oder fehlgeschlagene Aufrufe an ein Ziel gesendet werden sollen. Jede Funktion kann mehrere Ziele haben, sodass Sie separate Ziele für erfolgreiche und fehlgeschlagene Ereignisse konfigurieren können. Jeder Datensatz, der an das Ziel gesendet wird,

ist ein JSON-Dokument mit Details zum Aufruf. Wie Einstellungen zur Fehlerbehandlung können Sie Ziele für eine Funktion, eine Funktionsversion oder einen Alias konfigurieren.

> **Note**
>
> Sie können auch Aufzeichnungen über fehlgeschlagene Aufrufe für die folgenden Typen von Ereignisquellenzuordnungen speichern: Amazon Kinesis, AmazonDynamoDB, selbstverwalteter Apache Kafka und Amazon MSK.

In der folgenden Tabelle werden die unterstützten Ziele für Datensätze der asynchronen Aufrufen aufgelistet. Damit Lambda erfolgreich Datensätze an das von Ihnen ausgewählte Ziel senden kann, stellen Sie sicher, dass die Ausführungsrolle Ihrer Funktion auch die entsprechenden Berechtigungen enthält. In der Tabelle wird auch beschrieben, wie jeder Zieltyp den JSON-Aufrufdatensatz empfängt.

Zieltyp	Erforderliche Berechtigung	Zielspezifisches JSON-Format
Amazon-SQS-Warteschlange	sqs: SendMessage	Lambda übergibt den Aufrufdatensatz als `Message` an das Ziel.
Amazon SNS-Thema	sns:Publish	Lambda übergibt den Aufrufdatensatz als `Message` an das Ziel.
Lambda-Funktion	InvokeFunction	Lambda übergibt den Aufrufdatensatz als Nutzlast in der Funktion.
EventBridge	Ereignisse: PutEvents	• Lambda übergibt den Aufrufdatensatz wie `detail` im PutEvents Aufruf. • Der Wert für das `source`-Ereignisfeld ist `lambda`. • Der Wert für das `detail-type` -Ereignisfeld ist entweder „Lambda Function Invocation Result

Zieltyp	Erforderliche Berechtigung	Zielspezifisches JSON-Format
		– Success“ (Ergebnis des Lambda-Funktionsaufrufs: Erfolgreich) oder „Lambda Function Invocation Result – Failure“ (Ergebnis des Lambda-Funktionsaufrufs: Fehler). • Das `resource`-Ereignis feld enthält die Amazon Resource Names (ARNs) für Funktion und Ziel. • Weitere Veranstaltungsbere iche finden Sie unter EventBridge Amazon-Ve ranstaltungen.

Das folgende Beispiel zeigt einen Aufrufdatensatz für ein Ereignis, bei dem drei Verarbeitungsversuche aufgrund eines Funktionsfehlers fehlgeschlagen sind. Der Aufrufdatensatz enthält Details zum Ereignis, zur Antwort und zu dem Grund, warum der Datensatz gesendet wurde.

```
{
    "version": "1.0",
    "timestamp": "2019-11-14T18:16:05.568Z",
    "requestContext": {
        "requestId": "e4b46cbf-b738-xmpl-8880-a18cdf61200e",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:
$LATEST",
        "condition": "RetriesExhausted",
        "approximateInvokeCount": 3
    },
    "requestPayload": {
        "ORDER_IDS": [
            "9e07af03-ce31-4ff3-xmpl-36dce652cb4f",
            "637de236-e7b2-464e-xmpl-baf57f86bb53",
            "a81ddca6-2c35-45c7-xmpl-c3a03a31ed15"
        ]
    },
```

```
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "responsePayload": {
        "errorMessage": "RequestId: e4b46cbf-b738-xmpl-8880-a18cdf61200e Process exited
 before completing request"
    }
}
```

In den folgenden Schritten wird beschrieben, wie Sie mithilfe der Lambda-Konsole ein Ziel für eine Funktion konfigurieren.

So konfigurieren Sie ein Ziel für Datensätze der asynchronen Aufrufe

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add destination (Ziel hinzufügen).
4. Wählen Sie unter Source (Quelle) die Option Asynchronous invocation (Asynchroner Aufruf).
5. Wählen Sie unter Condition (Bedingung) eine der folgenden Optionen aus:
   - Bei Fehler – Es wird ein Datensatz gesendet, wenn das Ereignis alle Verarbeitungsversuche ausschöpft oder das maximale Alter überschreitet.
   - Bei Erfolg – Es wird ein Datensatz gesendet, wenn die Funktion einen asynchronen Aufruf erfolgreich verarbeitet.
6. Wählen Sie unter Destination type (Zieltyp) den Ressourcentyp aus, der den Aufrufdatensatz empfängt.
7. Wählen Sie unter Destination (Ziel) eine Ressource aus.
8. Wählen Sie Save aus.

Wenn ein Aufruf mit der Bedingung übereinstimmt, sendet Lambda ein JSON-Dokument mit Details zum Aufruf an das Ziel.

Zielspezifisches JSON-Format

- Für Amazon SQS und Amazon SNS (`SnsDestination` und `SqsDestination`) wird der Aufrufdatensatz als `Message` an das Ziel übergeben.
- Für Lambda (`LambdaDestination`) wird der Aufrufdatensatz als Nutzlast an die Funktion übergeben.
- Für EventBridge (`EventBridgeDestination`) wird der Aufrufdatensatz wie `detail` im PutEventsAufruf übergeben. Der Wert für das `source`-Ereignisfeld ist `lambda`. Der Wert für das `detail-type`-Ereignisfeld ist entweder Lambda Function Invocation Result – Success (Ergebnis des Lambda-Funktionsaufrufs: Erfolgreich) oder Lambda Function Invocation Result – Failure (Ergebnis des Lambda-Funktionsaufrufs: Fehler). Das `resource`-Ereignisfeld enthält die Amazon Resource Names (ARNs) für Funktion und Ziel. Weitere Veranstaltungsbereiche finden Sie unter EventBridge Amazon-Veranstaltungen.

Das folgende Beispiel zeigt einen Aufrufdatensatz für ein Ereignis, bei dem drei Verarbeitungsversuche aufgrund eines Funktionsfehlers fehlgeschlagen sind.

Example Aufrufdatensatzglauben

```
{
    "version": "1.0",
    "timestamp": "2019-11-14T18:16:05.568Z",
    "requestContext": {
        "requestId": "e4b46cbf-b738-xmpl-8880-a18cdf61200e",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function:
$LATEST",
        "condition": "RetriesExhausted",
        "approximateInvokeCount": 3
    },
    "requestPayload": {
        "ORDER_IDS": [
            "9e07af03-ce31-4ff3-xmpl-36dce652cb4f",
            "637de236-e7b2-464e-xmpl-baf57f86bb53",
            "a81ddca6-2c35-45c7-xmpl-c3a03a31ed15"
        ]
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
```

```
    },
    "responsePayload": {
        "errorMessage": "RequestId: e4b46cbf-b738-xmpl-8880-a18cdf61200e Process exited
 before completing request"
    }
}
```

Der Aufrufdatensatz enthält Details zum Ereignis, zur Antwort und zu dem Grund, warum der Datensatz gesendet wurde.

Zurückverfolgen von Anforderungen zu Zielen

Sie können AWS X-Ray verwenden, um eine verbundene Ansicht jeder Anforderung zu sehen, während sie in die Warteschlange gestellt, von einer Lambda-Funktion verarbeitet und an den Zielservice übergeben wird. Wenn Sie X-Ray-Tracing für eine Funktion oder einen Service aktivieren, der eine Funktion aufruft, fügt Lambda der Anforderung einen X-Ray-Header hinzu und übergibt den Header an den Zielservice. Traces von Upstream-Services werden automatisch mit Traces von Downstream-Lambda-Funktionen und Zieldiensten verknüpft, sodass eine end-to-end Ansicht der gesamten Anwendung entsteht. Weitere Informationen zum Tracing finden Sie unter Visualisieren Sie Lambda-Funktionsaufrufe mit AWS X-Ray.

Konfigurations-API für asynchrone Aufrufe

Verwenden Sie die folgenden API-Operationen, um asynchrone Aufrufeinstellungen mit dem AWS CLI oder AWS SDK zu verwalten.

- PutFunctionEventInvokeConfig
- GetFunctionEventInvokeConfig
- UpdateFunctionEventInvokeConfig
- ListFunctionEventInvokeKonfigurationen
- DeleteFunctionEventInvokeConfig

Verwenden Sie den Befehl, um den asynchronen Aufruf mit dem AWS CLI zu konfigurieren. `put-function-event-invoke-config` Im folgenden Beispiel wird eine Funktion mit einem maximalen Ereignisalter von 1 Stunde und ohne Wiederholversuche konfiguriert.

```
aws lambda put-function-event-invoke-config --function-name error \
```

```
--maximum-event-age-in-seconds 3600 --maximum-retry-attempts 0
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "LastModified": 1573686021.479,
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:error:$LATEST",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {}
    }
}
```

Der Befehl `put-function-event-invoke-config` überschreibt alle vorhandenen Konfigurationen für die Funktion, die Version oder den Alias. Um eine Option zu konfigurieren, ohne andere zurückzusetzen, verwenden Sie `update-function-event-invoke-config`. Im folgenden Beispiel wird Lambda so konfiguriert, dass ein Datensatz an eine SQS-Standardwarteschlange namens `destination` gesendet wird, wenn ein Ereignis nicht verarbeitet werden kann.

```
aws lambda update-function-event-invoke-config --function-name error \
--destination-config '{"OnFailure":{"Destination": "arn:aws:sqs:us-
east-2:123456789012:destination"}}'
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "LastModified": 1573687896.493,
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:error:$LATEST",
    "MaximumRetryAttempts": 0,
    "MaximumEventAgeInSeconds": 3600,
    "DestinationConfig": {
        "OnSuccess": {},
        "OnFailure": {
            "Destination": "arn:aws:sqs:us-east-2:123456789012:destination"
        }
    }
}
```

Warteschlangen für unzustellbare Nachrichten

Als eine Alternativ zu einem Zielort bei Ausfall können Sie Ihre Funktion mit einer Warteschlangen für unzustellbare Nachrichten konfigurieren, um verworfene Ereignisse zur weiteren Verarbeitung zu speichern. Eine Warteschlange für unzustellbare Nachrichten fungiert genauso wie ein Ziel bei Ausfall, da sie verwendet wird, wenn alle Verarbeitungsversuche eines Ereignisses fehlschlagen oder ein Ereignis abläuft, ohne verarbeitet zu werden. Da eine Warteschlange für unzustellbare Nachrichten jedoch Teil der versionsspezifischen Konfiguration einer Funktion ist, ist sie gesperrt, wenn Sie eine Version veröffentlichen. Ausfallziele unterstützen auch zusätzliche Ziele und enthalten Details zur Reaktion der Funktion im Aufrufdatensatz.

Um Ereignisse in einer Warteschlange für unzustellbare Nachrichten erneut zu verarbeiten, können Sie sie als Ereignisquelle für Ihre Lambda-Funktion festlegen. Alternativ können Sie die Ereignisse manuell abrufen.

Sie können eine Amazon-SQS-Standardwarteschlange oder ein Amazon-SNS-Standardthema für Ihre Warteschlange für unzustellbare Nachrichten auswählen. SQS-FIFO-Warteschlangen und SNS-FIFO-Themen werden nicht unterstützt. Wenn Sie über keine Warteschlangen oder Themen verfügen, erstellen Sie sie. Wählen Sie den Zieltyp aus, der Ihrem Anwendungsfall entspricht.

- Amazon-SQS-Warteschlange – Eine Warteschlange nimmt fehlgeschlagene Ereignisse auf, bis sie abgerufen werden. Wählen Sie eine Amazon SQS SQS-Standardwarteschlange, wenn Sie erwarten, dass eine einzelne Entität, z. B. eine Lambda-Funktion oder ein CloudWatch Alarm, das fehlgeschlagene Ereignis verarbeitet. Weitere Informationen finden Sie unter Verwenden von Lambda mit Amazon SQS.

  Erstellen Sie in der Amazon-SQS-Konsole eine Warteschlange.

- Amazon-SNS-Thema – Ein Thema leitet fehlgeschlagene Ereignisse an eine oder mehrere Ziele. Wählen Sie ein Amazon-SNS-Standardthema aus, wenn Sie erwarten, dass mehrere Entitäten auf ein fehlgeschlagenes Ereignis reagieren. Sie können beispielsweise ein Thema so konfigurieren, dass Ereignisse an eine E-Mail-Adresse, eine Lambda-Funktion und/oder einen HTTP-Endpunkt gesendet werden. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktionen mit Amazon SNS SNS-Benachrichtigungen.

  Erstellen Sie ein Thema in der Amazon-SNS-Konsole.

Um Ereginisse an eine Warteschlange oder an ein Thema zu senden, benötigt Ihre Funktion zusätzliche Berechtigungen. Fügen Sie eine Richtlinie mit den erforderlichen Berechtigungen zur Ausführungsrolle Ihrer Funktion hinzu.

- Amazon SQS — SQS: SendMessage
- Amazon SNS – sns:Publish

Wenn die Zielwarteschlange oder das Thema mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, muss die Ausführungsrolle auch ein Benutzer in der ressourcenbasierten Richtliniedes Schlüssels sein.

Nachdem das Ziel erstellt und die Ausführungsrolle Ihrer Funktion aktualisiert wurde, fügen Sie die Warteschlange für unzustellbare Nachrichten zu Ihrer Funktion hinzu. Sie können mehrere Funktionen zum Senden von Ereignissen an dasselbe Ziel konfigurieren.

So konfigurieren Sie eine Warteschlange für unzustellbare Nachrichten

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie „Konfiguration“ und dann „Asynchroner Aufruf“ aus.
4. Wählen Sie unter Asynchronous invocation (Asynchroner Aufruf) die Option Edit (Bearbeiten).
5. Legen Sie die DLQ-Ressource auf Amazon SQS oder Amazon SNS fest.
6. Wählen Sie die Ziel-Warteschlange oder das Ziel-Thema aus.
7. Wählen Sie Save aus.

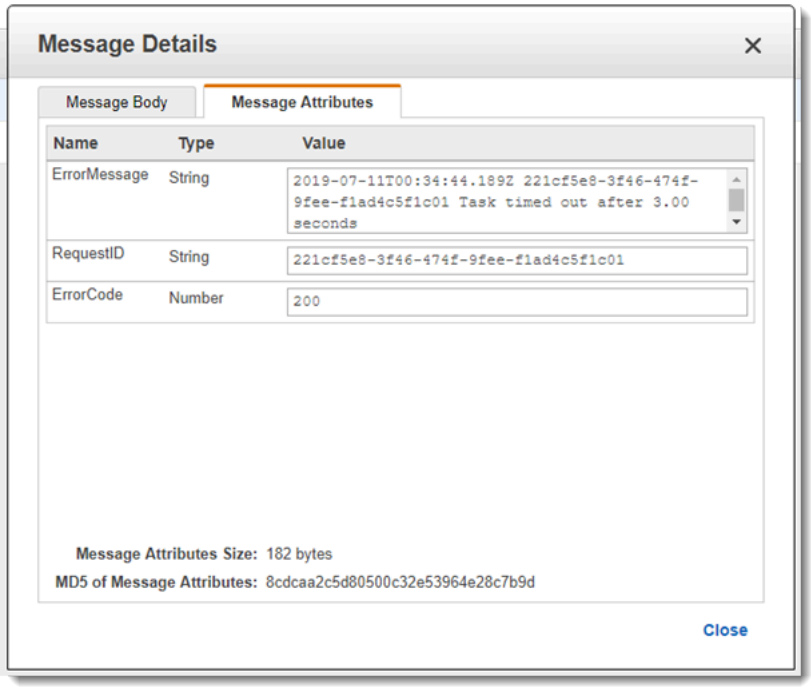
Verwenden Sie den Befehl, um eine Warteschlange für unzustellbare Briefe mit dem zu AWS CLI konfigurieren. `update-function-configuration`

```
aws lambda update-function-configuration --function-name my-function \
--dead-letter-config TargetArn=arn:aws:sns:us-east-2:123456789012:my-topic
```

Lambda sendet das Ereignis mit zusätzlichen Informationen in den Attributen an die Warteschlange für unzustellbare Nachrichten. Sie können anhand dieser Informationen den von der Funktion zurückgegebenen Fehler erkennen oder das Ereignis mit Protokollen oder einer AWS X-Ray -Ablaufverfolgung korrelieren.

Nachrichtenattribute der Warteschlange für unzustellbare Nachrichten

- RequestID (Zeichenfolge) – Die ID der Aufrufanforderung. Anforderungs-IDs erscheinen in Funktionsprotokollen. Sie können das X-Ray-SDK auch verwenden, um die Anforderungs-ID für ein Attribut in der Ablaufverfolgung aufzuzeichnen. Anschließend können Sie anhand der Anforderungs-ID in der X-Ray-Konsole nach Spuren suchen.
- ErrorCode(Nummer) — Der HTTP-Statuscode.
- ErrorMessage(String) — Die ersten 1 KB der Fehlermeldung.



Wenn Lambda keine Nachricht an die Warteschlange für unzustellbare Briefe senden kann, löscht es das Ereignis und gibt die Fehler-Metrik aus. DeadLetter Dies kann bei mangelnden Berechtigungen passieren oder wenn die Gesamtgröße der Nachricht den Grenzwert der Zielwarteschlange oder des Ziel-Themas überschreitet. Nehmen wir zum Beispiel an, dass eine Amazon-SNS-Benachrichtigung mit einem Text von fast 256 KB eine Funktion auslöst, die zu einem Fehler führt. In diesem Fall können die Ereignisdaten, die Amazon SNS hinzufügt, in Kombination mit den Attributen, die Lambda hinzufügt, dazu führen, dass die Nachricht die maximale Größe überschreitet, die in der Warteschlange für unzustellbare Nachrichten zulässig ist.

Wenn Sie Amazon SQS als Ereignisquelle verwenden, konfigurieren Sie eine Warteschlange für unzustellbare Nachrichten für die Amazon-SQS-Warteschlange selbst und nicht für die Lambda-Funktion. Weitere Informationen finden Sie unter Verwenden von Lambda mit Amazon SQS.

Wie Lambda Datensätze aus Stream- und warteschlangenbasierten Ereignisquellen verarbeitet

Eine Ereignisquellenzuordnung ist eine Lambda-Ressource, die Elemente aus stream- und warteschlangenbasierten Diensten liest und eine Funktion mit Datensatzstapeln aufruft. Die folgenden Dienste verwenden Ereignisquellenzuordnungen, um Lambda-Funktionen aufzurufen:

- Amazon-DynamoDB
- Amazon Kinesis
- Amazon MQ
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Selbstverwaltetes Apache Kafka
- Amazon-Simple-Queue-Service (Amazon SQS)
- Amazon DocumentDB (mit MongoDB-Kompatibilität) (Amazon DocumentDB)

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Wie unterscheiden sich Zuordnungen von Ereignisquellen von direkten Triggern

Einige AWS Dienste können Lambda-Funktionen mithilfe von Triggern direkt aufrufen. Diese Dienste leiten Ereignisse an Lambda weiter, und die Funktion wird sofort aufgerufen, wenn das angegebene Ereignis eintritt. Trigger eignen sich für diskrete Ereignisse und die Verarbeitung in Echtzeit. Wenn Sie mit der Lambda-Konsole einen Trigger erstellen, interagiert die Konsole mit dem entsprechenden AWS Dienst, um die Ereignisbenachrichtigung für diesen Dienst zu konfigurieren. Der Trigger wird tatsächlich von dem Dienst gespeichert und verwaltet, der die Ereignisse generiert, nicht von Lambda. Hier sind einige Beispiele für Dienste, die Trigger verwenden, um Lambda-Funktionen aufzurufen:

- Amazon Simple Storage Service (Amazon S3): Ruft eine Funktion auf, wenn ein Objekt in einem Bucket erstellt, gelöscht oder geändert wird. Weitere Informationen finden Sie unter Tutorial: Verwenden eines Amazon-S3-Auslösers zum Aufrufen einer Lambda-Funktion.
- Amazon Simple Notification Service (Amazon SNS): Ruft eine Funktion auf, wenn eine Nachricht unter einem SNS-Thema veröffentlicht wird. Weitere Informationen finden Sie unter Tutorial: Verwendung AWS Lambda mit Amazon Simple Notification Service.
- Amazon API Gateway: Ruft eine Funktion auf, wenn eine API-Anfrage an einen bestimmten Endpunkt gestellt wird. Weitere Informationen finden Sie unter Aufrufen einer Lambda-Funktion mithilfe eines Amazon API Gateway Gateway-Endpunkts.

Ereignisquellenzuordnungen sind Lambda-Ressourcen, die innerhalb des Lambda-Service erstellt und verwaltet werden. Zuordnungen von Ereignisquellen sind für die Verarbeitung umfangreicher Streaming-Daten oder Nachrichten aus Warteschlangen konzipiert. Die stapelweise Verarbeitung von Datensätzen aus einem Stream oder einer Warteschlange ist effizienter als die Verarbeitung einzelner Datensätze.

Batching-Verhalten

Standardmäßig batcht eine Ereignisquellenzuordnung Datensätze in einer einzigen Nutzlast, die Lambda an Ihre Funktion sendet. Zur Feinabstimmung des Batchverhaltens können Sie ein Batchfenster (MaximumBatchingWindowInSekunden) und eine Batchgröße () konfigurieren. BatchSize Ein Batch-Fenster ist die maximale Zeitspanne zur Erfassung von Datensätzen in einer einzigen Nutzlast. Eine Batch-Größe ist die maximale Anzahl von Datensätzen in einem einzigen Batch. Lambda ruft Ihre Funktion auf, wenn eines der folgenden drei Kriterien erfüllt ist:

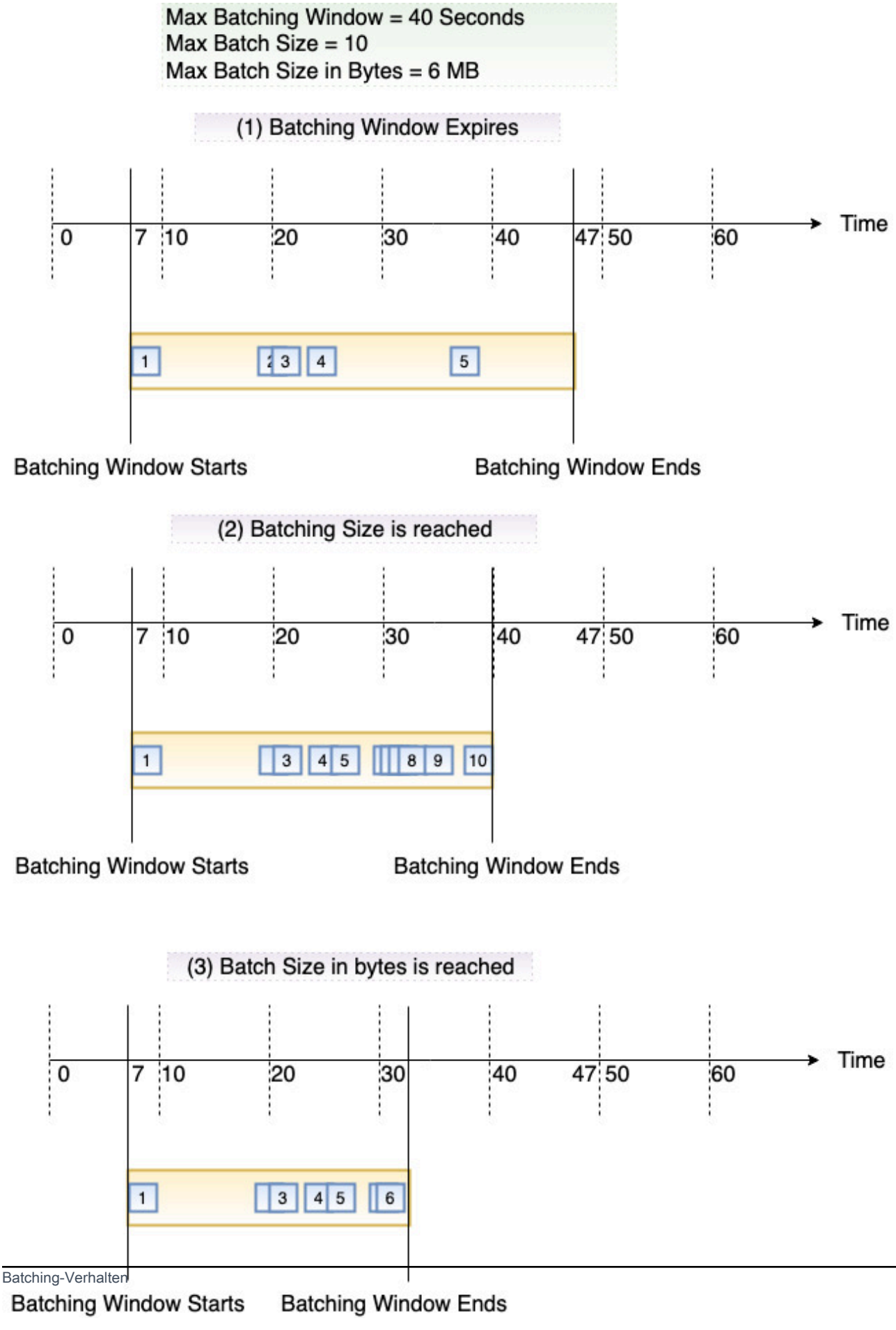
- Das Batching-Fenster erreicht seinen Maximalwert. Das Standardverhalten des Batchfensters hängt von der jeweiligen Ereignisquelle ab.
  - Für Kinesis-, DynamoDB- und Amazon SQS SQS-Ereignisquellen: Das Standard-Batch-Fenster beträgt 0 Sekunden. Das bedeutet, dass Lambda Batches nur dann an Ihre Funktion sendet, wenn entweder die Batchgröße erreicht oder die Nutzlastgrößenbeschränkung erreicht ist. Um ein Batching-Fenster festzulegen, konfigurieren Sie. `MaximumBatchingWindowInSeconds` Sie können diesen Parameter auf einen beliebigen Wert zwischen 0 und 300 Sekunden in Schritten von 1 Sekunde festlegen. Wenn Sie ein Batching-Fenster konfigurieren, beginnt das nächste Fenster, sobald der vorherige Funktionsaufruf abgeschlossen ist.
  - Für Amazon-MSK-, selbstverwaltete Apache-Kafka-, Amazon-MQ- und Amazon-DocumentDB-Ereignisquellen: Das standardmäßige Batching-Fenster beträgt 500 ms. Sie können

`MaximumBatchingWindowInSeconds` auf einen beliebigen Wert von 0 Sekunden bis 300 Sekunden in Sekundenschritten einstellen. Ein Batch-Fenster beginnt, sobald der erste Datensatz eintrifft.

> **Note**
>
> Da Sie Änderungen nur `MaximumBatchingWindowInSeconds` in Sekundenschritten vornehmen können, können Sie nach der Änderung nicht mehr zum standardmäßigen Batchfenster von 500 ms zurückkehren. Um das Standard-Batch-Fenster wiederherzustellen, müssen Sie eine neue Ereignisquellenzuordnung erstellen.

- Die Batch-Größe wird erreicht. Die minimale Batch-Größe beträgt 1. Die Standard- und die maximale Batch-Größe hängen von der Ereignisquelle ab. Einzelheiten zu diesen Werten finden Sie in der BatchSizeSpezifikation für den `CreateEventSourceMapping` API-Vorgang.
- Die Nutzlastgröße erreicht 6 MB. Sie können dieses Limit nicht ändern.

Das folgende Diagramm verdeutlicht diese Bedingungen. Angenommen, ein Batch-Fenster beginnt bei `t = 7` Sekunden. Im ersten Szenario erreicht das Batch-Fenster sein Maximum von 40 Sekunden bei `t = 47` Sekunden nach dem Erfassen von 5 Datensätzen. Im zweiten Szenario erreicht die Batch-Größe 10, bevor das Batch-Fenster abläuft, sodass das Batch-Fenster früh endet. Im dritten Szenario wird die maximale Nutzlastgröße erreicht, bevor das Batch-Fenster abläuft, sodass das Batch-Fenster frühzeitig endet.


Max Batching Window = 40 Seconds
Max Batch Size = 10
Max Batch Size in Bytes = 6 MB
(1) Batching Window Expires
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
Batching Window Starts
Batching Window Ends
(2) Batching Size is reached
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
8
9
10
Batching Window Starts
Batching Window Ends
(3) Batch Size in bytes is reached
0
7
10
20
30
40
47
50
60
Time
1
3
4
5
6
Batching Window Starts
Batching Window Ends

API für die Ereignisquellenzuordnung

Um eine Ereignisquelle mit der AWS Command Line Interface (AWS CLI) oder einem AWS-SDK zu verwalten, können Sie die folgenden API-Operationen verwenden:

- CreateEventSourceMapping
- ListEventSourceMappings
- GetEventSourceMapping
- UpdateEventSourceMapping
- DeleteEventSourceMapping

Verwendung AWS Lambda mit Amazon DynamoDB

> **Note**
>
> Wenn Sie Daten an ein anderes Ziel als eine Lambda-Funktion senden oder die Daten vor dem Senden anreichern möchten, finden Sie weitere Informationen unter Amazon EventBridge Pipes.

Sie können eine AWS Lambda Funktion verwenden, um Datensätze in einem Amazon DynamoDB DynamoDB-Stream zu verarbeiten. Mit DynamoDB Streams können Sie eine Lambda-Funktion auslösen, damit jedes Mal, wenn eine DynamoDB-Tabelle aktualisiert wird, weitere Aufgaben ausgeführt werden.

Lambda liest Datensätze aus dem Stream und ruft Ihre Funktion synchron mit einem Ereignis auf, das Stream-Datensätze enthält. Lambda liest Datensätze in Batches und ruft Ihre Funktion auf, um Datensätze aus dem Batch zu verarbeiten.

Sections

- Fehlerbehandlung
- CloudWatch Amazon-Metriken
- Zeitfenster
- Melden von Batch-Elementen
- Konfigurationsparameter zu Amazon DynamoDB Streams
- Tutorial: Verwendung AWS Lambda mit Amazon DynamoDB DynamoDB-Streams
- Beispiel-Funktionscode
- AWS SAM-Vorlage für eine DynamoDB-Anwendung

Beispielereignis

Example


```
{
  "Records": [
    {
      "eventID": "1",
      "eventVersion": "1.0",
      "dynamodb": {
        "Keys": {
          "Id": {
            "N": "101"
          }
        },
        "NewImage": {
          "Message": {
            "S": "New item!"
          },
          "Id": {
            "N": "101"
          }
        },
        "StreamViewType": "NEW_AND_OLD_IMAGES",
        "SequenceNumber": "111",
        "SizeBytes": 26
      },
      "awsRegion": "us-west-2",
      "eventName": "INSERT",
      "eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
```

```
      "eventSource": "aws:dynamodb"
    },
    {
      "eventID": "2",
      "eventVersion": "1.0",
      "dynamodb": {
        "OldImage": {
          "Message": {
            "S": "New item!"
          },
          "Id": {
            "N": "101"
          }
        },
        "SequenceNumber": "222",
        "Keys": {
          "Id": {
            "N": "101"
          }
        },
        "SizeBytes": 59,
        "NewImage": {
          "Message": {
            "S": "This item has changed"
          },
          "Id": {
            "N": "101"
          }
        },
        "StreamViewType": "NEW_AND_OLD_IMAGES"
      },
      "awsRegion": "us-west-2",
      "eventName": "MODIFY",
      "eventSourceARN": "arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525",
      "eventSource": "aws:dynamodb"
    }
  ]}
```

Abrufen und Stapeln von Streams

Lambda fragt Shards in Ihrem DynamoDB-Stream nach Datensätzen bei einer Basisrate von viermal pro Sekunde ab. Sind Datensätze verfügbar, ruft Lambda Ihre Funktion auf und wartet auf das

Ergebnis. Ist die Verarbeitung erfolgreich, setzt Lambda die Abrufe fort, bis es weitere Datensätze erhält.

Standardmäßig ruft Lambda Ihre Funktion auf, sobald Datensätze verfügbar sind. Wenn der Batch, den Lambda aus der Ereignisquelle liest, nur einen Datensatz enthält, sendet Lambda nur einen Datensatz an die Funktion. Damit die Funktion nicht mit einer kleinen Anzahl von Datensätzen aufgerufen wird, können Sie die Ereignisquelle anweisen, Datensätze bis zu 5 Minuten lang zu puffern, indem Sie ein Batch-Fenster konfigurieren. Bevor die Funktion aufgerufen wird, liest Lambda so lange Datensätze aus der Ereignisquelle, bis es einen vollständigen Batch erfasst hat, das Batch-Verarbeitungsfenster abläuft oder der Batch die Nutzlastgrenze von 6 MB erreicht. Weitere Informationen finden Sie unter Batching-Verhalten.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Konfigurieren Sie die ParallelizationFactorEinstellung so, dass ein Shard eines DynamoDB-Streams mit mehr als einem Lambda-Aufruf gleichzeitig verarbeitet wird. Sie können die Anzahl der gleichzeitigen Batches angeben, die Lambda von einem Shard über einen Parallelisierungsfaktor von 1 (Standard) bis 10 abfragt. Wenn Sie die Anzahl der gleichzeitigen Batches pro Shard erhöhen, sorgt Lambda trotzdem für die Verarbeitung in der Reihenfolge auf Artikelebene (Partition und Sortierschlüssel).

Startpositionen für Abfragen und Streams

Beachten Sie, dass die Stream-Abfrage bei der Erstellung und Aktualisierung der Zuordnung von Ereignisquellen letztendlich konsistent ist.

- Bei der Erstellung der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis mit der Abfrage von Ereignissen aus dem Stream begonnen wird.
- Bei Aktualisierungen der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis die Abfrage von Ereignissen aus dem Stream gestoppt und neu gestartet wird.

Dieses Verhalten bedeutet, dass, wenn Sie `LATEST` als Startposition für den Stream angeben, die Zuordnung von Ereignisquellen bei der Erstellung oder Aktualisierung möglicherweise Ereignisse übersieht. Um sicherzustellen, dass keine Ereignisse übersehen werden, geben Sie die Stream-Startposition als `TRIM_HORIZON` an.

Gleichzeitige Leser eines Shard in DynamoDB Streams

Für Einzelregionstabellen, bei denen es sich nicht um globale Tabellen handelt, können Sie bis zu zwei Lambda-Funktionen entwerfen, die gleichzeitig aus demselben DynamoDB-Streams-Shard lesen. Eine Überschreitung dieses Grenzwerts kann zu einer Anforderungsdrosselung führen. Für globale Tabellen empfehlen wir, die Anzahl der gleichzeitigen Funktionen auf eine zu beschränken, um eine Anforderungsdrosselung zu vermeiden.

Berechtigungen für die Ausführungsrolle

Die AWSLambdaDynamoDBExecutionRole AWS verwaltete Richtlinie umfasst die Berechtigungen, die Lambda benötigt, um aus Ihrem DynamoDB-Stream zu lesen. Fügen Sie diese verwaltete Richtlinie der Ausführungsrolle Ihrer Funktion hinzu.

Um Datensätze fehlgeschlagener Batches an eine SQS-Standardwarteschlange oder ein SNS-Standardthema zu senden, benötigt Ihre Funktion zusätzliche Berechtigungen. Jeder Zielservice benötigt eine andere Berechtigung wie folgt:

- Amazon SQS — SQS: SendMessage
- Amazon SNS – sns:Publish

Fügen Sie Berechtigungen hinzu und erstellen Sie die Zuordnung der Ereignisquelle

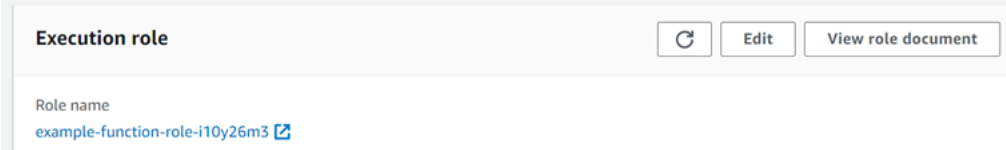
Erstellen Sie eine Ereignisquellenzuordnung, um Lambda anzuweisen, Datensätze aus Ihrem Stream an eine Lambda-Funktion zu senden. Sie können mehrere Ereignisquellen-Zuweisung erstellen, um gleiche Daten mit mehreren Lambda-Funktionen oder Elemente aus mehreren Streams mit nur einer Funktion zu verarbeiten.

Um Ihre Funktion so zu konfigurieren, dass sie aus DynamoDB Streams liest, fügen Sie die AWSLambdaDynamoDBExecutionRole AWS verwaltete Richtlinie Ihrer Ausführungsrolle hinzu und erstellen Sie dann einen DynamoDB-Trigger.

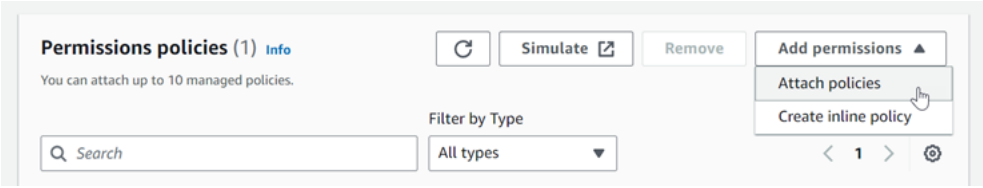
Um Berechtigungen hinzuzufügen und einen Trigger zu erstellen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

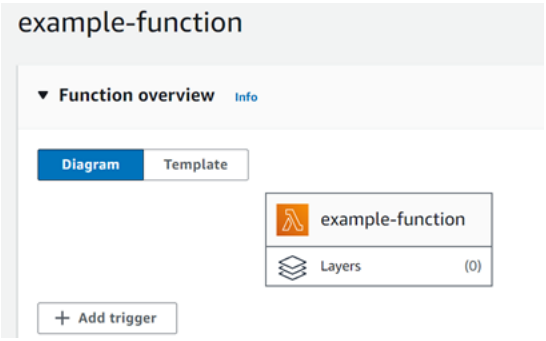
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Berechtigungen aus.
4. Wählen Sie unter Rollenname den Link zu Ihrer Ausführungsrolle aus. Dieser Link öffnet die Rolle in der IAM-Konsole.



5. Wählen Sie Berechtigungen hinzufügen aus und wählen Sie dann Richtlinien direkt anhängen aus.



6. Geben Sie im Suchfeld `AWSLambdaDynamoDBExecutionRole` ein. Fügen Sie diese Richtlinie Ihrer Ausführungsrolle hinzu. Dies ist eine AWS verwaltete Richtlinie, die die Berechtigungen enthält, die Ihre Funktion zum Lesen aus dem DynamoDB-Stream benötigt. Weitere Informationen zu dieser Richtlinie finden Sie AWSLambdaDynamoDBExecutionRolein der Referenz zu AWS verwalteten Richtlinien.
7. Kehren Sie zu Ihrer Funktion in der Lambda-Konsole zurück. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).



8. Wählen Sie einen Auslösertyp aus.
9. Konfigurieren Sie die erforderlichen Optionen und wählen Sie dann Add (Hinzufügen) aus.

Lambda unterstützt die folgenden Optionen für DynamoDB-Ereignisquellen:

Optionen für die Ereignisquelle

- DynamoDB-Tabelle – Die DynamoDB-Tabelle, aus der Datensätze gelesen werden sollen.
- Batchgröße – Die Anzahl der Datensätze, die in jedem Batch bis zu 10.000 an die Funktion gesendet werden sollen. Lambda übergibt alle Datensätze im Batch in einem einzigen Aufruf an die Funktion, solange die Gesamtgröße der Ereignisse nicht das Nutzlast-Limit für synchrone Aufrufe überschreitet (6 MB).
- Batchfenster – Geben Sie die maximale Zeitspanne zur Erfassung von Datensätzen vor dem Aufruf der Funktion in Sekunden an.
- Startposition – Verarbeiten Sie nur neue Datensätze oder alle vorhandenen Datensätze.
  - Neueste – Verarbeiten Sie Datensätze, die neu zum Stream hinzugefügt wurden.
  - Horizont trimmen – Verarbeiten Sie alle Datensätze im Stream.

  Nach der Verarbeitung aller vorhandenen Datensätze hat die Funktion aufgeholt und setzt die Verarbeitung neuer Datensätze fort.
- On-failure destination (Ziel bei Ausfall) – Eine SQS-Warteschlange oder ein SNS-Thema für Datensätze, die nicht verarbeitet werden können. Wenn Lambda einen Datensatz-Batch verwirft, weil er zu alt ist oder alle Wiederholungen erschöpft hat, sendet es Details zum Batch an die Warteschlange oder das Thema.
- Wiederholungsversuche – Die maximale Anzahl von Wiederholungen von Lambda, wenn die Funktion einen Fehler zurückgibt. Dies gilt nicht für Servicefehler oder Drosselungen, bei denen der Batch die Funktion nicht erreicht hat.
- Höchstalter des Datensatzes – Das maximale Alter eines Datensatzes, den Lambda an Ihre Funktion sendet.
- Batch bei Fehler aufteilen – Wenn die Funktion einen Fehler zurückgibt, teilen Sie den Batch vor dem erneuten Versuch in zwei Teile. Ihre ursprüngliche Einstellung für die Batch-Größe bleibt unverändert.
- Gleichzeitige Batches pro Shard – Verarbeitet gleichzeitig mehrere Batches aus demselben Shard.
- Aktiviert – Auf „true“ festlegen, um die Ereignisquellenzuordnung zu aktivieren. Auf "false" festlegen, um die Verarbeitung von Datensätzen zu beenden. Lambda merkt sich den zuletzt verarbeiteten Datensatz und setzt die Verarbeitung nach erneuter Aktivierung der Zuordnung an dieser Stelle fort.

> **Note**
>
> Für GetRecords API-Aufrufe, die von Lambda als Teil von DynamoDB-Triggern aufgerufen werden, fallen keine Gebühren an.

Um die Konfiguration der Ereignisquelle zu einem späteren Zeitpunkt zu verwalten, wählen Sie den Auslöser im Designer aus.

Fehlerbehandlung

Die Fehlerbehandlung für DynamoDB-Ereignisquellenzuordnungen hängt davon ab, ob der Fehler vor dem Aufruf der Funktion oder während des Funktionsaufrufs auftritt:

- Vor dem Aufruf: Wenn eine Lambda-Ereignisquellenzuordnung die Funktion aufgrund von Drosselung oder anderen Problemen nicht aufrufen kann, versucht sie es erneut, bis die Datensätze ablaufen oder das in der Ereignisquellenzuordnung konfigurierte Höchstalter (Sekunden) überschreiten. MaximumRecord AgeIn
- Während des Aufrufs: Wenn die Funktion aufgerufen wird, aber einen Fehler zurückgibt, versucht Lambda es erneut, bis die Datensätze ablaufen, das Höchstalter (MaximumRecordAgeInSekunden) überschreiten oder das konfigurierte Wiederholungskontingent (Versuche) erreicht haben. MaximumRetry Bei Funktionsfehlern können Sie auch BisectBatchOnFunctionError konfigurieren, wodurch ein fehlgeschlagener Batch in zwei kleinere Batches aufgeteilt wird, wodurch fehlerhafte Datensätze isoliert und Timeouts vermieden werden. Durch das Aufteilen von Batches wird das Wiederholungskontingent nicht aufgebraucht.

Wenn die Fehlerbehandlungsmaßnahmen fehlschlagen, verwirft Lambda die Datensätze und setzt die Verarbeitung von Batches aus dem Stream fort. Bei den Standardeinstellungen bedeutet dies, dass ein fehlerhafter Datensatz die Verarbeitung auf dem betroffenen Shard für bis zu einen Tag blockieren kann. Um dies zu vermeiden, konfigurieren Sie die Ereignisquellenzuordnung Ihrer Funktion mit einer angemessenen Anzahl von Wiederholungen und einem maximalen Datensatzalter, das zu Ihrem Anwendungsfall passt.

Konfiguration von Zielen für fehlgeschlagene Aufrufe

Um Datensätze zu fehlgeschlagenen Aufrufen zur Zuordnung von Ereignisquellen beizubehalten, fügen Sie der Zuordnung von Ereignisquellen Ihrer Funktion ein Ziel hinzu. Jeder an das Ziel gesendete Datensatz ist ein JSON-Dokument mit Metadaten über den fehlgeschlagenen Aufruf.

Sie können jedes Amazon SNS SNS-Thema oder jede Amazon SQS SQS-Warteschlange als Ziel konfigurieren. Ihre Ausführungsrolle muss über Berechtigungen für das Ziel verfügen:

- Für SQS-Ziele: sqs: SendMessage
- Für SNS-Ziele: sns:Publish

Gehen Sie folgendermaßen vor, um ein Ausfallziel mit der Konsole zu konfigurieren:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add destination (Ziel hinzufügen).
4. Wählen Sie als Quelle die Option Aufruf der Zuordnung von Ereignisquellen aus.
5. Wählen Sie für die Zuordnung von Ereignisquellen eine Ereignisquelle aus, die für diese Funktion konfiguriert ist.
6. Wählen Sie für Bedingung die Option Bei Ausfall aus. Für Aufrufe zur Zuordnung von Ereignisquellen ist dies die einzig akzeptierte Bedingung.
7. Wählen Sie unter Zieltyp den Zieltyp aus, an den Lambda Aufrufdatensätze sendet.
8. Wählen Sie unter Destination (Ziel) eine Ressource aus.
9. Wählen Sie Save aus.

Sie können mit () auch ein Ziel für den Fall eines Fehlers konfigurieren. AWS Command Line Interface AWS CLI Mit dem folgenden Befehl create-event-source-mapping wird beispielsweise eine Ereignisquellenzuordnung mit einem SQS-Ziel für den Fall eines Fehlers hinzugefügt: `MyFunction`

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

Der folgende Befehl update-event-source-mapping aktualisiert eine Ereignisquellenzuordnung, sodass fehlgeschlagene Aufrufdatensätze nach zwei Wiederholungsversuchen oder wenn die Datensätze älter als eine Stunde sind, an ein SNS-Ziel gesendet werden.

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--maximum-retry-attempts 2 \
--maximum-record-age-in-seconds 3600 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-
east-1:123456789012:dest-topic"}}'
```

Aktualisierte Einstellungen werden asynchron angewendet und werden erst nach Abschluss des Vorgangs in der Ausgabe berücksichtigt. Verwenden Sie den Befehl get-event-source-mapping, um den aktuellen Status anzuzeigen.

Um ein Ziel zu entfernen, geben Sie eine leere Zeichenfolge als Argument für den `destination-config`-Parameter an:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Das folgende Beispiel zeigt einen Aufrufdatensatz für einen DynamoDB-Stream.

Example Aufrufdatensatz

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:13:49.717Z",
    "DDBStreamBatchInfo": {
        "shardId": "shardId-00000001573689847184-864758bb",
        "startSequenceNumber": "800000000003126276362",
        "endSequenceNumber": "800000000003126276362",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:13:19Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:13:19Z",
```

```
        "batchSize": 1,
        "streamArn": "arn:aws:dynamodb:us-east-2:123456789012:table/mytable/
stream/2019-11-14T00:04:06.388"
    }
}
```

Sie können diese Informationen verwenden, um die betroffenen Datensätze aus dem Stream für die Fehlersuche abzurufen. Die tatsächlichen Datensätze sind nicht enthalten, daher müssen Sie diesen Datensatz verarbeiten und aus dem Stream abrufen, bevor sie ablaufen und verloren gehen.

CloudWatch Amazon-Metriken

Lambda gibt die `IteratorAge`-Metrik aus, wenn Ihre Funktion die Verarbeitung eines Batches von Datensätzen fertigstellt. Die Metrik gibt an, wie alt der letzte Datensatz im Batch bei Fertigstellung der Verarbeitung war. Wenn Ihre Funktion neue Ereignisse verarbeitet, können Sie mit dem Iterator-Alter die Latenz zwischen dem Zeitpunkt, zu dem ein Datensatz hinzugefügt wird und dem Zeitpunkt, zu dem die Funktion verarbeitet wird, schätzen.

Eine steigende Tendenz beim Iterator-Alter kann auf Probleme mit Ihrer Funktion hindeuten. Weitere Informationen finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Zeitfenster

Lambda-Funktionen können kontinuierliche Stream-Verarbeitungsanwendungen ausführen. Ein Stream entspricht einer unbegrenzten Menge von Daten, die kontinuierlich durch Ihre Anwendung fließen. Um Informationen aus dieser sich ständig aktualisierenden Eingabe zu analysieren, können Sie die enthaltenen Datensätze mithilfe eines zeitlich definierten Fensters binden.

Rollierende Fenster sind unterschiedliche Zeitfenster, die sich in regelmäßigen Abständen öffnen und schließen. Standardmäßig sind Lambda-Aufrufe zustandslos – Sie können sie nicht für die Verarbeitung von Daten über mehrere kontinuierliche Aufrufe hinweg ohne eine externe Datenbank verwenden. Mit rollierenden Fenstern können Sie jedoch Ihren Status über Aufrufe hinweg beibehalten. Dieser Zustand enthält das Gesamtergebnis der Nachrichten, die zuvor für das aktuelle Fenster verarbeitet wurden. Ihr Zustand kann maximal 1 MB pro Shard betragen. Wenn er diese Größe überschreitet, wird Lambda das Fenster vorzeitig beenden.

Jeder Datensatz in einem Stream gehört zu einem bestimmten Fenster. Lambda verarbeitet jeden Datensatz mindestens einmal, garantiert jedoch nicht, dass jeder Datensatz nur einmal verarbeitet wird. In seltenen Fällen, etwa bei der Fehlerbehandlung, werden einige Datensätze möglicherweise mehrmals verarbeitet. Datensätze werden beim ersten Mal immer in der richtigen Reihenfolge

verarbeitet. Wenn Datensätze mehr als einmal verarbeitet werden, werden sie nicht in der richtigen Reihenfolge verarbeitet.

Aggregation und Verarbeitung

Ihre benutzerverwaltete Funktion wird sowohl zur Aggregation als auch zur Verarbeitung der Endergebnisse dieser Aggregation aufgerufen. Lambda aggregiert alle im Fenster empfangenen Datensätze. Sie können diese Datensätze in mehreren Stapeln erhalten, jeweils als ein separater Aufruf. Jeder Aufruf erhält einen Zustand. Wenn Sie also rollierende Fenster verwenden, muss Ihre Lambda-Funktionsantwort eine `state`-Eigenschaft enthalten. Wenn die Antwort keine `state`-Eigenschaft enthält, betrachtet Lambda dies als fehlgeschlagenen Aufruf. Um diese Bedingung zu erfüllen, kann Ihre Funktion ein `TimeWindowEventResponse`-Objekt zurückgeben, das die folgende JSON-Form aufweist:

Example **`TimeWindowEventResponse`**-Werte

```
{
    "state": {
        "1": 282,
        "2": 715
    },
    "batchItemFailures": []
}
```

> **Note**
>
> Für Java-Funktionen empfehlen wir, eine `Map<String, String>` zu verwenden, um den Status darzustellen.

Am Ende des Fensters wird das Flag `isFinalInvokeForWindow` auf `true` gesetzt, um anzugeben, dass es sich um den Endzustand handelt und dass es für die Verarbeitung bereit ist. Nach der Verarbeitung werden das Fenster und Ihr endgültiger Aufruf wird abgeschlossen, und dann wird der Zustand gelöscht.

Am Ende Ihres Fensters verwendet Lambda die endgültige Verarbeitung für Aktionen an den Aggregationsergebnissen. Ihre endgültige Verarbeitung wird synchron aufgerufen. Nach erfolgreichem Aufruf zeigt Ihre Funktion auf die Sequenznummer und die Stream-Verarbeitung wird fortgesetzt. Wenn der Aufruf nicht erfolgreich ist, unterbricht Ihre Lambda-Funktion die weitere Verarbeitung bis zu einem erfolgreichen Aufruf.

Example DynamodbTimeWindowEvent

```
{
   "Records":[
      {
         "eventID":"1",
         "eventName":"INSERT",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"111",
            "SizeBytes":26,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"2",
         "eventName":"MODIFY",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
```

```
            "Message":{
               "S":"This item has changed"
            },
            "Id":{
               "N":"101"
            }
         },
         "OldImage":{
            "Message":{
               "S":"New item!"
            },
            "Id":{
               "N":"101"
            }
         },
         "SequenceNumber":"222",
         "SizeBytes":59,
         "StreamViewType":"NEW_AND_OLD_IMAGES"
      },
      "eventSourceARN":"stream-ARN"
   },
   {
      "eventID":"3",
      "eventName":"REMOVE",
      "eventVersion":"1.0",
      "eventSource":"aws:dynamodb",
      "awsRegion":"us-east-1",
      "dynamodb":{
         "Keys":{
            "Id":{
               "N":"101"
            }
         },
         "OldImage":{
            "Message":{
               "S":"This item has changed"
            },
            "Id":{
               "N":"101"
            }
         },
         "SequenceNumber":"333",
         "SizeBytes":38,
         "StreamViewType":"NEW_AND_OLD_IMAGES"
```

```
         },
         "eventSourceARN":"stream-ARN"
      }
   ],
    "window": {
        "start": "2020-07-30T17:00:00Z",
        "end": "2020-07-30T17:05:00Z"
    },
    "state": {
        "1": "state1"
    },
    "shardId": "shard123456789",
    "eventSourceARN": "stream-ARN",
    "isFinalInvokeForWindow": false,
    "isWindowTerminatedEarly": false
}
```

Konfiguration

Sie können rollierende Fenster konfigurieren, wenn Sie eine Ereignisquellenzuordnung erstellen oder aktualisieren. Um ein Taumelfenster zu konfigurieren, geben Sie das Fenster in Sekunden an (TumblingWindowInSeconds). Mit dem folgenden Beispielbefehl AWS Command Line Interface (AWS CLI) wird eine Quellenzuordnung für Streaming-Ereignisse erstellt, die ein Wechselfenster von 120 Sekunden hat. Die für Aggregation und Verarbeitung definierte Lambda-Funktion wird `tumbling-window-example-function` genannt.

```
aws lambda create-event-source-mapping \
--event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table/
stream/2024-06-10T19:26:16.525 \
--function-name tumbling-window-example-function \
--starting-position TRIM_HORIZON \
--tumbling-window-in-seconds 120
```

Lambda bestimmt die rollierenden Fenstergrenzen basierend auf dem Zeitpunkt, zu dem Datensätze in den Stream eingefügt wurden. Für alle Datensätze steht ein ungefährer Zeitstempel zur Verfügung, den Lambda in Grenzbestimmungen verwendet.

Rollierende Fensteraggregationen unterstützen kein Resharding. Wenn der Shard endet, betrachtet Lambda das Fenster als geschlossen und die untergeordneten Shards beginnen ihr eigenes Fenster in einem neuen Zustand.

Rollierende Fenster unterstützen vollständig die bestehenden Wiederholungsrichtlinien `maxRetryAttempts` und `maxRecordAge`.

Example Handler.py – Aggregation und Verarbeitung

Die folgende Python-Funktion veranschaulicht, wie Sie Ihren Endzustand aggregieren und dann verarbeiten:

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

#Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
        print('Destination invoke')
    else:
        print('Aggregate invoke')

#Check for early terminations
    if event['isWindowTerminatedEarly']:
        print('Window terminated early')

    #Aggregation logic
    state = event['state']
    for record in event['Records']:
        state[record['dynamodb']['NewImage']['Id']] = state.get(record['dynamodb']
['NewImage']['Id'], 0) + 1

    print('Returning state: ', state)
    return {'state': state}
```

Melden von Batch-Elementen

Beim Konsumieren und Verarbeiten von Streaming-Daten aus einer Ereignisquelle werden standardmäßig Lambda-Checkpoints auf die höchste Sequenznummer eines Batches nur dann überprüft, wenn der Batch ein voller Erfolg ist. Lambda behandelt alle anderen Ergebnisse als einen vollständigen Fehler und versucht, den Batch bis zum Wiederholungslimit zu verarbeiten. Um beim Verarbeiten von Stapeln aus einem Stream Teilerfolge zu ermöglichen, aktivieren Sie `ReportBatchItemFailures`. Das Zulassen von Teilerfolgen kann dazu beitragen, die Anzahl der Wiederholungen in einer Aufzeichnung zu reduzieren, obwohl die Möglichkeit von Wiederholungen in einer erfolgreichen Aufzeichnung nicht vollständig verhindert wird.

Um die Option zu aktivieren`ReportBatchItemFailures`, nehmen Sie den Enum-Wert **`ReportBatchItemFailures`** in die FunctionResponseTypenliste auf. Diese Liste zeigt an, welche Antworttypen für Ihre Funktion aktiviert sind. Sie können diese Liste konfigurieren, wenn Sie eine Ereignisquellenzuordnung erstellen oder aktualisieren.

Berichtsyntax

Beim Konfigurieren von Berichten zu Batch-Elementfehlern wird die `StreamsEventResponse`-Klasse mit einer Liste von Batch-Elementfehlern zurückgegeben. Sie können ein `StreamsEventResponse`-Objekt verwenden, um die Sequenznummer des ersten fehlgeschlagenen Datensatzes im Batch zurückzugeben. Sie können auch Ihre eigene benutzerdefinierte Klasse mit der richtigen Antwortsyntax erstellen. Die folgende JSON-Struktur zeigt die erforderliche Antwortsyntax:

```
{
  "batchItemFailures": [
        {
            "itemIdentifier": "<SequenceNumber>"
        }
    ]
}
```

> **Note**
>
> Wenn das `batchItemFailures`-Array mehrere Elemente enthält, verwendet Lambda den Datensatz mit der niedrigsten Sequenznummer als Kontrollpunkt. Lambda wiederholt dann alle Datensätze ab diesem Kontrollpunkt.

Erfolgs- und Misserfolgsbedingungen

Lambda behandelt einen Batch als vollständigen Erfolg, wenn Sie eines der folgenden Elemente zurückgeben:

- Eine leere `batchItemFailure`-Liste
- Eine ungültige `batchItemFailure`-Liste
- Ein leeres `EventResponse`
- Ein ungültiges `EventResponse`

Lambda behandelt einen Batch als vollständigen Misserfolg, wenn Sie eines der folgenden Elemente zurückgeben:

- Eine leere Zeichenfolge `itemIdentifier`
- Ein ungültiges `itemIdentifier`
- Ein `itemIdentifier` mit einem falschen Schlüsselnamen

Lambda wiederholt Fehler basierend auf Ihrer Wiederholungsstrategie.

Einen Batch halbieren

Wenn Ihr Aufruf fehlschlägt und `BisectBatchOnFunctionError` eingeschaltet ist, wird der Stapel unabhängig von Ihrer `ReportBatchItemFailures`-Einstellung halbiert.

Wenn eine partielle Batch-Erfolgsantwort empfangen wird und sowohl `BisectBatchOnFunctionError` als auch `ReportBatchItemFailures` aktiviert sind, wird der Batch mit der zurückgegebenen Sequenznummer halbiert und Lambda versucht nur die verbleibenden Datensätze erneut.

Hier sind einige Beispiele für Funktionscodes, die die Liste der fehlgeschlagenen Nachrichten-IDs im Batch zurückgeben:

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von.NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
 ILambdaContext context)

    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");
        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>();
        StreamsEventResponse streamsEventResponse = new StreamsEventResponse();

        foreach (var record in dynamoEvent.Records)
        {
            try
            {
                var sequenceNumber = record.Dynamodb.SequenceNumber;
                context.Logger.LogInformation(sequenceNumber);
            }
            catch (Exception ex)
            {
                context.Logger.LogError(ex.Message);
                batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
 { ItemIdentifier = record.Dynamodb.SequenceNumber });
            }
        }

        if (batchItemFailures.Count > 0)
        {
            streamsEventResponse.BatchItemFailures = batchItemFailures;
        }

        context.Logger.LogInformation("Stream processing complete.");
        return streamsEventResponse;
    }
```

```
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

type BatchItemFailure struct {
 ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
 BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
 (*BatchResult, error) {
 var batchItemFailures []BatchItemFailure
 curRecordSequenceNumber := ""

 for _, record := range event.Records {
  // Process your record
  curRecordSequenceNumber = record.Change.SequenceNumber
 }
```

```
 if curRecordSequenceNumber != "" {
  batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
 curRecordSequenceNumber})
 }

 batchResult := BatchResult{
  BatchItemFailures: batchItemFailures,
 }

 return &batchResult, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;
```

```
public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
 Serializable> {

    @Override
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
 input.getRecords()) {
          try {
                //Process your record
                StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
                curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse();
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda unter Verwendung von. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event) => {
  const records = event.Records;
  let curRecordSequenceNumber = "";

  for (const record of records) {
    try {
      // Process your record
      curRecordSequenceNumber = record.dynamodb.SequenceNumber;
    } catch (e) {
      // Return failed record's sequence number
      return { batchItemFailures: [{ itemIdentifier:
 curRecordSequenceNumber }] };
    }
  }

  return { batchItemFailures: [] };
};
```

Melden von DynamoDB-Batchelementfehlern mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { DynamoDBBatchItemFailure, DynamoDBStreamEvent } from "aws-lambda";

export const handler = async (event: DynamoDBStreamEvent):
 Promise<DynamoDBBatchItemFailure[]> => {
```

```
    const batchItemsFailures: DynamoDBBatchItemFailure[] = []
    let curRecordSequenceNumber

    for(const record of event.Records) {
        curRecordSequenceNumber = record.dynamodb?.SequenceNumber

        if(curRecordSequenceNumber) {
            batchItemsFailures.push({
                itemIdentifier: curRecordSequenceNumber
            })
        }
    }

    return batchItemsFailures
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von PHP.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';
```

```
class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $dynamoDbEvent = new DynamoDbEvent($event);
        $this->logger->info("Processing records");

        $records = $dynamoDbEvent->getRecords();
        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}
```

```
$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
    records = event["Records"]
    cur_record_sequence_number = ""

    records.each do |record|
      begin
        # Process your record
        cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
      rescue StandardError => e
        # Return failed record's sequence number
        return {"batchItemFailures" => [{"itemIdentifier" =>
 cur_record_sequence_number}]}
      end
    end

    {"batchItemFailures" => []}
  end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;

    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
 Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("".to_string()),
            });
            return Ok(response);
        }
```

```
        // Process your record here...
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Konfigurationsparameter zu Amazon DynamoDB Streams

Alle Lambda-Ereignisquelltypen verwenden dieselben CreateEventSourceMappingUpdateEventSourceMappingAPI-Operationen. Allerdings gelten nur einige der Parameter für DynamoDB Streams.

Ereignisquellparameter, die für DynamoDB Streams gelten

Parameter	Erforderlich	Standard	Hinweise
BatchSize	N	100	Höchstwert: 10 000.
BisectBatchOnFunctionFehler	N	false	
DestinationConfig	N		Ein Ziel der Amazon-SQS-Standardwarteschlange oder des Amazon-SNS-Standardthemas für verworfene Datensätze
Aktiviert	N	true	
EventSourceArn	Y		Der ARN des Datenstroms oder eines Stream-Konsumenten
FilterCriteria	N		Lambda-Ereignisfilterung
FunctionName	Y		
FunctionResponseTypen	N		Damit Ihre Funktion bestimmte Fehler in einem Batch meldet, beziehen Sie den Wert `ReportBatchItemFailures` in `FunctionResponseTypes` ein. Weitere Informationen finden Sie unter

Parameter	Erforderlich	Standard	Hinweise
			Melden von Batch-Elementen.
MaximumBatchingWindowInSekunden	N	0	
MaximumRecordAgeInSekunden	N	-1	-1 bedeutet unendlich: Fehlgeschlagene Datensätze werden wiederholt, bis der Datensatz abläuft. Das Datenaufbewahrungslimit für DynamoDB Streams beträgt 24 Stunden. Minimum: -1 Höchstwert: 604 800
MaximumRetryVersuche	N	-1	-1 bedeutet unendlich: Fehlgeschlagene Datensätze werden wiederholt, bis der Datensatz abläuft Minimum: 0 Höchstwert: 10 000.
ParallelizationFactor	N	1	Maximum: 10
StartingPosition	Y		TRIM_HORIZON oder LATEST
TumblingWindowInSeconds	N		Minimum: 0 Maximum: 900

Tutorial: Verwendung AWS Lambda mit Amazon DynamoDB DynamoDB-Streams

In diesem Tutorial erstellen Sie eine Lambda-Funktion zum Verarbeiten von Ereignissen aus einem Amazon-DynamoDB-Stream.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen der Ausführungsrolle

Erstellen Sie die Ausführungsrolle, die Ihrer Funktion die Erlaubnis erteilt, auf Ressourcen zuzugreifen AWS .

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.
   - Vertrauenswürdige Entität – Lambda.
   - Berechtigungen — AWSLambdaDynamoDBExecutionRole.
   - Role name (Name der Rolle – **`lambda-dynamodb-role`**.

Der AWSLambdaDynamoDBExecutionRolehat die Berechtigungen, die die Funktion benötigt, um Elemente aus DynamoDB zu lesen und Protokolle in Logs zu CloudWatch schreiben.

Erstellen der Funktion

Erstellen Sie eine Lambda-Funktion, die Ihre DynamoDB-Ereignisse verarbeitet. Der Funktionscode schreibt einige der eingehenden Ereignisdaten in Logs. CloudWatch

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von.NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext
 context)
    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }

        context.Logger.LogInformation("Stream processing complete.");
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main
```

```
import (
 "context"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-lambda-go/events"
 "fmt"
)

func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,
 error) {
 if len(event.Records) == 0 {
  return nil, fmt.Errorf("received empty event")
 }

 for _, record := range event.Records {
   LogDynamoDBRecord(record)
 }

 message := fmt.Sprintf("Records processed: %d", len(event.Records))
 return &message, nil
}

func main() {
 lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
 fmt.Println(record.EventID)
 fmt.Println(record.EventName)
 fmt.Printf("%+v\n", record.Change)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
 com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
 GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
 GSON.toJson(record.getDynamodb()));
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines DynamoDB-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

Konsumieren eines DynamoDB-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
}
const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein DynamoDB-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\DynamoDb\DynamoDbHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends DynamoDbHandler
{
    private StderrLogger $logger;

    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
    {
        $this->logger->info("Processing DynamoDb table items");
        $records = $event->getRecords();

        foreach ($records as $record) {
            $eventName = $record->getEventName();
            $keys = $record->getKeys();
            $old = $record->getOldImage();
            $new = $record->getNewImage();

            $this->logger->info("Event Name:".$eventName."\n");
            $this->logger->info("Keys:". json_encode($keys)."\n");
            $this->logger->info("Old Image:". json_encode($old)."\n");
            $this->logger->info("New Image:". json_encode($new));
```

```
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }

        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords items");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event:, context:)
    return 'received empty event' if event['Records'].empty?

    event['Records'].each do |record|
      log_dynamodb_record(record)
    end

    "Records processed: #{event['Records'].length}"
  end

  def log_dynamodb_record(record)
    puts record['eventID']
    puts record['eventName']
    puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
  end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein DynamoDB-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
   };


// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_dynamo_dbrecord(record);
    }
```

```
    tracing::info!("Dynamo db records processed");

    // Prepare the response
    Ok(())

}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();

    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

So erstellen Sie die Funktion

1. Kopieren Sie den Beispiel-Code in eine Datei mit dem Namen `example.js`.
2. Erstellen Sie ein Bereitstellungspaket.

```
zip function.zip example.js
```

3. Erstellen Sie eine Lambda-Funktion mit dem Befehl `create-function`.

```
aws lambda create-function --function-name ProcessDynamoDBRecords \
    --zip-file fileb://function.zip --handler example.handler --runtime nodejs18.x
 \
```

```
    --role arn:aws:iam::111122223333:role/lambda-dynamodb-role
```

Lambda-Funktion testen

In diesem Schritt rufen Sie Ihre Lambda-Funktion manuell mit dem `invoke` AWS Lambda CLI-Befehl und dem folgenden DynamoDB-Beispielereignis auf. Kopieren Sie Folgendes in eine Datei mit dem Namen. `input.txt`

Example input.txt

```
{
   "Records":[
      {
         "eventID":"1",
         "eventName":"INSERT",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"111",
            "SizeBytes":26,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"2",
         "eventName":"MODIFY",
         "eventVersion":"1.0",
```

```
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "NewImage":{
               "Message":{
                  "S":"This item has changed"
               },
               "Id":{
                  "N":"101"
               }
            },
            "OldImage":{
               "Message":{
                  "S":"New item!"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"222",
            "SizeBytes":59,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      },
      {
         "eventID":"3",
         "eventName":"REMOVE",
         "eventVersion":"1.0",
         "eventSource":"aws:dynamodb",
         "awsRegion":"us-east-1",
         "dynamodb":{
            "Keys":{
               "Id":{
                  "N":"101"
               }
            },
            "OldImage":{
               "Message":{
```

```
                  "S":"This item has changed"
               },
               "Id":{
                  "N":"101"
               }
            },
            "SequenceNumber":"333",
            "SizeBytes":38,
            "StreamViewType":"NEW_AND_OLD_IMAGES"
         },
         "eventSourceARN":"stream-ARN"
      }
   ]
}
```

Führen Sie den Befehl `invoke` aus.

```
aws lambda invoke --function-name ProcessDynamoDBRecords \
    --cli-binary-format raw-in-base64-out \
    --payload file://input.txt outputfile.txt
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Funktion gibt die Zeichenfolge `message` im Antworttext zurück.

Überprüfen Sie die Ausgabe in der Datei `outputfile.txt`.

Erstellen einer DynamoDB-Tabelle mit einem aktivierten Stream

Erstellen einer Amazon-DynamoDB-Tabelle mit einem aktivierten Stream.

So erstellen Sie eine DynamoDB-Tabelle

1. Öffnen Sie die DynamoDB-Konsole.
2. Wählen Sie Create table aus.
3. Erstellen Sie eine Tabelle mit den folgenden Einstellungen:
   - Tabellenname – **`lambda-dynamodb-stream`**
   - Primärschlüssel – **`id`** (Zeichenfolge)

4. Wählen Sie Erstellen.

So aktivieren Sie Streams

1. Öffnen Sie die DynamoDB-Konsole.
2. Wählen Sie Tables (Tabellen) aus.
3. Wählen Sie die Tabelle lambda-dynamodb-stream aus.
4. Wählen Sie unter Exports and streams (Exporte und Streams) die Option DynamoDB stream details (Details zu DynamoDB-Streams) aus.
5. Wählen Sie Turn on (Einschalten) aus.
6. Wählen Sie als Ansichtstyp die Option Nur Schlüsselattribute aus.
7. Wählen Sie Stream einschalten aus.

Notieren Sie sich den Stream-ARN. Sie benötigen diesen im nächsten Schritt, um die Lambda-Funktion dem Stream zuzuordnen. Weitere Informationen zur Aktivierung von Streams finden Sie unter Erfassen von Tabellenaktivitäten mit DynamoDB Streams.

Fügen Sie eine Ereignisquelle hinzu in AWS Lambda

Erstellen Sie eine Ereignisquellenzuordnung in AWS Lambda. Diese Ereignisquellenzuordnung ordnet den DynamoDB-Stream Ihrer Lambda-Funktion zu. Nachdem Sie diese Ereignisquellenzuordnung erstellt haben, AWS Lambda beginnt die Abfrage des Streams.

Führen Sie den Befehl AWS CLI `create-event-source-mapping` aus. Notieren Sie sich die UUID, nachdem Sie den Befehl ausgeführt haben. Sie benötigen diese UUID, um in Befehlen auf die Ereignisquellenzuordnung zu verweisen (beispielsweise beim Löschen der Ereignisquellen-Zuweisung).

```
aws lambda create-event-source-mapping --function-name ProcessDynamoDBRecords \
    --batch-size 100 --starting-position LATEST --event-source DynamoDB-stream-arn
```

Dadurch wird eine Zuweisung zwischen dem angegebenen DynamoDB-Stream und der Lambda-Funktion erstellt. Sie können einen DynamoDB-Stream mehreren Lambda-Funktionen und dieselbe Lambda-Funktion mehreren Streams zuordnen. Die Lambda-Funktionen teilen jedoch den Lesedurchsatz für den geteilten Stream.

Sie erhalten die Liste der Ereignisquellen-Zuweisungen, indem Sie folgenden Befehl ausführen.

```
aws lambda list-event-source-mappings
```

Die Liste gibt alle von Ihnen erstellten Ereignisquellenzuordnungen zurück und für jede Zuordnung zeigt sie u. a. den `LastProcessingResult`. Dieses Feld wird verwendet, um eine informative Meldung bereitzustellen, wenn Probleme auftreten. Werte wie `No records processed` (gibt an, dass die Abfrage noch nicht gestartet AWS Lambda wurde oder dass der Stream keine Datensätze enthält) und `OK` (gibt an, dass Datensätze AWS Lambda erfolgreich aus dem Stream gelesen und Ihre Lambda-Funktion aufgerufen wurden) weisen darauf hin, dass keine Probleme vorliegen. Bei Problemen erhalten Sie eine Fehlermeldung.

Bei einer großen Anzahl von Ereignisquellen-Zuweisungen verwenden Sie den Funktionsnamen-Parameter, um die Ergebnisse einzugrenzen.

```
aws lambda list-event-source-mappings --function-name ProcessDynamoDBRecords
```

Testen der Einrichtung

Testen Sie das Erlebnis. end-to-end Beim Aktualisieren der Tabelle schreibt DynamoDB Ereignisdatensätze in den Stream. Da AWS Lambda den Stream abfragt, erkennt es neue Datensätze im Stream und ruft Ihre Lambda-Funktion für Sie auf, indem Ereignisse an die Funktion übergeben werden.

1. Fügen Sie in der DynamoDB-Konsole Elemente hinzu, aktualisieren und löschen Sie diese und fügen Sie diese hinzu. DynamoDB schreibt Datensätze dieser Aktionen in den Stream.
2. AWS Lambda fragt den Stream ab und wenn es Aktualisierungen am Stream erkennt, ruft es Ihre Lambda-Funktion auf, indem es die im Stream gefundenen Ereignisdaten weitergibt.
3. Ihre Funktion wird in Amazon ausgeführt und erstellt Protokolle CloudWatch. Sie können die in der CloudWatch Amazon-Konsole gemeldeten Protokolle überprüfen.

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die DynamoDB-Tabelle

1. Öffnen Sie die Seite Tables (Tabellen) in der DynamoDB-Konsole.
2. Wählen Sie die von Ihnen erstellte Tabelle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie **`delete`** in das Textfeld ein.
5. Wählen Sie Delete Table (Tabelle löschen).

Beispiel-Funktionscode

Beispiel-Code steht für die folgenden Sprachen zur Verfügung.

Themen

- Node.js
- Java 11
- C#
- Python 3
- Go

Node.js

Das folgende Beispiel verarbeitet Nachrichten aus DynamoDB und protokollierte ihren Inhalt.

Example ProcessDynamoDBStream.js

```
console.log('Loading function');

exports.lambda_handler = function(event, context, callback) {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(function(record) {
        console.log(record.eventID);
        console.log(record.eventName);
        console.log('DynamoDB Record: %j', record.dynamodb);
    });
    callback(null, "message");
};
```

Komprimieren Sie den Beispielcode, um ein Bereitstellungspaket zu erstellen. Detaillierte Anweisungen finden Sie unter Bereitstellen von Node.js Lambda-Funktionen mit ZIP-Dateiarchiven.

Java 11

Das folgende Beispiel verarbeitet Nachrichten von DynamoDB und protokolliert ihren Inhalt. `handleRequest` ist der Handler, den AWS Lambda aufruft und Ereignisdaten bereitstellt. Der Handler verwendet die vordefinierte Klasse `DynamodbEvent`, die in der Bibliothek `aws-lambda-java-events` definiert ist.

Example DDB EventProcessor.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler2;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;

public class DDBEventProcessor implements
        RequestHandler2<DynamodbEvent, String> {

    public String handleRequest(DynamodbEvent ddbEvent, Context context) {
        for (DynamodbStreamRecord record : ddbEvent.getRecords()){
           System.out.println(record.getEventID());
           System.out.println(record.getEventName());
           System.out.println(record.getDynamodb().toString());
```

```
        }
        return "Successfully processed " + ddbEvent.getRecords().size() + " records.";
    }
}
```

Wenn der Handler normal ohne Ausnahmen zurückgegeben wird, betrachtet Lambda den Eingabebatch mit Datensätzen als erfolgreich verarbeitet und beginnt mit dem Lesen neuer Datensätze im Stream. Wenn der Handler eine Ausnahme ausgibt, betrachtet Lambda den Eingabebatch mit Datensätzen als nicht verarbeitet und ruft die Funktion mit demselben Batch an Datensätzen erneut auf.

Abhängigkeiten

- `aws-lambda-java-core`
- `aws-lambda-java-events`

Erstellen Sie den Code mit den Abhängigkeiten der Lambda-Bibliothek, um Bereitstellungspakete zu erstellen. Detaillierte Anweisungen finden Sie unter Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven.

C#

Das folgende Beispiel verarbeitet Nachrichten von DynamoDB und protokolliert ihren Inhalt. `ProcessDynamoEvent` ist der Handler, den AWS Lambda aufruft und Ereignisdaten bereitstellt. Der Handler verwendet die vordefinierte Klasse `DynamoDbEvent`, die in der Bibliothek `Amazon.Lambda.DynamoDBEvents` definiert ist.

Example ProcessingDynamoDBStreams.cs

```
using System;
using System.IO;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

using Amazon.Lambda.Serialization.Json;

namespace DynamoDBStreams
{
    public class DdbSample
    {
```

```
        private static readonly JsonSerializer _jsonSerializer = new JsonSerializer();

        public void ProcessDynamoEvent(DynamoDBEvent dynamoEvent)
        {
            Console.WriteLine($"Beginning to process {dynamoEvent.Records.Count}
 records...");

            foreach (var record in dynamoEvent.Records)
            {
                Console.WriteLine($"Event ID: {record.EventID}");
                Console.WriteLine($"Event Name: {record.EventName}");

                string streamRecordJson = SerializeObject(record.Dynamodb);
                Console.WriteLine($"DynamoDB Record:");
                Console.WriteLine(streamRecordJson);
            }

            Console.WriteLine("Stream processing complete.");
        }

        private string SerializeObject(object streamRecord)
        {
            using (var ms = new MemoryStream())
            {
                _jsonSerializer.Serialize(streamRecord, ms);
                return Encoding.UTF8.GetString(ms.ToArray());
            }
        }
    }
}
```

Ersetzen Sie `Program.cs` in einem .NET-Core-Projekt mit dem obigen Beispiel. Detaillierte Anweisungen finden Sie unter Erstellen und Bereitstellen von C#-Lambda-Funktionen mit ZIP-Dateiarchiven.

Python 3

Das folgende Beispiel verarbeitet Nachrichten aus DynamoDB und protokollierte ihren Inhalt.

Example ProcessDynamoDBStream.py

```
from __future__ import print_function
```

```
def lambda_handler(event, context):
    for record in event['Records']:
        print(record['eventID'])
        print(record['eventName'])
    print('Successfully processed %s records.' % str(len(event['Records'])))
```

Komprimieren Sie den Beispielcode, um ein Bereitstellungspaket zu erstellen. Detaillierte Anweisungen finden Sie unter Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen.

Go

Das folgende Beispiel verarbeitet Nachrichten aus DynamoDB und protokollierte ihren Inhalt.

Example

```
import (
    "strings"

    "github.com/aws/aws-lambda-go/events"
)

func handleRequest(ctx context.Context, e events.DynamoDBEvent) {

    for _, record := range e.Records {
        fmt.Printf("Processing request data for event ID %s, type %s.\n",
 record.EventID, record.EventName)

        // Print new values for attributes of type String
        for name, value := range record.Change.NewImage {
            if value.DataType() == events.DataTypeString {
                fmt.Printf("Attribute name: %s, value: %s\n", name, value.String())
            }
        }
    }
}
```

Erstellen Sie die ausführbare Datei mit `go build` und erstellen Sie ein Bereitstellungspaket. Detaillierte Anweisungen finden Sie unter Bereitstellen von Lambda-Go-Funktionen mit ZIP-Dateiarchiven.

AWS SAM-Vorlage für eine DynamoDB-Anwendung

Sie können verwenden, um diese Anwendung zu entwickeln AWS SAM. Weitere Informationen zum Erstellen von AWS SAM-Vorlagen finden Sie unter AWS SAM-Vorlagengrundlagen im AWS Serverless Application Model Entwicklerhandbuch.

Nachfolgend finden Sie eine AWS SAM-Beispielvorlage für die Anwendung aus dem Tutorial. Kopieren Sie den unten stehenden Text in eine Datei vom Typ .yaml und speichern Sie sie neben der ZIP-Datei, die Sie zuvor erzeugt haben. Beachten Sie, dass die `Handler`- und `Runtime`-Parameterwerte den Werten entsprechen sollten, die Sie bei der Erzeugung der Funktion im vorherigen Abschnitt verwendet haben.

Example template.yaml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Resources:
  ProcessDynamoDBStream:
    Type: AWS::Serverless::Function
    Properties:
      Handler: handler
      Runtime: runtime
      Policies: AWSLambdaDynamoDBExecutionRole
      Events:
        Stream:
          Type: DynamoDB
          Properties:
            Stream: !GetAtt DynamoDBTable.StreamArn
            BatchSize: 100
            StartingPosition: TRIM_HORIZON

  DynamoDBTable:
    Type: AWS::DynamoDB::Table
    Properties:
      AttributeDefinitions:
        - AttributeName: id
          AttributeType: S
      KeySchema:
        - AttributeName: id
          KeyType: HASH
      ProvisionedThroughput:
        ReadCapacityUnits: 5
```

```
        WriteCapacityUnits: 5
      StreamSpecification:
        StreamViewType: NEW_IMAGE
```

Weitere Informationen zum Packen und Bereitstellen Ihrer Serverless-Anwendung über die Package- und Deploy-Befehle finden Sie im Artikel zum Bereitstellen von Serverless-Anwendungen im AWS Serverless Application Model Entwicklerhandbuch.

So verarbeitet Lambda Datensätze aus Amazon Kinesis Data Streams

Sie können eine Lambda-Funktion verwenden, um Datensätze in einem Amazon Kinesis Kinesis-Datenstream zu verarbeiten. Sie können eine Lambda-Funktion einem Kinesis Data Streams Streams-Verbraucher mit gemeinsamem Durchsatz (Standard-Iterator) oder einem dedizierten Durchsatzverbraucher mit erweitertem Fan-Out zuordnen. Bei Standard-Iteratoren fragt Lambda jeden Shard in Ihrem Kinesis-Stream nach Datensätzen ab, die das HTTP-Protokoll verwenden. Die Ereignisquellenzuordnung teilt den Lesedurchsatz mit anderen Konsumenten des Shards zusammen.

Weitere Informationen zu Kinesis-Datenströmen finden Sie unter Daten aus Amazon Kinesis Data Streams.

> **Note**
>
> Kinesis berechnet Gebühren für jeden Shard, sowie bei verbessertem Rundsenden für Daten, die aus dem Stream gelesen werden. Details zu den Preisen finden Sie unter Amazon-Kinesis- Preise.

Abfragen und Stapeln von Streams

Lambda liest Datensätze aus dem Datenstrom und ruft Ihre Funktion synchron mit einem Ereignis auf, das Stream-Datensätze enthält. Lambda liest Datensätze in Batches und ruft Ihre Funktion auf, um Datensätze aus dem Batch zu verarbeiten. Jeder Batch enthält Datensätze aus einem einzelnen Shard/Datenstrom.

Standardmäßig ruft Lambda Ihre Funktion auf, sobald Datensätze verfügbar sind. Wenn der Batch, den Lambda aus der Ereignisquelle liest, nur einen Datensatz enthält, sendet Lambda nur einen Datensatz an die Funktion. Damit die Funktion nicht mit einer kleinen Anzahl von Datensätzen aufgerufen wird, können Sie die Ereignisquelle anweisen, Datensätze bis zu 5 Minuten lang zu

puffern, indem Sie ein Batch-Fenster konfigurieren. Bevor die Funktion aufgerufen wird, liest Lambda so lange Datensätze aus der Ereignisquelle, bis es einen vollständigen Batch erfasst hat, das Batch-Verarbeitungsfenster abläuft oder der Batch die Nutzlastgrenze von 6 MB erreicht. Weitere Informationen finden Sie unter Batching-Verhalten.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Konfigurieren Sie die ParallelizationFactorEinstellung so, dass ein Shard eines Kinesis-Datenstroms mit mehr als einem Lambda-Aufruf gleichzeitig verarbeitet wird. Sie können die Anzahl der gleichzeitigen Batches angeben, die Lambda von einem Shard über einen Parallelisierungsfaktor von 1 (Standard) bis 10 abfragt. Wenn `ParallelizationFactor` beispielsweise auf 2 gesetzt ist, können Sie maximal 200 gleichzeitige Lambda-Aufrufe haben, um 100 Kinesis-Daten-Shards zu verarbeiten (in der Praxis werden womöglich andere Werte für die Metrik `ConcurrentExecutions` angezeigt). Dies hilft, den Verarbeitungsdurchsatz hochzuskalieren, wenn das Datenvolumen flüchtig ist und `IteratorAge` hoch ist. Wenn Sie die Anzahl der gleichzeitigen Batches pro Shard erhöhen, sorgt Lambda trotzdem für die Verarbeitung in der Reihenfolge auf Partitionsschlüsselebene.

Sie können es auch `ParallelizationFactor` mit Kinesis-Aggregation verwenden. Das Verhalten der Ereignisquellenzuordnung hängt davon ab, ob Sie das erweiterte Fan-Out verwenden:

- Ohne erweitertes Fan-Out: Alle Ereignisse innerhalb eines aggregierten Ereignisses müssen denselben Partitionsschlüssel haben. Der Partitionsschlüssel muss außerdem mit dem des aggregierten Ereignisses übereinstimmen. Wenn die Ereignisse innerhalb des aggregierten Ereignisses unterschiedliche Partitionsschlüssel haben, kann Lambda nicht garantieren, dass die Ereignisse in der richtigen Reihenfolge nach Partitionsschlüsseln verarbeitet werden.
- Mit verbessertem Fan-Out: Zunächst dekodiert Lambda das aggregierte Ereignis in seine einzelnen Ereignisse. Das aggregierte Ereignis kann einen anderen Partitionsschlüssel haben als die darin enthaltenen Ereignisse. Ereignisse, die nicht dem Partitionsschlüssel entsprechen, werden jedoch gelöscht und gehen verloren. Lambda verarbeitet diese Ereignisse nicht und sendet sie nicht an ein konfiguriertes Fehlerziel.

Beispielereignis

Example

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1545084650.987
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
        },
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692540925702759324208523137515618",
                "data": "VGhpcyBpcyBvbmx5IGEgdGVzdC4=",
                "approximateArrivalTimestamp": 1545084711.166
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692540925702759324208523137515618",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-
stream"
        }
```

```
    ]
}
```

Amazon Kinesis Data Streams Streams-Datensätze mit Lambda verarbeiten

Um Amazon Kinesis Data Streams Streams-Datensätze mit Lambda zu verarbeiten, erstellen Sie einen Consumer für Ihren Stream und anschließend eine Lambda-Ereignisquellenzuordnung.

Konfigurieren Ihres Daten-Streams und Ihrer Funktion

Ihre Lambda-Funktion ist eine Konsumentenanwendung für Ihren Daten-Stream. Sie verarbeitet jeweils einen Batch Datensätzen aus jedem Shard. Sie können eine Lambda-Funktion zu einem Konsumenten mit gemeinsam genutztem Durchsatz (Standard-Iterator) oder zu einem Konsumenten mit dediziertem Durchsatz mit erweitertem Rundsenden zuweisen.

- Standard-Iterator: Lambda fragt jeden Shard in Ihrem Kinesis-Stream mit einer Basisrate von einmal pro Sekunde nach Datensätzen ab. Wenn mehr Datensätze verfügbar sind, verarbeitet Lambda Batches, bis die Funktion mit dem Stream gleichzieht. Die Ereignisquellenzuordnung teilt den Lesedurchsatz mit anderen Konsumenten des Shards zusammen.
- Verbesserter Fan-Out: Um die Latenz zu minimieren und den Lesedurchsatz zu maximieren, sollten Sie einen Data-Stream-Consumer mit erweitertem Fan-Out einrichten. Stream-Konsumenten mit erweitertem Rundsenden erhalten eine dedizierte Verbindung für jeden Shard, der keine Auswirkungen auf andere Anwendungen hat, die aus dem Stream lesen. Stream-Konsumenten verwenden HTTP/2, um die Latenz zu reduzieren, indem Datensätze über eine langlebige Verbindung an Lambda übertragen und Anforderungs-Header komprimiert werden. Sie können einen Stream-Consumer mit der Kinesis RegisterStreamConsumer API erstellen.

```
aws kinesis register-stream-consumer \
--consumer-name con1 \
--stream-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Consumer": {
        "ConsumerName": "con1",
        "ConsumerARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream/
consumer/con1:1540591608",
```

```
        "ConsumerStatus": "CREATING",
        "ConsumerCreationTimestamp": 1540591608.0
    }
}
```

Um die Geschwindigkeit zu erhöhen, mit der Ihre Funktion Datensätze verarbeitet, fügen Sie Ihrem Datenstream Shards hinzu. Lambda verarbeitet Datensätze in jedem Shard in der Reihenfolge. Es beendet die Verarbeitung zusätzlicher Datensätze in einem Shard, wenn Ihre Funktion einen Fehler zurückgibt. Mehr Shards bedeutet, dass mehr Stapel verarbeitet und gleichzeitig die Auswirkungen von Fehlern auf die Nebenläufigkeit verringert werden.

Wenn Ihre Funktion nicht hochskalieren kann, um alle gleichzeitigen Stapel zu verarbeiten, fordern Sie eine Kontingenterhöhung an oder reservieren Sie Gleichzeitigkeit für Ihre Funktion.

Erstellen Sie eine Ereignisquellenzuordnung, um eine Lambda-Funktion aufzurufen

Um Ihre Lambda-Funktion mit Datensätzen aus Ihrem Datenstrom aufzurufen, erstellen Sie eine Ereignisquellenzuordnung. Sie können mehrere Ereignisquellenzuordnungen erstellen, um gleiche Daten mit mehreren Lambda-Funktionen oder Elemente aus mehreren Daten-Streams mit nur einer Funktion zu verarbeiten. Bei der Verarbeitung von Elementen aus mehreren Streams enthält jeder Batch nur Datensätze aus einem einzigen Shard oder Stream.

Sie können Zuordnungen von Ereignisquellen konfigurieren, um Datensätze aus einem Stream in einem anderen zu verarbeiten. AWS-Konto Weitere Informationen hierzu finden Sie unter the section called “Kontoübergreifende Zuordnungen”.

Bevor Sie eine Ereignisquellenzuordnung erstellen, müssen Sie Ihrer Lambda-Funktion die Erlaubnis erteilen, aus einem Kinesis-Datenstream zu lesen. Lambda benötigt die folgenden Berechtigungen, um Ressourcen im Zusammenhang mit Ihrem Kinesis-Datenstrom zu verwalten:

- Kinesis: DescribeStream
- Kinesis: Zusammenfassung DescribeStream
- Kinesis: GetRecords
- Kinesis: Iterator GetShard
- Kinese: ListShards
- Kinese: ListStreams
- Kinesis: Scherbe SubscribeTo

Die AWS verwaltete Richtlinie AWSLambdaKinesisExecutionRoleumfasst diese Berechtigungen. Fügen Sie diese verwaltete Richtlinie zu Ihrer Funktion hinzu, wie im folgenden Verfahren beschrieben.

AWS Management Console

So fügen Sie Ihrer Funktion Kinesis-Berechtigungen hinzu

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie auf der Registerkarte Konfiguration die Option Berechtigungen aus.
3. Wählen Sie im Bereich Ausführungsrolle unter Rollenname den Link zur Ausführungsrolle Ihrer Funktion aus. Dieser Link öffnet die Seite für diese Rolle in der IAM-Konsole.
4. Wählen Sie im Bereich „Berechtigungsrichtlinien“ die Option „Berechtigungen hinzufügen“ und anschließend „Richtlinien anhängen“ aus.
5. Geben Sie im Suchfeld **`AWSLambdaKinesisExecutionRole`** ein.
6. Aktivieren Sie das Kontrollkästchen neben der Richtlinie und wählen Sie „Berechtigung hinzufügen“ aus.

AWS CLI

So fügen Sie Ihrer Funktion Kinesis-Berechtigungen hinzu

- Führen Sie den folgenden CLI-Befehl aus, um die `AWSLambdaKinesisExecutionRole` Richtlinie zur Ausführungsrolle Ihrer Funktion hinzuzufügen:

```
aws iam attach-role-policy \
--role-name MyFunctionRole \
--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaKinesisExecutionRole
```

AWS SAM

So fügen Sie Ihrer Funktion Kinesis-Berechtigungen hinzu

- Fügen Sie der Definition Ihrer Funktion die `Policies` Eigenschaft hinzu, wie im folgenden Beispiel gezeigt:

```
Resources:
```

```
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./my-function/
      Handler: index.handler
      Runtime: nodejs20.x
      Policies:
        - AWSLambdaKinesisExecutionRole
```

Nachdem Sie die erforderlichen Berechtigungen konfiguriert haben, erstellen Sie die Zuordnung der Ereignisquelle.

AWS Management Console

So erstellen Sie das Kinesis-Ereignisquellen-Mapping

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie im Bereich Function overview (Funktionsübersicht) die Option Add trigger (Auslöser hinzufügen).
3. Wählen Sie unter Trigger-Konfiguration für die Quelle Kinesis aus.
4. Wählen Sie den Kinesis-Stream aus, für den Sie das Event-Quellen-Mapping erstellen möchten, und optional einen Consumer Ihres Streams.
5. (Optional) Bearbeiten Sie die Stapelgröße, die Startposition und das Stapelfenster für Ihre Ereignisquellenzuordnung.
6. Wählen Sie Hinzufügen aus.

Wenn Sie Ihre Ereignisquellenzuordnung von der Konsole aus erstellen, muss Ihre IAM-Rolle über die Berechtigungen kinesis: ListStreams und kinesis: ListStream Consumers verfügen.

AWS CLI

So erstellen Sie das Kinesis-Ereignisquellen-Mapping

- Führen Sie den folgenden CLI-Befehl aus, um eine Kinesis-Ereignisquellenzuordnung zu erstellen. Wählen Sie Ihre eigene Batchgröße und Startposition entsprechend Ihrem Anwendungsfall.

```
aws lambda create-event-source-mapping \
```

```
--function-name MyFunction \
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \
--starting-position LATEST \
--batch-size 100
```

Um ein Batching-Fenster anzugeben, fügen Sie die `--maximum-batching-window-in-seconds` Option hinzu. Weitere Informationen zur Verwendung dieses und anderer Parameter finden Sie unter create-event-source-mapping in der Befehlsreferenz.AWS CLI

AWS SAM

So erstellen Sie das Kinesis-Ereignisquellen-Mapping

- Fügen Sie der Definition Ihrer Funktion die `KinesisEvent` Eigenschaft hinzu, wie im folgenden Beispiel gezeigt:

```
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: ./my-function/
      Handler: index.handler
      Runtime: nodejs20.x
      Policies:
        - AWSLambdaKinesisExecutionRole
      Events:
        KinesisEvent:
          Type: Kinesis
          Properties:
            Stream: !GetAtt MyKinesisStream.Arn
            StartingPosition: LATEST
            BatchSize: 100

  MyKinesisStream:
    Type: AWS::Kinesis::Stream
    Properties:
      ShardCount: 1
```

Weitere Informationen zum Erstellen einer Ereignisquellenzuordnung für Kinesis Data Streams finden Sie unter Kinesis im AWS Serverless Application Model Entwicklerhandbuch. AWS SAM

Abfrage und Startposition des Streams

Beachten Sie, dass die Stream-Abfrage bei der Erstellung und Aktualisierung der Zuordnung von Ereignisquellen letztendlich konsistent ist.

- Bei der Erstellung der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis mit der Abfrage von Ereignissen aus dem Stream begonnen wird.
- Bei Aktualisierungen der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis die Abfrage von Ereignissen aus dem Stream gestoppt und neu gestartet wird.

Dieses Verhalten bedeutet, dass, wenn Sie `LATEST` als Startposition für den Stream angeben, die Zuordnung von Ereignisquellen bei der Erstellung oder Aktualisierung möglicherweise Ereignisse übersieht. Um sicherzustellen, dass keine Ereignisse übersehen werden, geben Sie die Startposition des Streams als `TRIM_HORIZON` oder `AT_TIMESTAMP` an.

Erstellen einer kontenübergreifenden Zuordnung von Ereignisquellen

Amazon Kinesis Data Streams unterstützt ressourcenbasierte Richtlinien. Aus diesem Grund können Sie Daten, die in einen Stream aufgenommen wurden, in einem Konto AWS-Konto mit einer Lambda-Funktion in einem anderen Konto verarbeiten.

Um eine Ereignisquellenzuordnung für Ihre Lambda-Funktion mithilfe eines Kinesis-Streams in einem anderen zu erstellen AWS-Konto, müssen Sie den Stream mithilfe einer ressourcenbasierten Richtlinie konfigurieren, um Ihrer Lambda-Funktion die Berechtigung zum Lesen von Elementen zu erteilen. Informationen dazu, wie Sie Ihren Stream so konfigurieren, dass er kontoübergreifenden Zugriff ermöglicht, finden Sie unter Zugriff mit kontoübergreifenden AWS Lambda Funktionen teilen im Amazon Kinesis Streams Streams-Entwicklerhandbuch.

Nachdem Sie Ihren Stream mit einer ressourcenbasierten Richtlinie konfiguriert haben, die Ihrer Lambda-Funktion die erforderlichen Berechtigungen erteilt, erstellen Sie die Ereignisquellenzuordnung mit einer der im vorherigen Abschnitt beschriebenen Methoden.

Wenn Sie Ihr Event-Quellen-Mapping mit der Lambda-Konsole erstellen möchten, fügen Sie den ARN Ihres Streams direkt in das Eingabefeld ein. Wenn Sie einen Verbraucher für Ihren Stream angeben möchten, wird das Stream-Feld durch Einfügen des ARN des Verbrauchers automatisch aufgefüllt.

Konfiguration einer partiellen Batch-Antwort mit Kinesis Data Streams und Lambda

Beim Konsumieren und Verarbeiten von Streaming-Daten aus einer Ereignisquelle werden standardmäßig Lambda-Checkpoints auf die höchste Sequenznummer eines Batches nur dann

überprüft, wenn der Batch ein voller Erfolg ist. Lambda behandelt alle anderen Ergebnisse als einen vollständigen Fehler und versucht, den Batch bis zum Wiederholungslimit zu verarbeiten. Um beim Verarbeiten von Stapeln aus einem Stream Teilerfolge zu ermöglichen, aktivieren Sie `ReportBatchItemFailures`. Das Zulassen von Teilerfolgen kann dazu beitragen, die Anzahl der Wiederholungen in einer Aufzeichnung zu reduzieren, obwohl die Möglichkeit von Wiederholungen in einer erfolgreichen Aufzeichnung nicht vollständig verhindert wird.

Um die Option zu aktivieren`ReportBatchItemFailures`, nehmen Sie den Enum-Wert **`ReportBatchItemFailures`** in die Typenliste auf. FunctionResponse Diese Liste zeigt an, welche Antworttypen für Ihre Funktion aktiviert sind. Sie können diese Liste konfigurieren, wenn Sie eine Ereignisquellenzuordnung erstellen oder aktualisieren.

Berichtsyntax

Beim Konfigurieren von Berichten zu Batch-Elementfehlern wird die `StreamsEventResponse`-Klasse mit einer Liste von Batch-Elementfehlern zurückgegeben. Sie können ein `StreamsEventResponse`-Objekt verwenden, um die Sequenznummer des ersten fehlgeschlagenen Datensatzes im Batch zurückzugeben. Sie können auch Ihre eigene benutzerdefinierte Klasse mit der richtigen Antwortsyntax erstellen. Die folgende JSON-Struktur zeigt die erforderliche Antwortsyntax:

```
{
  "batchItemFailures": [
        {
            "itemIdentifier": "<SequenceNumber>"
        }
    ]
}
```

> **Note**
>
> Wenn das `batchItemFailures`-Array mehrere Elemente enthält, verwendet Lambda den Datensatz mit der niedrigsten Sequenznummer als Kontrollpunkt. Lambda wiederholt dann alle Datensätze ab diesem Kontrollpunkt.

Erfolgs- und Misserfolgsbedingungen

Lambda behandelt einen Batch als vollständigen Erfolg, wenn Sie eines der folgenden Elemente zurückgeben:

- Eine leere `batchItemFailure`-Liste
- Eine ungültige `batchItemFailure`-Liste
- Ein leeres `EventResponse`
- Ein ungültiges `EventResponse`

Lambda behandelt einen Batch als vollständigen Misserfolg, wenn Sie eines der folgenden Elemente zurückgeben:

- Eine leere Zeichenfolge `itemIdentifier`
- Ein ungültiges `itemIdentifier`
- Ein `itemIdentifier` mit einem falschen Schlüsselnamen

Lambda wiederholt Fehler basierend auf Ihrer Wiederholungsstrategie.

Einen Batch halbieren

Wenn Ihr Aufruf fehlschlägt und `BisectBatchOnFunctionError` eingeschaltet ist, wird der Stapel unabhängig von Ihrer `ReportBatchItemFailures`-Einstellung halbiert.

Wenn eine partielle Batch-Erfolgsantwort empfangen wird und sowohl `BisectBatchOnFunctionError` als auch `ReportBatchItemFailures` aktiviert sind, wird der Batch mit der zurückgegebenen Sequenznummer halbiert und Lambda versucht nur die verbleibenden Datensätze erneut.

Hier sind einige Beispiele für Funktionscodes, die die Liste der fehlgeschlagenen Nachrichten-IDs im Batch zurückgeben:

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
 ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return new StreamsEventResponse();
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
```

```
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                return new StreamsEventResponse
                {
                    BatchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>
                    {
                        new StreamsEventResponse.BatchItemFailure
 { ItemIdentifier = record.Kinesis.SequenceNumber }
                    }
                };
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
        return new StreamsEventResponse();
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}

public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Artikeln mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, record := range kinesisEvent.Records {
  curRecordSequenceNumber := ""

  // Process your record
  if /* Your record processing condition here */ {
   curRecordSequenceNumber = record.Kinesis.SequenceNumber
  }

  // Add a condition to check if the record processing failed
  if curRecordSequenceNumber != "" {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": curRecordSequenceNumber})
  }
 }

 kinesisBatchResponse := map[string]interface{}{
```

```
  "batchItemFailures": batchItemFailures,
 }
 return kinesisBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
 StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
```

```
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
 input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
 kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse(batchItemFailures);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Javascript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
```

```
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";
```

```
const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  logger.info(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $kinesisEvent = new KinesisEvent($event);
        $this->logger->info("Processing records");
        $records = $kinesisEvent->getRecords();
```

```
        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
```

```
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
 immediately.
      # Lambda will immediately begin to retry processing from this failed item
 onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
  sleep(1)
  data
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
```

```
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
 Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",
            record.event_id.as_deref().unwrap_or_default()
        );

        let record_processing_result = process_record(record);

        if record_processing_result.is_err() {
            response.batch_item_failures.push(KinesisBatchItemFailure {
                item_identifier: record.kinesis.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());
```

```
    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Verworfene Batch-Datensätze für eine Kinesis Data Streams Streams-Ereignisquelle in Lambda aufbewahren

Die Fehlerbehandlung für Kinesis-Ereignisquellenzuordnungen hängt davon ab, ob der Fehler vor dem Aufruf der Funktion oder während des Funktionsaufrufs auftritt:

- Vor dem Aufruf: Wenn eine Lambda-Ereignisquellenzuordnung die Funktion aufgrund von Drosselung oder anderen Problemen nicht aufrufen kann, versucht sie es erneut, bis die Datensätze ablaufen oder das in der Ereignisquellenzuordnung konfigurierte Höchstalter (Sekunden) überschreiten. MaximumRecord AgeIn
- Während des Aufrufs: Wenn die Funktion aufgerufen wird, aber einen Fehler zurückgibt, versucht Lambda es erneut, bis die Datensätze ablaufen, das Höchstalter

(MaximumRecordAgeInSekunden) überschreiten oder das konfigurierte Wiederholungskontingent (Versuche) erreicht haben. MaximumRetry Bei Funktionsfehlern können Sie auch BisectBatchOnFunctionError konfigurieren, wodurch ein fehlgeschlagener Batch in zwei kleinere Batches aufgeteilt wird, wodurch fehlerhafte Datensätze isoliert und Timeouts vermieden werden. Durch das Aufteilen von Batches wird das Wiederholungskontingent nicht aufgebraucht.

Wenn die Fehlerbehandlungsmaßnahmen fehlschlagen, verwirft Lambda die Datensätze und setzt die Verarbeitung von Batches aus dem Stream fort. Bei den Standardeinstellungen bedeutet dies, dass ein fehlerhafter Datensatz die Verarbeitung auf dem betroffenen Shard für bis zu eine Woche blockieren kann. Um dies zu vermeiden, konfigurieren Sie die Ereignisquellenzuordnung Ihrer Funktion mit einer angemessenen Anzahl von Wiederholungen und einem maximalen Datensatzalter, das zu Ihrem Anwendungsfall passt.

Konfiguration von Zielen für fehlgeschlagene Aufrufe

Um Datensätze zu fehlgeschlagenen Aufrufen zur Zuordnung von Ereignisquellen beizubehalten, fügen Sie der Zuordnung von Ereignisquellen Ihrer Funktion ein Ziel hinzu. Jeder Datensatz, der an das Ziel gesendet wird, ist ein JSON-Dokument mit Metadaten über den fehlgeschlagenen Aufruf. Sie können jedes Amazon SNS SNS-Thema oder jede Amazon SQS SQS-Warteschlange als Ziel konfigurieren. Ihre Ausführungsrolle muss über Berechtigungen für das Ziel verfügen:

- Für SQS-Ziele: sqs: SendMessage
- Für SNS-Ziele: sns:Publish

Gehen Sie folgendermaßen vor, um ein Ausfallziel mit der Konsole zu konfigurieren:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add destination (Ziel hinzufügen).
4. Wählen Sie als Quelle die Option Aufruf der Zuordnung von Ereignisquellen aus.
5. Wählen Sie für die Zuordnung von Ereignisquellen eine Ereignisquelle aus, die für diese Funktion konfiguriert ist.
6. Wählen Sie für Bedingung die Option Bei Ausfall aus. Für Aufrufe zur Zuordnung von Ereignisquellen ist dies die einzig akzeptierte Bedingung.
7. Wählen Sie unter Zieltyp den Zieltyp aus, an den Lambda Aufrufdatensätze sendet.

8. Wählen Sie unter Destination (Ziel) eine Ressource aus.
9. Wählen Sie Save aus.

Sie können mit () auch ein Ziel für den Fall eines Fehlers konfigurieren. AWS Command Line Interface AWS CLI Mit dem folgenden Befehl create-event-source-mapping wird beispielsweise eine Ereignisquellenzuordnung mit einem SQS-Ziel für den Fall eines Fehlers hinzugefügt: `MyFunction`

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

Der folgende Befehl update-event-source-mapping aktualisiert eine Ereignisquellenzuordnung, sodass fehlgeschlagene Aufrufdatensätze nach zwei Wiederholungsversuchen oder wenn die Datensätze älter als eine Stunde sind, an ein SNS-Ziel gesendet werden.

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--maximum-retry-attempts 2 \
--maximum-record-age-in-seconds 3600 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sns:us-
east-1:123456789012:dest-topic"}}'
```

Aktualisierte Einstellungen werden asynchron angewendet und werden erst nach Abschluss des Vorgangs in der Ausgabe berücksichtigt. Verwenden Sie den Befehl get-event-source-mapping, um den aktuellen Status anzuzeigen.

Um ein Ziel zu entfernen, geben Sie eine leere Zeichenfolge als Argument für den `destination-config`-Parameter an:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Das folgende Beispiel zeigt, was Lambda bei einem fehlgeschlagenen Aufruf der Kinesis-Ereignisquelle an eine SQS-Warteschlange oder ein SNS-Thema sendet. Da Lambda nur die Metadaten für diese Zieltypen sendet, verwenden Sie die `endSequenceNumber` Felder`streamArn`,, und `shardId``startSequenceNumber`, um den vollständigen Originaldatensatz abzurufen.

```
{
    "requestContext": {
        "requestId": "c9b8fa9f-5a7f-xmpl-af9c-0c604cde93a5",
        "functionArn": "arn:aws:lambda:us-east-2:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted",
        "approximateInvokeCount": 1
    },
    "responseContext": {
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KinesisBatchInfo": {
        "shardId": "shardId-000000000001",
        "startSequenceNumber":
 "49601189658422359378836298521827638475320189012309704722",
        "endSequenceNumber":
 "49601189658422359378836298522902373528957594348623495186",
        "approximateArrivalOfFirstRecord": "2019-11-14T00:38:04.835Z",
        "approximateArrivalOfLastRecord": "2019-11-14T00:38:05.580Z",
        "batchSize": 500,
        "streamArn": "arn:aws:kinesis:us-east-2:123456789012:stream/mystream"
    }
}
```

Sie können diese Informationen verwenden, um die betroffenen Datensätze aus dem Stream für die Fehlersuche abzurufen. Die tatsächlichen Datensätze sind nicht enthalten, daher müssen Sie diesen Datensatz verarbeiten und aus dem Stream abrufen, bevor sie ablaufen und verloren gehen.

Implementierung der statusbehafteten Kinesis Data Streams Streams-Verarbeitung in Lambda

Lambda-Funktionen können kontinuierliche Stream-Verarbeitungsanwendungen ausführen. Ein Stream entspricht einer unbegrenzten Menge von Daten, die kontinuierlich durch Ihre Anwendung fließen. Um Informationen aus dieser sich ständig aktualisierenden Eingabe zu analysieren, können Sie die enthaltenen Datensätze mithilfe eines zeitlich definierten Fensters binden.

Rollierende Fenster sind unterschiedliche Zeitfenster, die sich in regelmäßigen Abständen öffnen und schließen. Standardmäßig sind Lambda-Aufrufe zustandslos – Sie können sie nicht für die

Verarbeitung von Daten über mehrere kontinuierliche Aufrufe hinweg ohne eine externe Datenbank verwenden. Mit rollierenden Fenstern können Sie jedoch Ihren Status über Aufrufe hinweg beibehalten. Dieser Zustand enthält das Gesamtergebnis der Nachrichten, die zuvor für das aktuelle Fenster verarbeitet wurden. Ihr Zustand kann maximal 1 MB pro Shard betragen. Wenn er diese Größe überschreitet, wird Lambda das Fenster vorzeitig beenden.

Jeder Datensatz in einem Stream gehört zu einem bestimmten Fenster. Lambda verarbeitet jeden Datensatz mindestens einmal, garantiert jedoch nicht, dass jeder Datensatz nur einmal verarbeitet wird. In seltenen Fällen, etwa bei der Fehlerbehandlung, werden einige Datensätze möglicherweise mehrmals verarbeitet. Datensätze werden beim ersten Mal immer in der richtigen Reihenfolge verarbeitet. Wenn Datensätze mehr als einmal verarbeitet werden, werden sie nicht in der richtigen Reihenfolge verarbeitet.

Aggregation und Verarbeitung

Ihre benutzerverwaltete Funktion wird sowohl zur Aggregation als auch zur Verarbeitung der Endergebnisse dieser Aggregation aufgerufen. Lambda aggregiert alle im Fenster empfangenen Datensätze. Sie können diese Datensätze in mehreren Stapeln erhalten, jeweils als ein separater Aufruf. Jeder Aufruf erhält einen Zustand. Wenn Sie also rollierende Fenster verwenden, muss Ihre Lambda-Funktionsantwort eine `state`-Eigenschaft enthalten. Wenn die Antwort keine `state`-Eigenschaft enthält, betrachtet Lambda dies als fehlgeschlagenen Aufruf. Um diese Bedingung zu erfüllen, kann Ihre Funktion ein `TimeWindowEventResponse`-Objekt zurückgeben, das die folgende JSON-Form aufweist:

Example **`TimeWindowEventResponse`**-Werte

```
{
    "state": {
        "1": 282,
        "2": 715
    },
    "batchItemFailures": []
}
```

> **Note**
>
> Für Java-Funktionen empfehlen wir, eine `Map<String, String>` zu verwenden, um den Status darzustellen.

Am Ende des Fensters wird das Flag `isFinalInvokeForWindow` auf `true` gesetzt, um anzugeben, dass es sich um den Endzustand handelt und dass es für die Verarbeitung bereit ist. Nach der Verarbeitung werden das Fenster und Ihr endgültiger Aufruf wird abgeschlossen, und dann wird der Zustand gelöscht.

Am Ende Ihres Fensters verwendet Lambda die endgültige Verarbeitung für Aktionen an den Aggregationsergebnissen. Ihre endgültige Verarbeitung wird synchron aufgerufen. Nach erfolgreichem Aufruf zeigt Ihre Funktion auf die Sequenznummer und die Stream-Verarbeitung wird fortgesetzt. Wenn der Aufruf nicht erfolgreich ist, unterbricht Ihre Lambda-Funktion die weitere Verarbeitung bis zu einem erfolgreichen Aufruf.

Example KinesisTimeWindowEvent

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1607497475.000
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-kinesis-role",
            "awsRegion": "us-east-1",
            "eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-
stream"
        }
    ],
    "window": {
        "start": "2020-12-09T07:04:00Z",
        "end": "2020-12-09T07:06:00Z"
    },
    "state": {
        "1": 282,
```

```
        "2": 715
    },
    "shardId": "shardId-000000000006",
    "eventSourceARN": "arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream",
    "isFinalInvokeForWindow": false,
    "isWindowTerminatedEarly": false
}
```

Konfiguration

Sie können rollierende Fenster konfigurieren, wenn Sie eine Ereignisquellenzuordnung erstellen oder aktualisieren. Um ein Tumbling-Fenster zu konfigurieren, geben Sie das Fenster in Sekunden an (). TumblingWindowInSeconds Der folgende Beispielbefehl AWS Command Line Interface (AWS CLI) erstellt eine Quellenzuordnung für Streaming-Ereignisse mit einem Wechselfenster von 120 Sekunden. Die für Aggregation und Verarbeitung definierte Lambda-Funktion wird `tumbling-window-example-function` genannt.

```
aws lambda create-event-source-mapping \
--event-source-arn arn:aws:kinesis:us-east-1:123456789012:stream/lambda-stream \
--function-name tumbling-window-example-function \
--starting-position TRIM_HORIZON \
--tumbling-window-in-seconds 120
```

Lambda bestimmt die rollierenden Fenstergrenzen basierend auf dem Zeitpunkt, zu dem Datensätze in den Stream eingefügt wurden. Für alle Datensätze steht ein ungefährer Zeitstempel zur Verfügung, den Lambda in Grenzbestimmungen verwendet.

Rollierende Fensteraggregationen unterstützen kein Resharding. Wenn ein Shard endet, betrachtet Lambda das aktuelle Fenster als geschlossen, und alle untergeordneten Shards beginnen ihr eigenes Fenster in einem neuen Zustand. Wenn dem aktuellen Fenster keine neuen Datensätze hinzugefügt werden, wartet Lambda bis zu 2 Minuten, bevor es annimmt, dass das Fenster vorbei ist. Dadurch wird sichergestellt, dass die Funktion alle Datensätze im aktuellen Fenster liest, auch wenn die Datensätze zeitweise hinzugefügt werden.

Rollierende Fenster unterstützen vollständig die bestehenden Wiederholungsrichtlinien `maxRetryAttempts` und `maxRecordAge`.

Example Handler.py – Aggregation und Verarbeitung

Die folgende Python-Funktion veranschaulicht, wie Sie Ihren Endzustand aggregieren und dann verarbeiten:

```
def lambda_handler(event, context):
    print('Incoming event: ', event)
    print('Incoming state: ', event['state'])

#Check if this is the end of the window to either aggregate or process.
    if event['isFinalInvokeForWindow']:
        # logic to handle final state of the window
        print('Destination invoke')
    else:
        print('Aggregate invoke')

#Check for early terminations
    if event['isWindowTerminatedEarly']:
        print('Window terminated early')

    #Aggregation logic
    state = event['state']
    for record in event['Records']:
        state[record['kinesis']['partitionKey']] = state.get(record['kinesis']
['partitionKey'], 0) + 1

    print('Returning state: ', state)
    return {'state': state}
```

Lambda-Parameter für Amazon Kinesis Data Streams Streams-Ereignisquellenzuordnungen

Alle Lambda-Ereignisquellenzuordnungen verwenden dieselben API-Operationen CreateEventSourceMapping. UpdateEventSourceMapping Allerdings gelten nur einige der Parameter für Kinesis.

Ereignisquellparameter, die für Kinesis gelten

Parameter	Erforderlich	Standard	Hinweise
BatchSize	N	100	Höchstwert: 10 000.
BisectBatchOnFunctionFehler	N	false	
DestinationConfig	N		Amazon SQS SQS-Warteschlange

Parameter	Erforderlich	Standard	Hinweise
			oder Amazon SNS SNS-Themenziel für verworfene Datensätze. Weitere Informationen finden Sie unter Konfiguration von Zielen für fehlgeschlagene Aufrufe.
Aktiviert	N	true	
EventSourceArn	Y		Der ARN des Datenstroms oder eines Stream-Konsumenten
FunctionName	Y		
FunctionResponseTypen	N		Damit Ihre Funktion bestimmte Fehler in einem Batch meldet, beziehen Sie den Wert `ReportBatchItemFailures` in `FunctionResponseTypes` ein. Weitere Informationen finden Sie unter Konfiguration einer partiellen Batch-Antwort mit Kinesis Data Streams und Lambda.
MaximumBatchingWindowInSekunden	N	0	

Parameter	Erforderlich	Standard	Hinweise
MaximumRecordAgeInSekunden	N	-1	-1 bedeutet unendlich : Lambda verwirft keine Datensätze (die Datenaufbewahrungseinstellungen von Kinesis Data Streams gelten weiterhin) Minimum: -1 Höchstwert: 604 800
MaximumRetryVersuche	N	-1	-1 bedeutet unendlich : Fehlgeschlagene Datensätze werden wiederholt, bis der Datensatz abläuft Minimum: -1 Höchstwert: 10 000.
ParallelizationFactor	N	1	Maximum: 10
StartingPosition	Y		AT_TIMESTAMP, TRIM_HORIZON, oder LATEST
StartingPositionZeitstempel	N		Nur gültig, wenn auf StartingPosition AT_TIMESTAMP gesetzt ist. Die Zeit, ab der mit dem Lesen begonnen werden soll, in Unix-Zeit sekunden

Parameter	Erforderlich	Standard	Hinweise
TumblingWindowInSeconds	N		Minimum: 0 Maximum: 900

Tutorial: Lambda mit Kinesis Data Streams verwenden

In diesem Tutorial erstellen Sie eine Lambda-Funktion, um Ereignisse aus einem Amazon Kinesis Kinesis-Datenstream zu verarbeiten.

1. Die benutzerdefinierte Anwendung schreibt die Datensätze zum Stream.
2. AWS Lambda fragt den Stream ab und ruft, wenn es neue Datensätze im Stream erkennt, Ihre Lambda-Funktion auf.
3. AWS Lambda führt die Lambda-Funktion aus, indem es die Ausführungsrolle annimmt, die Sie bei der Erstellung der Lambda-Funktion angegeben haben.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen der Ausführungsrolle

Erstellen Sie die Ausführungsrolle, die Ihrer Funktion die Berechtigung zum Zugriff auf AWS Ressourcen erteilt.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.
   - Trusted entity (Vertrauenswürdige Entität – AWS Lambda.
   - Berechtigungen — AWSLambdaKinesisExecutionRole.
   - Role name (Name der Rolle – **`lambda-kinesis-role`**.

Die AWSLambdaKinesisExecutionRoleRichtlinie verfügt über die Berechtigungen, die die Funktion benötigt, um Elemente aus Kinesis zu lesen und Protokolle in Logs zu CloudWatch schreiben.

Erstellen der Funktion

Erstellen Sie eine Lambda-Funktion, die Ihre Kinesis-Nachrichten verarbeitet. Der Funktionscode protokolliert die Ereignis-ID und die Ereignisdaten des Kinesis-Datensatzes in CloudWatch Logs.

In diesem Tutorial wird die Node.js 18.x-Laufzeit verwendet. Es stehen aber auch Beispielcodes für andere Laufzeitensprachen zur Verfügung. Sie können die Registerkarte im folgenden Feld auswählen, um Code für die gewünschte Laufzeit anzusehen. Der JavaScript Code, den Sie in diesem Schritt verwenden, befindet sich im ersten Beispiel, das auf der JavaScriptRegisterkarte angezeigt wird.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegrationSampleCode;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
```

```
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main
```

```
import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
 if len(kinesisEvent.Records) == 0 {
  log.Printf("empty Kinesis event received")
  return nil
 }

 for _, record := range kinesisEvent.Records {
  log.Printf("processed Kinesis event with EventId: %v", record.EventID)
  recordDataBytes := record.Kinesis.Data
  recordDataText := string(recordDataBytes)
  log.Printf("record data: %v", recordDataText)
  // TODO: Do interesting work based on the new data
 }
 log.Printf("successfully processed %v records", len(kinesisEvent.Records))
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {
            logger.log("Empty Kinesis Event received");
            return null;
        }
        for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
            try {
                logger.log("Processed Event with EventId: "+record.getEventID());
                String data = new String(record.getKinesis().getData().array());
                logger.log("Data:"+ data);
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex) {
                logger.log("An error occurred:"+ex.getMessage());
                throw ex;
            }
        }
        logger.log("Successfully processed:"+event.getRecords().size()+"
 records");
        return null;
    }

}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda verwenden. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      throw err;
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Ein Kinesis-Ereignis mit Lambda verwenden. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
```

```
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      throw err;
    }
    logger.info(`Successfully processed ${event.Records.length} records.`);
  }
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda mithilfe von PHP verarbeiten.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleKinesis(KinesisEvent $event, Context $context): void
    {
        $this->logger->info("Processing records");
        $records = $event->getRecords();
        foreach ($records as $record) {
            $data = $record->getData();
```

```
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
```

```
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda unter Verwendung von Ruby verarbeiten.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
  puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
 here.
  return data
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
 {
    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    event.payload.records.iter().for_each(|record| {
        tracing::info!("EventId:
 {}",record.event_id.as_deref().unwrap_or_default());

        let record_data = std::str::from_utf8(&record.kinesis.data);

        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
```

```
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

So erstellen Sie die Funktion

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir kinesis-tutorial
cd kinesis-tutorial
```

2. Kopieren Sie den JavaScript Beispielcode in eine neue Datei mit dem Namen. `index.js`
3. Erstellen Sie ein Bereitstellungspaket.

```
zip function.zip index.js
```

4. Erstellen Sie eine Lambda-Funktion mit dem Befehl `create-function`.

```
aws lambda create-function --function-name ProcessKinesisRecords \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
--role arn:aws:iam::111122223333:role/lambda-kinesis-role
```

Lambda-Funktion testen

Rufen Sie Ihre Lambda-Funktion manuell mit dem `invoke` AWS Lambda CLI-Befehl und einem Kinesis-Beispielereignis auf.

Lambda-Funktion testen

1. Kopieren Sie das folgende JSON in eine Datei und speichern Sie sie unter `input.txt`.

```
{
    "Records": [
        {
            "kinesis": {
                "kinesisSchemaVersion": "1.0",
                "partitionKey": "1",
                "sequenceNumber":
 "49590338271490256608559692538361571095921575989136588898",
                "data": "SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
                "approximateArrivalTimestamp": 1545084650.987
            },
            "eventSource": "aws:kinesis",
            "eventVersion": "1.0",
            "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
            "eventName": "aws:kinesis:record",
            "invokeIdentityArn": "arn:aws:iam::111122223333:role/lambda-kinesis-
role",
            "awsRegion": "us-east-2",
            "eventSourceARN": "arn:aws:kinesis:us-east-2:111122223333:stream/
lambda-stream"
        }
    ]
}
```

2. Verwenden Sie den `invoke`-Befehl, um das Ereignis an die Funktion zu senden.

```
aws lambda invoke --function-name ProcessKinesisRecords \
--cli-binary-format raw-in-base64-out \
--payload file://input.txt outputfile.txt
```

Die cli-binary-format Option ist erforderlich, wenn Sie Version 2 verwenden AWS CLI . Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-`

`format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Antwort wird in gespeicher `out.txt`.

Kinesis-Stream erstellen

Verwenden Sie den Befehl `create-stream` , um einen Stream zu erstellen.

```
aws kinesis create-stream --stream-name lambda-stream --shard-count 1
```

Führen Sie den folgenden `describe-stream`-Befehl aus, um den Stream-ARN zu erhalten.

```
aws kinesis describe-stream --stream-name lambda-stream
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StreamDescription": {
        "Shards": [
            {
                "ShardId": "shardId-000000000000",
                "HashKeyRange": {
                    "StartingHashKey": "0",
                    "EndingHashKey": "340282366920746074317682119384634633455"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber":
 "49591073947768692513481539594623130411957558361251844610"
                }
            }
        ],
        "StreamARN": "arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream",
        "StreamName": "lambda-stream",
        "StreamStatus": "ACTIVE",
        "RetentionPeriodHours": 24,
        "EnhancedMonitoring": [
            {
                "ShardLevelMetrics": []
            }
```

```
        ],
        "EncryptionType": "NONE",
        "KeyId": null,
        "StreamCreationTimestamp": 1544828156.0
    }
}
```

Sie benötigen im nächsten Schritt den Stream-ARN, um die Lambda-Funktion dem Stream zuzuordnen.

Hinzufügen einer Ereignisquelle in AWS Lambda

Führen Sie den Befehl AWS CLI `add-event-source` aus.

```
aws lambda create-event-source-mapping --function-name ProcessKinesisRecords \
--event-source  arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream \
--batch-size 100 --starting-position LATEST
```

Notieren Sie die Zuweisungs-ID zur späteren Verwendung. Sie erhalten eine Liste der Zuweisungen von Ereignisquellen, indem Sie den `list-event-source-mappings`-Befehl ausführen.

```
aws lambda list-event-source-mappings --function-name ProcessKinesisRecords \
--event-source arn:aws:kinesis:us-east-1:111122223333:stream/lambda-stream
```

In der Antwort können Sie überprüfen, ob der Statuswert is `enabled`. Ereignisquellen-Zuweisungen können deaktiviert werden, um Abfragen vorübergehend zu pausieren, ohne dass Datensätze verloren gehen.

Testen der Einrichtung

Zum Testen der Ereignisquellen-Zuweisung fügen Sie Ihrem Kinesis-Stream Ereignisdatensätze hinzu. Der Wert `--data` ist eine Zeichenfolge, die die CLI vor dem Senden an Kinesis mit base64 verschlüsselt. Der gleiche Befehl kann mehrmals ausgeführt werden, um dem Stream mehrere Datensätze hinzuzufügen.

```
aws kinesis put-record --stream-name lambda-stream --partition-key 1 \
--data "Hello, this is a test."
```

Lambda verwendet die Ausführungsrolle, um Datensätze aus dem Stream zu lesen. Anschließend wird Ihre Lambda-Funktion aufgerufen und Datensatzbatches werden übergeben. Die Funktion

dekodiert Daten aus jedem Datensatz, protokolliert sie und sendet die Ausgabe an CloudWatch Logs. Zeigen Sie die Protokolle in der CloudWatch -Konsole an.

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie den Kinesis-Stream

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Kinesis-Konsole unter https://console.aws.amazon.com/kinesis.
2. Wählen Sie den von Ihnen erstellten Stream aus
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein.
5. Wählen Sie Löschen.

Verwenden von Lambda mit Amazon MQ

> **Note**
>
> Wenn Sie Daten an ein anderes Ziel als eine Lambda-Funktion senden oder die Daten vor dem Senden anreichern möchten, finden Sie weitere Informationen unter Amazon EventBridge Pipes.

Amazon MQ ist ein verwalteter Message-Broker-Service für Apache ActiveMQ und RabbitMQ. Mit einem Message Broker können Software-Anwendungen und -Komponenten mithilfe verschiedener Programmiersprachen, Betriebssysteme und formeller Messaging-Protokolle entweder über Themen- oder Queue-Ereigniszielen miteinander kommunizieren.

Amazon MQ kann auch Amazon-Elastic-Compute-Cloud-(Amazon-EC2)-Instances in Ihrem Namen verwalten, indem es ActiveMQ- oder RabbitMQ-Broker installiert und verschiedene Netzwerktopologien und andere Infrastrukturanforderungen bereitstellt.

Verwenden Sie eine Lambda-Funktion, um Datensätze von Ihrem Amazon-MQ-Message-Broker zu verarbeiten. Lambda ruft Ihre Funktion über ein Ereignisquellen-Zuweisung auf, eine Lambda-Ressource, die Nachrichten von Ihrem Broker liest und die Funktion synchron aufruft.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Das Amazon-MQ-Ereignisquellen-Zuweisung hat die folgenden Konfigurationseinschränkungen:

- Parallelität – Lambda-Funktionen, die eine Amazon MQ-Zuordnung von Ereignisquellen verwenden, haben eine Standardeinstellung für maximale Parallelität. Für ActiveMQ begrenzt der Lambda-Service die Anzahl der gleichzeitigen Ausführungsumgebungen auf fünf. Für RabbitMQ ist die Anzahl der gleichzeitigen Ausführungsumgebungen auf 1 begrenzt. Selbst wenn Sie die reservierten oder bereitgestellten Parallelitätseinstellungen Ihrer Funktion ändern, stellt der Lambda-Service keine weiteren Ausführungsumgebungen zur Verfügung. Wenn Sie eine Erhöhung

der standardmäßigen maximalen Parallelität beantragen möchten, wenden Sie sich an AWS Support.

- Kontoübergreifend – Lambda unterstützt keine kontoübergreifende Verarbeitung. Sie können Lambda nicht zur Verarbeitung von Datensätzen von einem Amazon-MQ-Message Broker verwenden, der sich in einem anderen AWS-Konto befindet.
- Authentifizierung — Für ActiveMQ wird nur das ActiveMQ SimpleAuthentication Plugin unterstützt. Für RabbitMQ wird nur der PLAIN-Authentifizierungsmechanismus unterstützt. Benutzer müssen es verwenden, AWS Secrets Manager um ihre Anmeldeinformationen zu verwalten. Weitere Informationen zur ActiveMQ-Authentifizierung finden Sie unter Integrieren von ActiveMQ-Brokern mit LDAP im Amazon-MQ-Entwicklerhandbuch.
- Verbindungskontingent – Broker haben eine maximale Anzahl zulässiger Verbindungen pro Wire-Level-Protokoll. Dieses Kontingent basiert auf dem Instance-Typ des Brokers. Weitere Informationen finden Sie im Abschnitt Broker in Kontingente in Amazon MQ im Amazon-MQ-Entwicklerhandbuch.
- Konnektivität – Sie können Broker in einer öffentlichen oder privaten Virtual Private Cloud (VPC) erstellen. Bei privaten VPCs benötigt Ihre Lambda-Funktion Zugriff auf die VPC, um Nachrichten zu empfangen. Weitere Informationen finden Sie unter the section called “Netzwerkkonfiguration” an späterer Stelle in diesem Thema.
- Ereignisziele – Es werden nur Warteschlangenziele unterstützt. Sie können jedoch ein virtuelles Thema verwenden, das sich intern wie ein Thema verhält, während es mit Lambda als eine Warteschlange interagiert. Weitere Informationen finden Sie unter virtuelle Ziele auf der Apache-ActiveMQ-Website und virtuelle Hosts auf der RabbitMQ-Website.
- Netzwerktopologie – Für ActiveMQ wird nur ein Einzelinstance- oder Standby-Broker pro Ereignisquellen-Zuweisung unterstützt. Für RabbitMQ wird nur eine Einzelinstance-Broker- oder Cluster-Bereitstellung pro Ereignisquellen-Zuweisung unterstützt. Single-Instance-Broker benötigen einen Failover-Endpunkt. Weitere Informationen zu diesen Broker-Bereitstellungsmodi finden Sie unter Aktive MQ-Broker-Architektur und Broker-Architektur von Rabbit MQ im Entwicklerhandbuch für Amazon MQ.
- Protokolle – Die unterstützten Protokolle hängen vom Typ der Amazon-MQ-Integration ab.
  - Für ActiveMQ-Integrationen verwendet Lambda Nachrichten mithilfe des OpenWire /Java Message Service (JMS) -Protokolls. Es werden keine anderen Protokolle unterstützt, um Nachrichten zu verbrauchen. Innerhalb des JMS-Protokolls werden nur `TextMessage` und `BytesMessage` unterstützt. Lambda unterstützt auch benutzerdefinierte JMS-Eigenschaften. Weitere Informationen zum OpenWire Protokoll finden Sie OpenWireauf der Apache ActiveMQ-Website.

- Bei RabbitMQ-Integrationen verbraucht Lambda Nachrichten mit dem AMQP-0-9-1-Protokoll. Es werden keine anderen Protokolle unterstützt, um Nachrichten zu verbrauchen. Weitere Informationen zur Implementierung des AMQP 0-9-1-Protokolls durch RabbitMQ finden Sie im Kompletten AMQ-0-9-1-Referenzhandbuch auf der RabbitMQ-Website.

Lambda unterstützt automatisch die neuesten Versionen von ActiveMQ und RabbitMQ, die Amazon MQ unterstützt. Die neuesten unterstützten Versionen finden Sie in den Amazon-MQ-Versionshinweisen im Amazon-MQ-Entwicklerhandbuch.

> **Note**
>
> Amazon MQ hat standardmäßig ein wöchentliches Wartungsfenster für Broker. Während dieses Zeitfensters sind Broker nicht verfügbar. Für Broker ohne Standby kann Lambda während dieses Fensters keine Nachrichten verarbeiten.

Abschnitte

Konsumentengruppe von Lambda

Um mit Amazon MQ zu interagieren, erstellt Lambda eine Verbrauchergruppe, die aus Ihren Amazon-MQ-Brokern lesen kann. Die Verbrauchergruppe wird mit derselben ID wie die Ereignisquellen-Zuweisung-UUID erstellt.

Für Amazon-MQ-Ereignisquellen batcht Lambda Datensätze und sendet sie in einer einzigen Nutzlast an Ihre Funktion. Um das Verhalten zu steuern, können Sie das Batch-Fenster und die Batch-Größe konfigurieren. Lambda pullt Nachrichten, bis es die Nutzlastgröße von maximal 6 MB verarbeitet, das Batch-Fenster abläuft oder die Anzahl der Datensätze die volle Batch-Größe erreicht. Weitere Informationen finden Sie unter Batching-Verhalten.

Die Konsumentengruppe ruft die Nachrichten als ein BLOB von Bytes ab, base64-codiert sie dann in eine einzelne JSON-Nutzlast und ruft dann Ihre Funktion auf. Wenn Ihre Funktion einen Fehler für eine der Nachrichten in einem Batch zurückgibt, wiederholt Lambda den gesamten Nachrichtenbatch, bis die Verarbeitung erfolgreich ist oder die Nachrichten ablaufen.

> **Note**
>
> Während Lambda-Funktionen in der Regel ein maximales Timeout-Limit von 15 Minuten haben, unterstützen Ereignisquellenzuordnungen für Amazon MSK, selbstverwaltetes Apache Kafka, Amazon DocumentDB, Amazon MQ für ActiveMQ und RabbitMQ nur Funktionen mit einem maximalen Timeout-Limit von 14 Minuten. Diese Einschränkung stellt sicher, dass die Ereignisquellenzuordnung Funktionsfehler und Wiederholungsversuche ordnungsgemäß verarbeiten kann.

Sie können die Parallelitätsnutzung einer bestimmten Funktion mithilfe der `ConcurrentExecutions` Metrik in Amazon CloudWatch überwachen. Weitere Hinweise zur Gleichzeitigkeitsskalierung finden Sie unter the section called “Konfigurieren reservierter Gleichzeitigkeit”.

Example Amazon-MQ-Datensatzereignisse

ActiveMQ

```
{
   "eventSource": "aws:mq",
   "eventSourceArn": "arn:aws:mq:us-
west-2:111122223333:broker:test:b-9bcfa592-423a-4942-879d-eb284b418fc8",
   "messages": [
      {
        "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
west-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
        "messageType": "jms/text-message",
        "deliveryMode": 1,
        "replyTo": null,
        "type": null,
        "expiration": "60000",
        "priority": 1,
        "correlationId": "myJMSCoID",
        "redelivered": false,
        "destination": {
```

```
          "physicalName": "testQueue"
        },
        "data":"QUJDOkFBQUE=",
        "timestamp": 1598827811958,
        "brokerInTime": 1598827811958,
        "brokerOutTime": 1598827811959,
        "properties": {
          "index": "1",
          "doAlarm": "false",
          "myCustomProperty": "value"
        }
      },
      {
        "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
west-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
        "messageType": "jms/bytes-message",
        "deliveryMode": 1,
        "replyTo": null,
        "type": null,
        "expiration": "60000",
        "priority": 2,
        "correlationId": "myJMSCoID1",
        "redelivered": false,
        "destination": {
          "physicalName": "testQueue"
        },
        "data":"LQaGQ82S48k=",
        "timestamp": 1598827811958,
        "brokerInTime": 1598827811958,
        "brokerOutTime": 1598827811959,
        "properties": {
          "index": "1",
          "doAlarm": "false",
          "myCustomProperty": "value"
        }
      }
   ]
}
```

RabbitMQ

```
{
```

```
  "eventSource": "aws:rmq",
  "eventSourceArn": "arn:aws:mq:us-
west-2:111122223333:broker:pizzaBroker:b-9bcfa592-423a-4942-879d-eb284b418fc8",
  "rmqMessagesByQueue": {
    "pizzaQueue::/": [
      {
        "basicProperties": {
          "contentType": "text/plain",
          "contentEncoding": null,
          "headers": {
            "header1": {
              "bytes": [
                118,
                97,
                108,
                117,
                101,
                49
              ]
            },
            "header2": {
              "bytes": [
                118,
                97,
                108,
                117,
                101,
                50
              ]
            },
            "numberInHeader": 10
          },
          "deliveryMode": 1,
          "priority": 34,
          "correlationId": null,
          "replyTo": null,
          "expiration": "60000",
          "messageId": null,
          "timestamp": "Jan 1, 1970, 12:33:41 AM",
          "type": null,
          "userId": "AIDACKCEVSQ6C2EXAMPLE",
          "appId": null,
          "clusterId": null,
          "bodySize": 80
```

```
        },
        "redelivered": false,
        "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
      }
    ]
  }
}
```

> **Note**
>
> Im RabbitMQ-Beispiel ist `pizzaQueue` der Name der RabbitMQ-Warteschlange und `/` der Name des virtuellen Hosts. Beim Empfang von Nachrichten listet die Ereignisquelle Nachrichten unter `pizzaQueue::/` auf.

Berechtigungen für die Ausführungsrolle

Um Datensätze von einem Amazon-MQ-Broker zu lesen, benötigt Ihre Lambda-Funktion die folgenden Berechtigungen, die ihrer Ausführungsrolle hinzugefügt werden:

- mq: DescribeBroker
- secretsmanager: Wert GetSecret
- ec2: Schnittstelle CreateNetwork
- ec2: Schnittstelle DeleteNetwork
- ec2: Schnittstellen DescribeNetwork
- ec2: Gruppen DescribeSecurity
- ec2: DescribeSubnets
- ec2: DescribeVpcs
- protokolle: Gruppe CreateLog
- Protokolle: CreateLog Stream
- Protokolle: PutLog Ereignisse

> **Note**
>
> Wenn Sie einen verschlüsselten, von Kunden verwalteten Schlüssel verwenden, fügen Sie auch die `kms:Decrypt`-Berechtigung hinzu.

Netzwerkkonfiguration

Um Lambda über die Zuordnung von Ereignisquellen Vollzugriff auf Ihren Broker zu gewähren, muss Ihr Broker entweder einen öffentlichen Endpunkt (öffentliche IP-Adresse) verwenden oder Sie müssen Zugriff auf die Amazon-VPC gewähren, in der Sie den Broker erstellt haben.

Bei der Erstellung eines Amazon-MQ-Brokers wird das Flag `PubliclyAccessible` standardmäßig auf „false“ festgelegt. Damit Ihr Broker eine öffentliche IP-Adresse erhält, muss das Flag `PubliclyAccessible` auf „true“ festgelegt werden.

Eine bewährte Methode für die Verwendung von Amazon MQ mit Lambda besteht darin, AWS PrivateLink VPC-Endpunkte zu verwenden und Ihrer Lambda-Funktion Zugriff auf die VPC Ihres Brokers zu gewähren. Stellen Sie einen Endpunkt für Lambda und, nur für ActiveMQ, einen Endpunkt für AWS Security Token Service () bereit.AWS STS Wenn Ihr Broker Authentifizierung verwendet, stellen Sie auch einen Endpunkt für bereit. AWS Secrets Manager Weitere Informationen hierzu finden Sie unter the section called “Arbeiten mit VPC-Endpunkten”.

Alternativ können Sie in jedem öffentlichen Subnetz in der VPC, die Ihren Amazon MQ-Broker enthält, ein NAT-Gateway konfigurieren. Weitere Informationen finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Wenn Sie eine Ereignisquellenzuordnung für einen Amazon MQ-Broker erstellen, prüft Lambda, ob Elastic Network Interfaces (ENIs) bereits für die Subnetze und Sicherheitsgruppen der VPC Ihres Brokers vorhanden sind. Wenn Lambda vorhandene ENIs findet, versucht es, sie wiederzuverwenden. Andernfalls erstellt Lambda neue ENIs, um eine Verbindung zur Ereignisquelle herzustellen und Ihre Funktion aufzurufen.

> **Note**
>
> Lambda-Funktionen werden immer in VPCs ausgeführt, die dem Lambda-Service gehören. Diese VPCs werden automatisch vom Service verwaltet und sind für Kunden nicht sichtbar. Sie können Ihre Funktion auch mit einer Amazon VPC verbinden. In beiden Fällen hat die VPC-Konfiguration Ihrer Funktion keinen Einfluss auf die Zuordnung der Ereignisquelle. Nur

die Konfiguration der VPC der Ereignisquelle bestimmt, wie Lambda eine Verbindung zu Ihrer Ereignisquelle herstellt.

VPC-Sicherheitsgruppenregeln

Konfigurieren Sie die Sicherheitsgruppen für die Amazon VPC, die Ihren Cluster enthält, mit den folgenden Regeln (mindestens):

- Regeln für eingehenden Datenverkehr: Lassen Sie den gesamten Datenverkehr am Broker-Port für die Sicherheitsgruppe, die für Ihre Ereignisquelle angegeben ist, innerhalb der eigenen Sicherheitsgruppe zu. ActiveMQ verwendet standardmäßig Port 61617. RabbitMQ verwendet standardmäßig Port 5671.
- Ausgehende Regeln - Erlauben Sie allen Datenverkehr auf Port 443 für alle Ziele. Lassen Sie den gesamten Datenverkehr am Broker-Port innerhalb der eigenen Sicherheitsgruppe zu. ActiveMQ verwendet standardmäßig Port 61617. RabbitMQ verwendet standardmäßig Port 5671.
- Wenn Sie VPC-Endpunkte anstelle eines NAT-Gateways verwenden, müssen die Sicherheitsgruppen, die mit den VPC-Endpunkten verknüpft sind, den gesamten eingehenden Datenverkehr für Port 443 von den Sicherheitsgruppen der Ereignisquelle zulassen.

Arbeiten mit VPC-Endpunkten

Wenn Sie VPC-Endpunkte verwenden, werden API-Aufrufe zum Aufrufen Ihrer Funktion mithilfe der ENIs über diese Endpunkte geleitet. Der Lambda-Serviceprinzipal muss alle Funktionen aufrufen`lambda:InvokeFunction`, die diese ENIs verwenden. Darüber hinaus muss der Lambda-Serviceprinzipal für ActiveMQ Rollen aufrufen`sts:AssumeRole`, die die ENIs verwenden.

Standardmäßig haben VPC-Endpoints offene IAM-Richtlinien. Es hat sich bewährt, diese Richtlinien so einzuschränken, dass nur bestimmte Prinzipale die erforderlichen Aktionen über diesen Endpunkt ausführen können. Um sicherzustellen, dass Ihre Ereignisquellenzuordnung Ihre Lambda-Funktion aufrufen kann, muss die VPC-Endpunktrichtlinie zulassen, dass das Lambda-Serviceprinzip aufgerufen wird `lambda:InvokeFunction` und, für ActiveMQ,. `sts:AssumeRole` Wenn Sie Ihre VPC-Endpunktrichtlinien so einschränken, dass sie nur API-Aufrufe zulassen, die ihren Ursprung in Ihrer Organisation haben, verhindert, dass die Zuordnung der Ereignisquellen ordnungsgemäß funktioniert.

Die folgenden VPC-Endpunktrichtlinien zeigen, wie der erforderliche Zugriff für AWS STS und Lambda-Endpoints gewährt wird.

Example VPC-Endpunktrichtlinie — AWS STS Endpunkt (nur ActiveMQ)

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Example VPC-Endpunktrichtlinie — Lambda-Endpunkt

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Wenn Ihr Amazon MQ-Broker Authentifizierung verwendet, können Sie auch die VPC-Endpunktrichtlinie für den Secrets Manager Manager-Endpunkt einschränken. Um die Secrets Manager Manager-API aufzurufen, verwendet Lambda Ihre Funktionsrolle, nicht den Lambda-Serviceprinzipal. Das folgende Beispiel zeigt eine Secrets Manager Manager-Endpunktrichtlinie.

Example VPC-Endpunktrichtlinie — Secrets Manager Manager-Endpunkt

```
{
```

```
    "Statement": [
        {
            "Action": "secretsmanager:GetSecretValue",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "customer_function_execution_role_arn"
                ]
            },
            "Resource": "customer_secret_arn"
        }
    ]
}
```

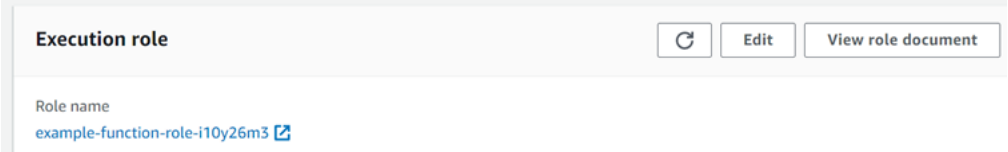
Fügen Sie Berechtigungen hinzu und erstellen Sie die Zuordnung der Ereignisquellen

Erstellen Sie ein Ereignisquellen-Zuweisung, um Lambda anzuweisen, Datensätze aus einem Amazon-MQ-Broker an eine Lambda-Funktion zu senden. Sie können mehrere Ereignisquellen-Zuweisungen erstellen, um gleiche Daten mit mehreren Funktionen oder Elemente aus mehreren Streams mit nur einer Funktion zu verarbeiten.

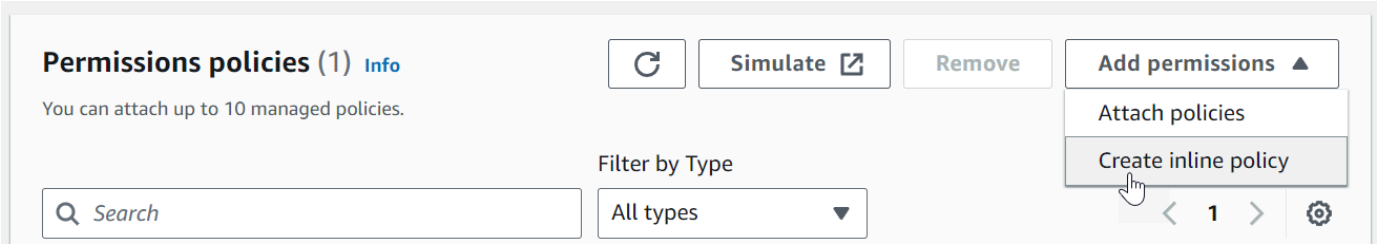
Um Ihre Funktion für das Lesen aus Amazon MQ zu konfigurieren, fügen Sie die erforderlichen Berechtigungen hinzu und erstellen Sie einen MQ-Trigger in der Lambda-Konsole.

Um Berechtigungen hinzuzufügen und einen Trigger zu erstellen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Berechtigungen aus.
4. Wählen Sie unter Rollenname den Link zu Ihrer Ausführungsrolle aus. Dieser Link öffnet die Rolle in der IAM-Konsole.



5. Wählen Sie Berechtigungen hinzufügen und dann Inline-Richtlinie erstellen aus.



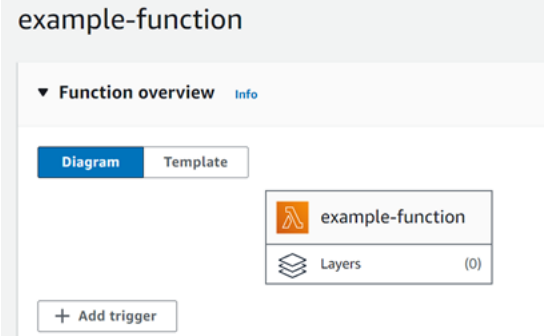
6. Wählen Sie im Richtlinieneditor JSON aus. Geben Sie die folgende Richtlinie ein: Ihre Funktion benötigt diese Berechtigungen, um von einem Amazon MQ-Broker lesen zu können.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mq:DescribeBroker",
        "secretsmanager:GetSecretValue",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Wenn Sie einen verschlüsselten, vom Kunden verwalteten Schlüssel verwenden, müssen Sie auch die `kms:Decrypt` Berechtigung hinzufügen.

7. Wählen Sie Weiter aus. Geben Sie einen Richtliniennamen ein und wählen Sie dann Richtlinie erstellen aus.

8. Kehren Sie zu Ihrer Funktion in der Lambda-Konsole zurück. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).



9. Wählen Sie den MQ-Triggertyp.
10. Konfigurieren Sie die erforderlichen Optionen und wählen Sie dann Add (Hinzufügen) aus.

Lambda unterstützt die folgenden Optionen für Amazon-MQ-Ereignisquellen.

- MQ-Broker – Wählen Sie einen Amazon-MQ-Broker aus.
- Batchgröße – Legen Sie die maximale Anzahl von Nachrichten fest, die in einem einzelnen Batch abgerufen werden sollen.
- Name der Warteschlange – Geben Sie die zu konsumierende Amazon-MQ-Warteschlange ein.
- Konfiguration des Zugriffs – Geben Sie die Informationen zum virtuellen Host und das Secrets Manager-Geheimnis ein, in dem Ihre Broker-Anmeldeinformationen gespeichert sind.
- Auslöser aktivieren – Deaktivieren Sie den Auslöser, um die Verarbeitung von Datensätzen anzuhalten.

Um den Auslöser zu aktivieren oder zu deaktivieren (oder zu löschen), wählen Sie den MQ-Auslöser im Designer aus. Verwenden Sie zum Neukonfigurieren des Auslösers die API-Vorgänge für die Ereignisquellen-Zuweisung.

Aktualisieren Sie die Zuordnung der Ereignisquellen

Verwenden Sie den `update-event-source-mapping` Befehl, um eine Ereignisquellenzuordnung zu aktualisieren. Der folgende Beispielbefehl aktualisiert eine Ereignisquellen-Zuweisung auf eine Stapelgröße von 2.

```
aws lambda update-event-source-mapping \
--uuid 91eaeb7e-c976-1234-9451-8709db01f137 \
```

```
--batch-size 2
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "UUID": "91eaeb7e-c976-1234-9451-8709db01f137",
    "BatchSize": 2,
    "EventSourceArn": "arn:aws:mq:us-east-1:123456789012:broker:ExampleMQBroker:b-
b4d492ef-bdc3-45e3-a781-cd1a3102ecca",
    "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:MQ-Example-
Function",
    "LastModified": 1601928393.531,
    "LastProcessingResult": "No records processed",
    "State": "Updating",
    "StateTransitionReason": "USER_INITIATED"
}
```

Lambda aktualisiert diese Einstellungen asynchron. Die Ausgabe spiegelt keine Änderungen wider, bis dieser Vorgang abgeschlossen ist. Verwenden Sie den `get-event-source-mapping`-Befehl, um den aktuellen Status Ihrer Ressource anzuzeigen.

```
aws lambda get-event-source-mapping \
--uuid 91eaeb7e-c976-4939-9451-8709db01f137
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "UUID": "91eaeb7e-c976-4939-9451-8709db01f137",
    "BatchSize": 2,
    "EventSourceArn": "arn:aws:mq:us-east-1:123456789012:broker:ExampleMQBroker:b-
b4d492ef-bdc3-45e3-a781-cd1a3102ecca",
    "FunctionArn": "arn:aws:lambda:us-east-1:123456789012:function:MQ-Example-
Function",
    "LastModified": 1601928393.531,
    "LastProcessingResult": "No records processed",
    "State": "Enabled",
    "StateTransitionReason": "USER_INITIATED"
}
```

Fehler bei der Ereignisquellen-Zuweisung

Wenn eine Lambda-Funktion auf einen nicht behebbaren Fehler stößt, stoppt Ihr Amazon-MQ-Konsument die Verarbeitung von Datensätzen. Alle anderen Konsumenten können die Verarbeitung fortsetzen, sofern sie nicht auf denselben Fehler stoßen. Um die potenzielle Ursache für einen gestoppten Konsumenten zu ermitteln, überprüfen Sie das `StateTransitionReason`-Feld in den Rücksendedetails Ihres `EventSourceMapping` auf einen der folgenden Codes:

`ESM_CONFIG_NOT_VALID`

Die Konfiguration der Ereignisquellen-Zuweisung ist ungültig.

`EVENT_SOURCE_AUTHN_ERROR`

Lambda konnte die Ereignisquelle nicht authentifizieren.

`EVENT_SOURCE_AUTHZ_ERROR`

Lambda verfügt nicht über die erforderlichen Berechtigungen für den Zugriff auf die Ereignisquelle.

`FUNCTION_CONFIG_NOT_VALID`

Die Konfiguration der Funktion ist ungültig.

Datensätze bleiben auch unbearbeitet, wenn Lambda sie aufgrund ihrer Größe fallen lässt. Die Größenbeschränkung für Lambda-Datensätze beträgt 6 MB. Um Nachrichten bei Funktionsfehlern erneut zuzustellen, können Sie eine Warteschlange für unzustellbare Nachrichten (DLQ) verwenden. Weitere Informationen finden Sie unter Erneute Zustellung von Nachrichten und DLQ-Handhabung auf der Apache-ActiveMQ-Website und Zuverlässigkeits-Leitfaden auf der RabbitMQ-Website.

> **Note**
>
> Lambda unterstützt keine benutzerdefinierten Richtlinien für die erneute Bereitstellung. Stattdessen verwendet Lambda eine Richtlinie mit den Standardwerten von der Seite Redelivery Policy auf der Apache ActiveMQ-Website, die auf 6 gesetzt sind. `maximumRedeliveries`

Konfigurationsparameter für Amazon MQ und RabbitMQ

Alle Lambda-Ereignisquelltypen verwenden dieselben CreateEventSourceMappingUpdateEventSourceMappingAPI-Operationen. Allerdings gelten nur einige der Parameter für Amazon MQ und RabbitMQ.

Ereignisquellparameter, die für Amazon MQ und RabbitMQ gelten

Parameter	Erforderlich	Standard	Hinweise
BatchSize	N	100	Höchstwert: 10 000.
Enabled	N	true	
FunctionName	Y		
FilterCriteria	N		Lambda-Ereignisfilterung
MaximumBatchingWindowInSekunden	N	500 ms	Batching-Verhalten
Warteschlangen	N		Der Name der zu verwendenden Zielwarteschlange des Amazon-MQ-Brokers.
SourceAccessKonfigurationen	N		Für ActiveMQ BASIC_AUTH-Anmeldeinformationen. Für RabbitMQ können sowohl BASIC_AUTH Anmeldeinformationen als auch VIRTUAL_HOST Informationen enthalten sein.

Verwenden von Lambda mit Amazon MSK

> **Note**
>
> Wenn Sie Daten an ein anderes Ziel als eine Lambda-Funktion senden oder die Daten vor dem Senden anreichern möchten, finden Sie weitere Informationen unter Amazon EventBridge Pipes.

Amazon Managed Streaming for Apache Kafka (Amazon MSK) ist ein vollständig verwalteter Service, mit dem Sie Anwendungen erstellen und ausführen können, die Apache Kafka zum Verarbeiten von Streaming-Daten verwenden. Amazon MSK vereinfacht die Einrichtung, Skalierung und Verwaltung von Clustern, auf denen Kafka ausgeführt wird. Amazon MSK erleichtert auch die Konfiguration Ihrer Anwendung für mehrere Availability Zones und aus Sicherheitsgründen mit AWS Identity and Access Management (IAM). Amazon MSK unterstützt mehrere Open-Source-Versionen von Kafka.

Amazon MSK als Ereignisquelle funktioniert ähnlich wie die Verwendung von Amazon Simple Queue Service (Amazon SQS) oder Amazon Kinesis. Lambda fragt intern neue Nachrichten von der Ereignisquelle ab und ruft dann synchron die Ziel-Lambda-Funktion auf. Lambda liest die Nachrichten in Batches und stellt diese Ihrer Funktion als Ereignisnutzlast zur Verfügung. Die maximale Batchgröße ist konfigurierbar (Standardeinstellung: 100 Nachrichten). Weitere Informationen finden Sie unter Batching-Verhalten.

> **Note**
>
> Während Lambda-Funktionen in der Regel ein maximales Timeout-Limit von 15 Minuten haben, unterstützen Ereignisquellenzuordnungen für Amazon MSK, selbstverwaltetes Apache Kafka, Amazon DocumentDB, Amazon MQ für ActiveMQ und RabbitMQ nur Funktionen mit einem maximalen Timeout-Limit von 14 Minuten. Diese Einschränkung stellt sicher, dass die Ereignisquellenzuordnung Funktionsfehler und Wiederholungsversuche ordnungsgemäß verarbeiten kann.

Lambda liest die Nachrichten nacheinander für jede Partition. Eine einzelne Lambda-Nutzlast kann Nachrichten von mehreren Partitionen enthalten. Nachdem Lambda jeden Batch verarbeitet hat, werden die Offsets der Nachrichten in diesem Batch festgeschrieben. Wenn Ihre Funktion einen Fehler für eine der Nachrichten in einem Batch zurückgibt, wiederholt Lambda den gesamten Nachrichtenbatch, bis die Verarbeitung erfolgreich ist oder die Nachrichten ablaufen.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Ein Beispiel für die Konfiguration von Amazon MSK als Ereignisquelle finden Sie im AWS Compute-Blog unter Amazon MSK als Ereignisquelle verwenden für AWS Lambda. Ein vollständiges Tutorial finden Sie unter Amazon-MSK-Lambda-Integration in den Amazon-MSK-Übungen.

Themen

Tutorial: Verwenden einer Amazon MSK-Ereignisquellenzuordnung zum Aufrufen einer Lambda-Funktion

In diesem Tutorial werden Sie wie folgt vorgehen:

- Erstellen Sie eine Lambda-Funktion in demselben AWS Konto wie ein vorhandener Amazon MSK-Cluster.
- Konfigurieren Sie Netzwerk und Authentifizierung für Lambda für die Kommunikation mit Amazon MSK.
- Richten Sie eine Lambda Amazon MSK-Ereignisquellenzuordnung ein, die Ihre Lambda-Funktion ausführt, wenn Ereignisse im Thema auftauchen.

Wenn Sie mit diesen Schritten fertig sind und Ereignisse an Amazon MSK gesendet werden, können Sie eine Lambda-Funktion einrichten, um diese Ereignisse automatisch mit Ihrem eigenen benutzerdefinierten Lambda-Code zu verarbeiten.

Was können Sie mit dieser Funktion machen?

Beispiellösung: Verwenden Sie eine MSK-Ereignisquellenzuordnung, um Ihren Kunden Live-Ergebnisse zu liefern.

Stellen Sie sich das folgende Szenario vor: Ihr Unternehmen hostet eine Webanwendung, über die Ihre Kunden Informationen zu Live-Events wie Sportspielen abrufen können. Aktuelle Informationen aus dem Spiel werden Ihrem Team über ein Kafka-Thema auf Amazon MSK zur Verfügung gestellt. Sie möchten eine Lösung entwerfen, die Updates aus dem MSK-Thema nutzt, um Kunden innerhalb einer von Ihnen entwickelten Anwendung einen aktuellen Überblick über das Live-Event zu bieten. Sie haben sich für den folgenden Entwurfsansatz entschieden: Ihre Client-Anwendungen kommunizieren mit einem serverlosen Backend, auf dem gehostet wird. AWS Clients stellen mithilfe der Amazon WebSocket API Gateway eine Verbindung über Websocket-Sitzungen her.

In dieser Lösung benötigen Sie eine Komponente, die MSK-Ereignisse liest, eine benutzerdefinierte Logik ausführt, um diese Ereignisse für die Anwendungsschicht vorzubereiten, und diese Informationen dann an die API Gateway weiterleitet. Sie können diese Komponente implementieren AWS Lambda, indem Sie Ihre benutzerdefinierte Logik in einer Lambda-Funktion bereitstellen und sie dann mit einer AWS Lambda Amazon MSK-Ereignisquellenzuordnung aufrufen.

Weitere Informationen zur Implementierung von Lösungen mit der Amazon API Gateway WebSocket API finden Sie WebSocket in den API-Tutorials in der API Gateway-Dokumentation.

Voraussetzungen

Ein AWS Konto mit den folgenden vorkonfigurierten Ressourcen:

Um diese Voraussetzungen zu erfüllen, empfehlen wir den Abschnitt Erste Schritte mit Amazon MSK in der Amazon MSK-Dokumentation.

- Ein Amazon MSK-Cluster. Weitere Informationen finden Sie unter Erstellen eines Amazon MSK-Clusters unter Erste Schritte mit Amazon MSK.
- Die folgende Konfiguration:
  - Stellen Sie sicher, dass die rollenbasierte IAM-Authentifizierung in den Sicherheitseinstellungen Ihres Clusters aktiviert ist. Dies verbessert Ihre Sicherheit, indem Ihre Lambda-Funktion darauf beschränkt wird, nur auf die benötigten Amazon MSK-Ressourcen zuzugreifen. Dies ist standardmäßig auf neuen Amazon MSK-Clustern aktiviert.
  - Stellen Sie sicher, dass der öffentliche Zugriff in Ihren Cluster-Netzwerkeinstellungen deaktiviert ist. Die Beschränkung des Internetzugangs Ihres Amazon MSK-Clusters erhöht Ihre Sicherheit, da begrenzt wird, wie viele Vermittler mit Ihren Daten umgehen. Dies ist standardmäßig auf neuen Amazon MSK-Clustern aktiviert.
- Ein Kafka-Thema in Ihrem Amazon MSK-Cluster, das Sie für diese Lösung verwenden können. Weitere Informationen finden Sie unter Erstellen eines Themas unter Erste Schritte mit Amazon MSK.
- Ein Kafka-Admin-Host, der so eingerichtet ist, dass er Informationen aus Ihrem Kafka-Cluster abruft und Kafka-Ereignisse zu Testzwecken an Ihr Thema sendet, z. B. eine Amazon EC2 EC2-Instance, auf der die Kafka-Admin-CLI und die Amazon MSK IAM-Bibliothek installiert sind. Weitere Informationen finden Sie unter Erstellen eines Client-Computers unter Erste Schritte mit Amazon MSK.

Nachdem Sie diese Ressourcen eingerichtet haben, erfassen Sie die folgenden Informationen aus Ihrem AWS Konto, um zu bestätigen, dass Sie bereit sind, fortzufahren.

- Der Name Ihres Amazon MSK-Clusters. Sie finden diese Informationen in der Amazon MSK-Konsole.
- Die Cluster-UUID, Teil des ARN für Ihren Amazon MSK-Cluster, den Sie in der Amazon MSK-Konsole finden. Folgen Sie den Verfahren unter Cluster auflisten in der Amazon MSK-Dokumentation, um diese Informationen zu finden.
- Die mit Ihrem Amazon MSK-Cluster verknüpften Sicherheitsgruppen. Sie finden diese Informationen in der Amazon MSK-Konsole. Bezeichnen Sie diese in den folgenden Schritten als Ihren *`Cluster SecurityGroups`*.

- Die ID der Amazon VPC, die Ihren Amazon MSK-Cluster enthält. Sie finden diese Informationen, indem Sie die mit Ihrem Amazon MSK-Cluster verknüpften Subnetze in der Amazon MSK-Konsole identifizieren und anschließend die Amazon VPC, die dem Subnetz zugeordnet ist, in der Amazon VPC-Konsole identifizieren.
- Der Name des in Ihrer Lösung verwendeten Kafka-Themas. Sie finden diese Informationen, indem Sie Ihren Amazon MSK-Cluster mit der `topics` Kafka-CLI von Ihrem Kafka-Admin-Host aus aufrufen. Weitere Informationen zur Themen-CLI finden Sie in der Kafka-Dokumentation unter Themen hinzufügen und entfernen.
- Der Name einer Verbrauchergruppe für Ihr Kafka-Thema, die für Ihre Lambda-Funktion geeignet ist. Diese Gruppe kann automatisch von Lambda erstellt werden, sodass Sie sie nicht mit der Kafka-CLI erstellen müssen. Wenn Sie Ihre Verbrauchergruppen verwalten müssen, finden Sie weitere Informationen zur CLI für Verbrauchergruppen unter Verwalten von Verbrauchergruppen in der Kafka-Dokumentation.

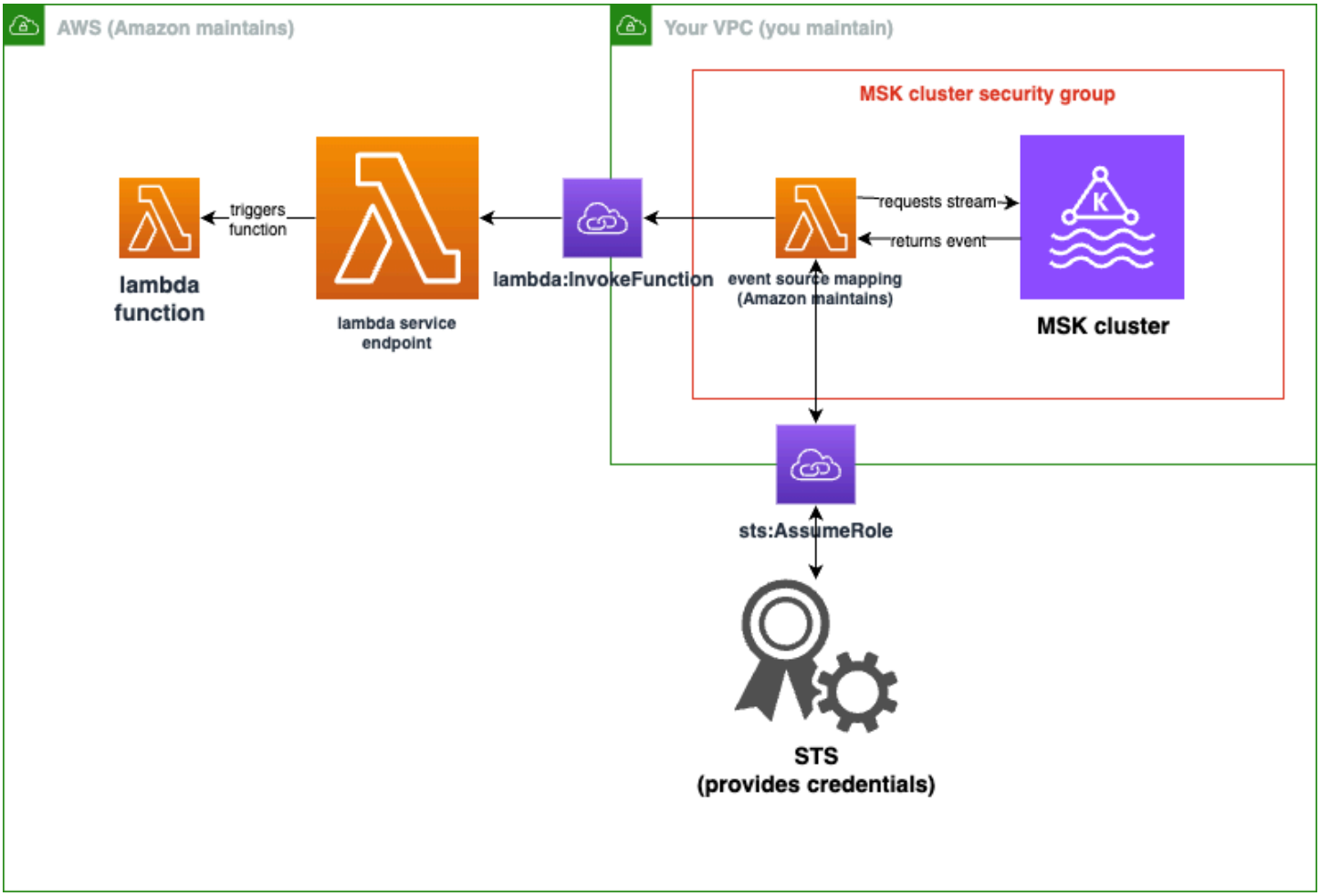
Die folgenden Berechtigungen in Ihrem Konto: AWS

- Erlaubnis, eine Lambda-Funktion zu erstellen und zu verwalten.
- Berechtigung zum Erstellen von IAM-Richtlinien und deren Verknüpfung mit Ihrer Lambda-Funktion.
- Erlaubnis, Amazon VPC-Endpoints zu erstellen und die Netzwerkkonfiguration in der Amazon VPC zu ändern, die Ihren Amazon MSK-Cluster hostet.

Netzwerkkonnektivität für Lambda für die Kommunikation mit Amazon MSK konfigurieren

Wird verwendet AWS PrivateLink , um Lambda und Amazon MSK zu verbinden. Sie können dies tun, indem Sie Amazon VPC-Schnittstellenendpunkte in der Amazon VPC-Konsole erstellen. Weitere Informationen zur Netzwerkkonfiguration finden Sie unter. the section called “Netzwerkkonfiguration”

Wenn eine Amazon MSK-Ereignisquellenzuordnung im Namen einer Lambda-Funktion ausgeführt wird, übernimmt sie die Ausführungsrolle der Lambda-Funktion. Diese IAM-Rolle autorisiert die Zuordnung für den Zugriff auf durch IAM gesicherte Ressourcen, wie z. B. Ihren Amazon MSK-Cluster. Obwohl sich die Komponenten eine gemeinsame Ausführungsrolle teilen, haben das Amazon MSK-Mapping und Ihre Lambda-Funktion unterschiedliche Konnektivitätsanforderungen für ihre jeweiligen Aufgaben, wie in der folgenden Abbildung dargestellt.



Ihre Ereignisquellenzuordnung gehört zu Ihrer Amazon MSK-Cluster-Sicherheitsgruppe. In diesem Netzwerkschritt erstellen Sie Amazon VPC-Endpoints aus Ihrer Amazon MSK-Cluster-VPC, um die Ereignisquellenzuordnung mit den Lambda- und STS-Services zu verbinden. Schützen Sie diese Endpunkte so, dass sie Datenverkehr von Ihrer Amazon MSK-Cluster-Sicherheitsgruppe akzeptieren. Passen Sie dann die Amazon MSK-Cluster-Sicherheitsgruppen so an, dass die Ereignisquellenzuordnung mit dem Amazon MSK-Cluster kommunizieren kann.

Sie können die folgenden Schritte mit dem konfigurieren. AWS Management Console

Um die Schnittstelle von Amazon VPC-Endpunkten für die Verbindung von Lambda und Amazon MSK zu konfigurieren

1. *Erstellen Sie eine Sicherheitsgruppe für Ihre Schnittstelle, Amazon VPC-Endpunkte, Endpunkt SecurityGroup, die eingehenden TCP-Verkehr auf 443 aus dem Cluster zulässt. SecurityGroups* Folgen Sie dem Verfahren unter Erstellen einer Sicherheitsgruppe in der Amazon EC2 EC2-Dokumentation, um eine

Sicherheitsgruppe zu erstellen. Folgen Sie dann dem Verfahren unter Regeln zu einer Sicherheitsgruppe hinzufügen in der Amazon EC2 EC2-Dokumentation, um die entsprechenden Regeln hinzuzufügen.

Erstellen Sie eine Sicherheitsgruppe mit den folgenden Informationen:

Wenn Sie Ihre Regeln für eingehenden Datenverkehr hinzufügen, erstellen Sie eine Regel für jede Sicherheitsgruppe im *`Cluster SecurityGroups`*. Für jede Regel:

- Wählen Sie als Typ die Option HTTPS aus.
- Wählen Sie als Quelle einen *`Cluster`* ausSecurityGroups.

2. Erstellen Sie einen Endpunkt, der den Lambda-Service mit der Amazon VPC verbindet, die Ihren Amazon MSK-Cluster enthält. Folgen Sie dem Verfahren unter Schnittstellenendpunkt erstellen.

   Erstellen Sie einen Schnittstellenendpunkt mit den folgenden Informationen:

   - Wählen Sie als Dienstname aus`com.amazonaws.`*`regionName`*`.lambda`, wo *`RegionName`* Ihre Lambda-Funktion hostet.
   - Wählen Sie für VPC die Amazon VPC aus, die Ihren Amazon MSK-Cluster enthält.
   - Wählen Sie für Sicherheitsgruppen den *`Endpunkt`* ausSecurityGroup, den Sie zuvor erstellt haben.
   - Wählen Sie für Subnetze die Subnetze aus, die Ihren Amazon MSK-Cluster hosten.
   - Geben Sie für Policy das folgende Richtliniendokument an, das den Endpunkt für die Verwendung durch den Lambda-Serviceprinzipal für die `lambda:InvokeFunction` Aktion sichert.

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
```

```
}
```

- Stellen Sie sicher, dass „DNS-Name aktivieren“ weiterhin aktiviert ist.

3. Erstellen Sie einen Endpunkt, der den AWS STS Service mit der Amazon VPC verbindet, die Ihren Amazon MSK-Cluster enthält. Folgen Sie dem Verfahren unter Schnittstellenendpunkt erstellen.

   Erstellen Sie einen Schnittstellenendpunkt mit den folgenden Informationen:

   - Wählen Sie als Dienstname die Option aus AWS STS.
   - Wählen Sie für VPC die Amazon VPC aus, die Ihren Amazon MSK-Cluster enthält.
   - *Wählen Sie für **Sicherheitsgruppen** den Endpunkt aus. SecurityGroup*
   - Wählen Sie für Subnetze die Subnetze aus, die Ihren Amazon MSK-Cluster hosten.
   - Geben Sie für Policy das folgende Richtliniendokument an, das den Endpunkt für die Verwendung durch den Lambda-Serviceprinzipal für die `sts:AssumeRole` Aktion sichert.

   ```
   {
       "Statement": [
           {
               "Action": "sts:AssumeRole",
               "Effect": "Allow",
               "Principal": {
                   "Service": [
                       "lambda.amazonaws.com"
                   ]
               },
               "Resource": "*"
           }
       ]
   }
   ```

   - Stellen Sie sicher, dass „DNS-Name aktivieren“ weiterhin aktiviert ist.

4. Lassen Sie für jede Sicherheitsgruppe, die Ihrem Amazon MSK-Cluster zugeordnet ist, d. h. im *Cluster SecurityGroups*, Folgendes zu:

   - Erlauben Sie den gesamten eingehenden und ausgehenden TCP-Verkehr auf 9098 für den gesamten *ClusterSecurityGroups, auch innerhalb des Clusters selbst*.
   - Lässt den gesamten ausgehenden TCP-Verkehr auf 443 zu.

Ein Teil dieses Datenverkehrs ist gemäß den Standardregeln für Sicherheitsgruppen zulässig. Wenn Ihr Cluster also an eine einzelne Sicherheitsgruppe angehängt ist und für diese Gruppe Standardregeln gelten, sind keine zusätzlichen Regeln erforderlich. Um Sicherheitsgruppenregeln anzupassen, folgen Sie den Verfahren unter Regeln zu einer Sicherheitsgruppe hinzufügen in der Amazon EC2 EC2-Dokumentation.

Fügen Sie Ihren Sicherheitsgruppen Regeln mit den folgenden Informationen hinzu:

- Geben Sie für jede eingehende Regel oder ausgehende Regel für Port 9098 Folgendes an
  - Wählen Sie für Type (Typ) Custom TCP (Benutzerdefiniertes TCP).
  - Geben Sie als Portbereich 9098 an.
  - Geben Sie als Quelle einen von *cluster SecurityGroups* an.
- Wählen Sie für jede eingehende Regel für Port 443 für Typ die Option HTTPS aus.

Erstellen Sie eine IAM-Rolle, damit Lambda aus Ihrem Amazon MSK-Thema lesen kann

Identifizieren Sie die Authentifizierungsanforderungen, die Lambda aus Ihrem Amazon MSK-Thema lesen muss, und definieren Sie sie dann in einer Richtlinie. Erstellen Sie eine Rolle, *Lambda AuthRole*, die Lambda autorisiert, diese Berechtigungen zu verwenden. Autorisieren Sie Aktionen in Ihrem Amazon MSK-Cluster mithilfe von `kafka-cluster` IAM-Aktionen. Autorisieren Sie Lambda anschließend, Amazon MSK `kafka` - und Amazon EC2 EC2-Aktionen durchzuführen, die für die Erkennung Ihres Amazon MSK-Clusters und die Verbindung zu ihm erforderlich sind, sowie CloudWatch Aktionen, damit Lambda protokollieren kann, was es getan hat.

Um die Authentifizierungsanforderungen für Lambda zum Lesen aus Amazon MSK zu beschreiben

1. Schreiben Sie ein IAM-Richtliniendokument (ein JSON-Dokument), *Cluster*, das es Lambda ermöglichtAuthPolicy, mithilfe Ihrer Kafka-Verbrauchergruppe aus Ihrem Kafka-Thema in Ihrem Amazon MSK-Cluster zu lesen. Lambda erfordert, dass beim Lesen eine Kafka-Verbrauchergruppe festgelegt wird.

   Passen Sie die folgende Vorlage an Ihre Voraussetzungen an:

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

```
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:DescribeGroup",
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeTopic",
                "kafka-cluster:ReadData",
                "kafka-cluster:DescribeClusterDynamicConfiguration"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:cluster/mskClusterName/cluster-
uuid",
                "arn:aws:kafka:region:account-id:topic/mskClusterName/cluster-
uuid/mskTopicName",
                "arn:aws:kafka:region:account-id:group/mskClusterName/cluster-
uuid/mskGroupName"
            ]
        }
    ]
}
```

Weitere Informationen finden Sie unterthe section called “Auf IAM-Rolle basierende Authentifizierung”. Beim Verfassen Ihrer Police:

- Geben Sie für *Region* und *Konto-ID* diejenigen an, die Ihren Amazon MSK-Cluster hosten.
- Geben Sie für *msk ClusterName* den Namen Ihres Amazon MSK-Clusters ein.
- Geben Sie für *cluster-uuid die UUID* im ARN für Ihren Amazon MSK-Cluster an.
- Geben Sie für *msk* den Namen Ihres Kafka-Themas TopicName an.
- Geben Sie für *msk GroupName* den Namen Ihrer Kafka-Verbrauchergruppe an.

2. Identifizieren Sie Amazon MSK, Amazon EC2 und die CloudWatch Berechtigungen, die Lambda benötigt, um Ihren Amazon MSK-Cluster zu erkennen und zu verbinden, und protokollieren Sie diese Ereignisse.

   Die `AWSLambdaMSKExecutionRole` verwaltete Richtlinie definiert die erforderlichen Berechtigungen auf unzulässige Weise. Verwenden Sie es in den folgenden Schritten.

   Überlegen Sie in einer Produktionsumgebung, ob `AWSLambdaMSKExecutionRole` Sie Ihre Ausführungsrollenrichtlinie auf der Grundlage des Prinzips der geringsten Rechte einschränken möchten, und schreiben Sie dann eine Richtlinie für Ihre Rolle, die diese verwaltete Richtlinie ersetzt.

Einzelheiten zur Sprache der IAM-Richtlinien finden Sie in der IAM-Dokumentation.

Nachdem Sie Ihr Richtliniendokument verfasst haben, erstellen Sie eine IAM-Richtlinie, damit Sie sie Ihrer Rolle zuordnen können. Sie können dies mithilfe der Konsole mit dem folgenden Verfahren tun.

Um eine IAM-Richtlinie anhand Ihres Richtliniendokuments zu erstellen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich auf der linken Seite Policies (Richtlinien).
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie im Bereich Policy editor (Richtlinien-Editor) die Option JSON aus.
5. *Cluster AuthPolicy* einfügen.
6. Wenn Sie mit dem Hinzufügen von Berechtigungen zur Richtlinie fertig sind, wählen Sie Next (Weiter) aus.
7. Geben Sie auf der Seite Review and create (Überprüfen und erstellen) unter Name einen Namen und unter Description (Beschreibung) (optional) eine Beschreibung für die Richtlinie ein, die Sie erstellen. Überprüfen Sie Permissions defined in this policy (In dieser Richtlinie definierte Berechtigungen), um die Berechtigungen einzusehen, die von Ihrer Richtlinie gewährt werden.
8. Wählen Sie Create policy (Richtlinie erstellen) aus, um Ihre neue Richtlinie zu speichern.

Weitere Informationen finden Sie in der IAM-Dokumentation unter IAM-Richtlinien erstellen.

Nachdem Sie nun über die entsprechenden IAM-Richtlinien verfügen, erstellen Sie eine Rolle und fügen Sie sie ihr hinzu. Sie können dies mithilfe der Konsole mit dem folgenden Verfahren tun.

So erstellen Sie eine Ausführungsrolle in der IAM-Konsole

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Typ der vertrauenswürdigen Entität die Option AWS -Service aus.
4. Wählen Sie unter Anwendungsfall Lambda aus.
5. Wählen Sie Weiter aus.
6. Wählen Sie die folgenden Richtlinien:
   - *Cluster AuthPolicy*

- `AWSLambdaMSKExecutionRole`

7. Wählen Sie Weiter aus.
8. Geben Sie als Rollenname *`Lambda`* ein AuthRole und wählen Sie dann Create role aus.

Weitere Informationen finden Sie unter the section called “Ausführungsrolle (Berechtigungen für Funktionen zum Zugriff auf andere Ressourcen)”.

Erstellen Sie eine Lambda-Funktion zum Lesen aus Ihrem Amazon MSK-Thema

Erstellen Sie eine Lambda-Funktion, die für die Verwendung Ihrer IAM-Rolle konfiguriert ist. Sie können Ihre Lambda-Funktion mit der Konsole erstellen.

So erstellen Sie eine Lambda-Funktion mit Ihrer Authentifizierungskonfiguration

1. Öffnen Sie die Lambda-Konsole und wählen Sie in der Kopfzeile Funktion erstellen aus.
2. Wählen Sie Verfassen von Grund auf aus.
3. Geben Sie als Funktionsname einen geeigneten Namen Ihrer Wahl ein.
4. Wählen Sie für Runtime die neueste unterstützte Version von`Node.js`, um den in diesem Tutorial bereitgestellten Code zu verwenden.
5. Wählen Sie Standardausführungsrolle ändern aus.
6. Wählen Sie Bestehende Rolle verwenden aus.
7. Wählen Sie für Existierende Rolle die Option *`Lambda AuthRole`* aus.

In einer Produktionsumgebung müssen Sie der Ausführungsrolle für Ihre Lambda-Funktion normalerweise weitere Richtlinien hinzufügen, um Ihre Amazon MSK-Ereignisse sinnvoll verarbeiten zu können. Weitere Informationen zum Hinzufügen von Richtlinien zu Ihrer Rolle finden Sie in der IAM-Dokumentation unter Hinzufügen oder Entfernen von Identitätsberechtigungen.

Erstellen Sie eine Ereignisquellenzuordnung zu Ihrer Lambda-Funktion

Ihre Amazon MSK-Ereignisquellenzuordnung stellt dem Lambda-Service die Informationen bereit, die erforderlich sind, um Ihr Lambda aufzurufen, wenn entsprechende Amazon MSK-Ereignisse eintreten. Sie können mit der Konsole eine Amazon MSK-Zuordnung erstellen. Erstellen Sie einen Lambda-Trigger, dann wird die Zuordnung der Ereignisquelle automatisch eingerichtet.

So erstellen Sie einen Lambda-Trigger (und eine Ereignisquellenzuordnung)

1. Navigieren Sie zur Übersichtsseite Ihrer Lambda-Funktion.
2. Wählen Sie im Bereich Funktionsübersicht unten links die Option Auslöser hinzufügen aus.
3. Wählen Sie in der Dropdownliste Quelle auswählen die Option Amazon MSK aus.
4. Legen Sie keine Authentifizierung fest.
5. Wählen Sie für MSK-Cluster den Namen Ihres Clusters aus.
6. Geben Sie für Batchgröße den Wert 1 ein. Dieser Schritt erleichtert das Testen dieser Funktion und ist kein idealer Wert für die Produktion.
7. Geben Sie als Themenname den Namen Ihres Kafka-Themas ein.
8. Geben Sie als Verbrauchergruppen-ID die ID Ihrer Kafka-Verbrauchergruppe an.

Aktualisieren Sie Ihre Lambda-Funktion, um Ihre Streaming-Daten zu lesen

Lambda stellt Informationen über Kafka-Ereignisse über den Parameter event method bereit. Ein Beispiel für die Struktur eines Amazon MSK-Ereignisses finden Sie unterthe section called “ Beispielereignis”. Nachdem Sie verstanden haben, wie Lambda-weitergeleitete Amazon MSK-Ereignisse interpretiert werden, können Sie Ihren Lambda-Funktionscode ändern, um die darin enthaltenen Informationen zu verwenden.

Geben Sie den folgenden Code für Ihre Lambda-Funktion ein, um den Inhalt eines Lambda Amazon MSK-Ereignisses zu Testzwecken zu protokollieren:

Node.js

```
exports.handler = async (event) => {
    // Iterate through keys
    for (let key in event.records) {
      console.log('Key: ', key)
      // Iterate through records
      event.records[key].map((record) => {
        console.log('Record: ', record)
        // Decode base64
        const msg = Buffer.from(record.value, 'base64').toString()
        console.log('Message:', msg)
      })
    }
}
```

Sie können Ihrem Lambda über die Konsole Funktionscode zur Verfügung stellen.

Um Ihren Lambda-Funktionscode zu aktualisieren

1. Navigieren Sie zur Übersichtsseite Ihrer Lambda-Funktion.
2. Wählen Sie die Registerkarte Code.
3. Geben Sie den bereitgestellten Code in die Codequell-IDE ein.
4. Wählen Sie in der Navigationsleiste für die Codequelle die Option Bereitstellen aus.

Testen Sie Ihre Lambda-Funktion, um sicherzustellen, dass sie mit Ihrem Amazon MSK-Thema verbunden ist

Sie können jetzt überprüfen, ob Ihr Lambda von der Ereignisquelle aufgerufen wird, indem Sie die Ereignisprotokolle überprüfen CloudWatch .

Um zu überprüfen, ob Ihre Lambda-Funktion aufgerufen wird

1. Verwenden Sie Ihren Kafka-Admin-Host, um Kafka-Ereignisse mithilfe der `kafka-console-producer` CLI zu generieren. Weitere Informationen finden Sie in der Kafka-Dokumentation unter Einige Ereignisse in das Thema schreiben. Senden Sie genügend Ereignisse, um den Stapel zu füllen, der durch die Batchgröße für Ihre im vorherigen Schritt definierte Ereignisquellenzuordnung definiert wurde, oder Lambda wartet, bis weitere Informationen aufgerufen werden.
2. Wenn Ihre Funktion ausgeführt wird, schreibt Lambda, was passiert ist. CloudWatch Navigieren Sie in der Konsole zur Detailseite Ihrer Lambda-Funktion.
3. Wählen Sie die Registerkarte Configuration aus.
4. Wählen Sie in der Seitenleiste Überwachungs- und Betriebstools aus.
5. Identifizieren Sie die CloudWatch Protokollgruppe unter Protokollierungskonfiguration. Die Protokollgruppe sollte mit beginnen`/aws/lambda`. Wählen Sie den Link zur Protokollgruppe.
6. Suchen Sie in der CloudWatch Konsole in den Protokollereignissen nach den Protokollereignissen, die Lambda an den Protokollstream gesendet hat. Stellen Sie fest, ob es Protokollereignisse gibt, die die Nachricht von Ihrem Kafka-Ereignis enthalten, wie in der folgenden Abbildung dargestellt. Falls ja, haben Sie erfolgreich eine Lambda-Funktion mit einer Lambda-Ereignisquellenzuordnung mit Amazon MSK verbunden.

```
2020-08-06T15:06:18.861-04:00	START RequestId: 88ebae59-be0c-4e22-9db7-4154b437e43a Version: $LATEST
2020-08-06T15:06:18.866-04:00	2020-08-06T19:06:18.866Z 88ebae59-be0c-4e22-9db7-4154b437e43a INFO Key: mytopic-0
2020-08-06T15:06:18.866-04:00	2020-08-06T19:06:18.866Z	88ebae59-be0c-4e22-9db7-4154b437e43a	INFO	Record: {
  topic: 'mytopic',
  partition: 0,
  offset: 38,
  timestamp: 1596740777633,
  timestampType: 'CREATE_TIME',
  value: 'TWVzc2FnZSAjMQ=='
}
2020-08-06T15:06:18.866-04:00	2020-08-06T19:06:18.866Z 88ebae59-be0c-4e22-9db7-4154b437e43a INFO Message: Message #1
2020-08-06T15:06:18.890-04:00	END RequestId: 88ebae59-be0c-4e22-9db7-4154b437e43a
```

Beispielereignis

Lambda sendet den Batch von Nachrichten im Ereignisparameter, wenn es Ihre Funktion aufruft. Die Ereignisnutzlast enthält ein Array von Meldungen. Jedes Array-Element enthält Details zum Amazon-MSK-Thema und zur Partitions-ID sowie einen Zeitstempel und eine base64-codierte Nachricht.

```
{
   "eventSource":"aws:kafka",
   "eventSourceArn":"arn:aws:kafka:sa-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
   "bootstrapServers":"b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
   "records":{
      "mytopic-0":[
         {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "key":"abcDEFghiJKLmnoPQRstuVWXyz1234==",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[
               {
                  "headerKey":[
                     104,
                     101,
                     97,
                     100,
                     101,
                     114,
                     86,
```

```
                    97,
                    108,
                    117,
                    101
                ]
            }
        ]
    }
  ]
 }
}
```

MSK-Cluster-Authentifizierung

Lambda benötigt eine Berechtigung, um auf den Amazon-MSK-Cluster zuzugreifen, Datensätze abzurufen und andere Aufgaben auszuführen. Amazon MSK unterstützt mehrere Optionen zur Steuerung des Client-Zugriffs auf den MSK-Cluster.

Cluster-Zugriffsoptionen

- Nicht authentifizierter Zugriff
- SASL/SCRAM-Authentifizierung
- Auf IAM-Rolle basierende Authentifizierung
- Gegenseitige TLS-Authentifizierung
- Konfigurieren des mTLS-Secrets
- So wählt Lambda einen Bootstrap-Broker

Nicht authentifizierter Zugriff

Wenn keine Clients über das Internet auf den Cluster zugreifen, können Sie einen nicht authentifizierten Zugriff verwenden.

SASL/SCRAM-Authentifizierung

Amazon MSK unterstützt die Authentifizierung mit Transport Layer Security (TLS)-Verschlüsselung von Simple Authentication and Security Layer/Salted Challenge Response Authentication Mechanism (SASL/SCRAM). Damit Lambda eine Verbindung zum Cluster herstellen kann, speichern Sie die Authentifizierungsdaten (Benutzername und Passwort) AWS Secrets Manager geheim.

Weitere Informationen zur Verwendung von Secrets Manager finden Sie unter Benutzername und Passwortauthentifizierung mit AWS Secrets Manager im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.

Amazon MSK unterstützt die SASL/PLAIN-Authentifizierung nicht.

Auf IAM-Rolle basierende Authentifizierung

Sie können IAM verwenden, um die Identität von Clients zu authentifizieren, die sich mit dem MSK-Cluster verbinden. Wenn die IAM-Authentifizierung auf Ihrem MSK-Cluster aktiv ist und Sie kein Geheimnis für die Authentifizierung angeben, verwendet Lambda automatisch standardmäßig die IAM-Authentifizierung. Verwenden Sie die IAM-Konsole oder API, um Richtlinien zu erstellen und zu implementieren, die auf Benutzern oder Rollen basieren. Weitere Informationen finden Sie unter IAM-Zugriffskontrolle im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.

Fügen Sie die folgenden Berechtigungen zur Ausführungsrolle Ihrer Funktion hinzu, um Lambda zu erlauben, sich mit dem MSK-Cluster zu verbinden, Datensätze zu lesen und andere erforderliche Aktionen auszuführen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:DescribeGroup",
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeTopic",
                "kafka-cluster:ReadData",
                "kafka-cluster:DescribeClusterDynamicConfiguration"
            ],
            "Resource": [
                "arn:aws:kafka:region:account-id:cluster/cluster-name/cluster-uuid",
                "arn:aws:kafka:region:account-id:topic/cluster-name/cluster-uuid/topic-
name",
                "arn:aws:kafka:region:account-id:group/cluster-name/cluster-
uuid/consumer-group-id"
            ]
        }
    ]
}
```

Sie können diese Berechtigungen für einen bestimmten Cluster, ein bestimmtes Thema und eine bestimmte Gruppe einteilen. Weitere Informationen finden Sie unter Amazon-MSK-Kafka-Aktionen im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.

Gegenseitige TLS-Authentifizierung

Gegenseitige TLS (mTLS) bietet eine bidirektionale Authentifizierung zwischen Client und Server. Der Client sendet ein Zertifikat an den Server, damit der Server den Client überprüfen kann, und der Server sendet ein Zertifikat an den Client, damit der Client den Server überprüfen kann.

Für Amazon MSK fungiert Lambda als der Client. Sie konfigurieren ein Client-Zertifikat (als Secret in Secrets Manager), um Lambda für die Broker in Ihrem MSK-Cluster zu authentifizieren. Das Client-Zertifikat muss von einer Zertifizierungsstelle im Trust Store des Servers signiert sein. Der MSK-Cluster sendet ein Serverzertifikat an Lambda, um die Broker für Lambda zu authentifizieren. Das Serverzertifikat muss von einer Zertifizierungsstelle (CA) signiert sein, die sich im AWS Trust Store befindet.

Informationen dazu, wie Sie ein Client-Zertifikat generieren, finden Sie unter Vorstellung von gegenseitiger TLS-Authentifizierung für Amazon MSK als Ereignisquelle.

Amazon MSK unterstützt keine selbstsignierten Serverzertifikate, da alle Broker in Amazon MSK öffentliche Zertifikate verwenden, die von Amazon-TrustServices-Zertifizierungsstellen signiert sind, denen Lambda standardmäßig vertraut.

Weitere Informationen über mTLS für Amazon MSK finden Sie unter Gegenseitige TLS-Authentifizierung im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.

Konfigurieren des mTLS-Secrets

Das Secret CLIENT_CERTIFICATE_TLS_AUTH erfordert ein Zertifikatfeld und ein Feld für einen privaten Schlüssel. Für einen verschlüsselten privaten Schlüssel erfordert das Secret ein Passwort für den privaten Schlüssel. Sowohl das Zertifikat als auch der private Schlüssel müssen im PEM-Format vorliegen.

> **Note**
>
> Lambda unterstützt die PBES1-Algorithmen (aber nicht PBES2) zur Verschlüsselung von privaten Schlüsseln.

Das Zertifikatfeld muss eine Liste von Zertifikaten enthalten, beginnend mit dem Client-Zertifikat, gefolgt von etwaigen Zwischenzertifikaten und endend mit dem Root-Zertifikat. Jedes Zertifikat muss in einer neuen Zeile mit der folgenden Struktur beginnen:

```
-----BEGIN CERTIFICATE-----
        <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager unterstützt Secrets von bis zu 65 536 Bytes, was genügend Platz für lange Zertifikatsketten bietet.

Der private Schlüssel muss im Format PKCS #8 mit folgender Struktur vorliegen:

```
-----BEGIN PRIVATE KEY-----
         <private key contents>
-----END PRIVATE KEY-----
```

Verwenden Sie für einen verschlüsselten privaten Schlüssel die folgende Struktur:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
          <private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

Im folgenden Beispiel sehen Sie den Inhalt eines Secrets für mTLS-Authentifizierung mit einem verschlüsselten privaten Schlüssel. Fügen Sie für einen verschlüsselten privaten Schlüssel das Passwort für den privaten Schlüssel in das Secret ein.

```
{
 "privateKeyPassword": "testpassword",
 "certificate": "-----BEGIN CERTIFICATE-----
MIIE5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPimO40s1cRqtFHXoal0QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFgjCCA2qgAwIBAgIQdjNZd6uFf9hbNC5RdfmHrzANBgkqhkiG9w0BAQsFADBb
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
```

```
-----END CERTIFICATE-----",
 "privateKey": "-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzgO9IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}
```

So wählt Lambda einen Bootstrap-Broker

Lambda wählt einen Bootstrap-Broker basierend auf den auf Ihrem Cluster verfügbaren Authentifizierungsmethoden aus und ob Sie ein Geheimnis für die Authentifizierung angeben.. Wenn Sie ein Geheimnis für MTLs oder SASL/SCRAM angeben, wählt Lambda automatisch diese Authentifizierungsmethode. Wenn Sie kein Geheimnis angeben, wählt Lambda die stärkste Authentifizierungsmethode aus, die in Ihrem Cluster aktiv ist. Im Folgenden ist die Reihenfolge der Priorität aufgeführt, in der Lambda einen Broker auswählt, von der stärksten zur schwächsten Authentifizierung:

- mTLS (Geheimnis für mTLS bereitgestellt)
- SASL/SCRAM (Geheimnis für SASL/SCRAM bereitgestellt)
- SASL IAM (kein Geheimnis angegeben und IAM-Authentifizierung aktiv)
- Nicht authentifiziertes TLS (kein Geheimnis bereitgestellt und IAM-Authentifizierung nicht aktiv)
- Klartext (kein Geheimnis angegeben und sowohl IAM-Authentifizierung als auch nicht authentifiziertes TLS sind nicht aktiv)

> **Note**
>
> Wenn Lambda keine Verbindung zum sichersten Brokertyp herstellen kann, versucht Lambda nicht, eine Verbindung zu einem anderen (schwächeren) Brokertyp herzustellen. Wenn Sie möchten, dass Lambda einen schwächeren Brokertyp wählt, deaktivieren Sie alle stärkeren Authentifizierungsmethoden in Ihrem Cluster.

Verwalten von API-Zugriff und -Berechtigungen

Neben dem Zugriff auf den Amazon-MSK-Cluster benötigt Ihre Funktion auch Berechtigungen, um verschiedene Amazon-MSK-API-Aktionen auszuführen. Sie fügen diese Berechtigungen zur

Ausführungsrolle der Funktion hinzu. Wenn Ihre Benutzer Zugriff auf Amazon-MSK-API-Aktionen benötigen, fügen Sie die erforderlichen Berechtigungen zur Identitätsrichtlinie für den Benutzer oder die Rolle hinzu.

Sie können Ihrer Ausführungsrolle jede der folgenden Berechtigungen manuell hinzufügen. Alternativ können Sie die AWS verwaltete Richtlinie AWSLambdaMSKExecutionRolean Ihre Ausführungsrolle anhängen. Die `AWSLambdaMSKExecutionRole`-Richtlinie enthält alle unten aufgeführten erforderlichen API-Aktionen und VPC-Berechtigungen.

Erforderliche Berechtigungen für Ausführungsrolle der Lambda-Funktion

Um Protokolle in einer Protokollgruppe in Amazon CloudWatch Logs zu erstellen und zu speichern, muss Ihre Lambda-Funktion in ihrer Ausführungsrolle über die folgenden Berechtigungen verfügen:

- Logs: Gruppe CreateLog
- Protokolle: CreateLog Stream
- Protokolle: PutLog Ereignisse

Damit Lambda in Ihrem Namen auf Ihren Amazon-MSK-Cluster zugreifen kann, muss Ihre Lambda-Funktion über die folgenden Berechtigungen in ihrer Ausführungsrolle verfügen:

- kafka: DescribeCluster
- Kafka: V2 DescribeCluster
- kafka: Makler GetBootstrap
- kafka: DescribeVpc Verbindung: Nur für kontoübergreifende Zuordnungen von Ereignisquellen erforderlich.
- kafka: ListVpc Verbindungen: In der Ausführungsrolle nicht erforderlich, aber für einen IAM-Prinzipal erforderlich, der eine kontenübergreifende Zuordnung von Ereignisquellen erstellt.

Sie müssen nur entweder `kafka:DescribeCluster` oder `kafka:DescribeClusterV2` hinzufügen. Für bereitgestellte MSK-Cluster funktioniert jede der beiden Berechtigungen. Für Serverless-MSK-Cluster müssen Sie `kafka:DescribeClusterV2` verwenden.

> **Note**
>
> Lambda plant, schließlich die `kafka:DescribeCluster`-Genehmigung aus dieser `AWSLambdaMSKExecutionRole`-Richtlinie zu entfernen. Wenn Sie diese Richtlinie

verwenden, sollten Sie alle Anwendungen, die `kafka:DescribeCluster` verwendet, auf `kafka:DescribeClusterV2` umstellen.

VPC-Berechtigungen

Wenn nur Benutzer innerhalb einer VPC auf Ihren Amazon-MSK-Cluster zugreifen können, muss Ihre Lambda-Funktion die Berechtigung zum Zugriff auf Ihre Amazon-VPC-Ressourcen haben. Zu diesen Ressourcen gehören Ihre VPC, Subnetze, Sicherheitsgruppen und Netzwerkschnittstellen. Um auf diese Ressourcen zugreifen zu können, muss die Ausführungsrolle Ihrer Funktion über die folgenden Berechtigungen verfügen. Diese Berechtigungen sind in der AWSLambdaMSKExecutionRole AWS verwalteten Richtlinie enthalten.

- ec2: Schnittstelle CreateNetwork
- ec2: Schnittstellen DescribeNetwork
- ec2: DescribeVpcs
- ec2: Schnittstelle DeleteNetwork
- ec2: DescribeSubnets
- ec2: Gruppen DescribeSecurity

Optionale Lambda-Funktionsberechtigungen

Ihre Lambda-Funktion benötigt möglicherweise auch Berechtigungen für Folgendes:

- Greifen Sie auf Ihr SCRAM-Secret zu, wenn Sie die SASL/SCRAM-Authentifizierung verwenden.
- Beschreiben Ihres Secrets-Manager-Secrets
- Greifen Sie auf Ihren AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel zu.
- Senden von Datensätzen zu fehlgeschlagenen Aufrufen an ein Ziel

Secrets Manager und AWS KMS Berechtigungen

Abhängig von der Art der Zugriffskontrolle, die Sie für Ihre Amazon MSK-Broker konfigurieren, benötigt Ihre Lambda-Funktion möglicherweise die Erlaubnis, auf Ihr SCRAM-Geheimnis (wenn Sie SASL/SCRAM-Authentifizierung verwenden) oder auf Secrets Manager-Geheimnis zuzugreifen, um

Ihren vom Kunden verwalteten Schlüssel zu entschlüsseln. AWS KMS Um auf diese Ressourcen zuzugreifen, muss die Ausführungsrolle Ihrer Funktion die folgenden Berechtigungen besitzen:

- kafka: Geheimnisse ListScram
- secretsmanager: Wert GetSecret
- kms:Decrypt

Hinzufügen von Berechtigungen zu Ihrer Ausführungsrolle

Gehen Sie wie folgt vor, um die AWS verwaltete Richtlinie mithilfe der IAM-Konsole AWSLambdaMSKExecutionRolezu Ihrer Ausführungsrolle hinzuzufügen.

Um eine AWS verwaltete Richtlinie hinzuzufügen

1. Öffnen Sie die Seite Richtlinien in der IAM-Konsole.
2. Geben Sie im Suchfeld den Namen der Richtlinie ein (`AWSLambdaMSKExecutionRole`).
3. Wählen Sie die Richtlinie aus der Liste aus und wählen Sie dann Richtlinienaktionen, Anhängen aus.
4. Wählen Sie auf der Seite Richtlinie anfügen Ihre Ausführungsrolle aus der Liste aus, und wählen Sie dann Richtlinie anfügen aus.

Gewähren von Benutzerzugriff mit einer IAM-Richtlinie

Standardmäßig haben Benutzer und Rollen keine Berechtigung zum Ausführen von Amazon-MSK-API-Operationen. Um Benutzern in Ihrem Unternehmen oder Konto Zugriff zu gewähren, können Sie eine identitätsbasierte Richtlinie hinzufügen oder aktualisieren. Weitere Informationen finden Sie unter Beispiele für identitätsbasierte Amazon-MSK-Richtlinien im Entwicklerhanbuch für Amazon Managed Streaming for Apache Kafka.

Authentifizierungs- und Autorisierungsfehler

Wenn eine der für die Nutzung von Daten aus dem Amazon MSK-Cluster erforderlichen Berechtigungen fehlt, zeigt Lambda in der Ereignisquellenzuordnung unter LastProcessing Ergebnis eine der folgenden Fehlermeldungen an.

Fehlermeldungen

- Cluster konnte Lambda nicht autorisieren

- SASL-Authentifizierung fehlgeschlagen
- Server konnte Lambda nicht authentifizieren
- Bereitgestelltes Zertifikat oder bereitgestellter privater Schlüssel ist ungültig

Cluster konnte Lambda nicht autorisieren

Bei SASL/SCRAM oder mTLS weist dieser Fehler darauf hin, dass der angegebene Benutzer nicht über alle nachfolgenden erforderlichen Berechtigungen für die Kafka-Zugriffskontrollliste (ACL) verfügt:

- DescribeConfigs Cluster
- Beschreiben von Gruppe
- Gruppe lesen
- Thema beschreiben
- Thema lesen

Zur IAM-Zugriffskontrolle fehlen der Ausführungsrolle Ihrer Funktion eine oder mehrere der Berechtigungen, die für den Zugriff auf die Gruppe oder das Thema erforderlich sind. Prüfen Sie die Liste der erforderlichen Berechtigungen in the section called “Auf IAM-Rolle basierende Authentifizierung”.

Wenn Sie Kafka-ACLs oder eine IAM-Richtlinie mit den erforderlichen Kafka-Cluster-Berechtigungen erstellen, geben Sie das Thema und die Gruppe als Ressourcen an. Der Themenname muss mit dem Thema in der Ereignisquellenzuordnung übereinstimmen. Der Gruppenname muss mit der UUID der Ereignisquellenzuordnung übereinstimmen.

Nachdem Sie der Ausführungsrolle die erforderlichen Berechtigungen hinzugefügt haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden.

SASL-Authentifizierung fehlgeschlagen

Bei SASL/SCRAM weist dieser Fehler darauf hin, dass der angegebene Benutzername und das Passwort ungültig sind.

Zur IAM-Zugriffskontrolle fehlt der Ausführungsrolle die Berechtigung `kafka-cluster:Connect` für den MSK-Cluster. Fügen Sie der Rolle diese Berechtigung hinzu und geben Sie den Amazon-Ressourcenname (ARN) des Clusters als Ressource an.

Dieser Fehler wird Ihnen möglicherweise in zeitlichen Abständen angezeigt. Der Cluster lehnt Verbindungen ab, wenn die Anzahl der TCP-Verbindungen das Amazon-MSK-Servicekontingent überschreitet. Lambda zieht sich zurück und versucht es erneut, bis eine Verbindung erfolgreich ist. Nachdem Lambda eine Verbindung zum Cluster hergestellt hat und nach Datensätzen abfragt, ändert sich das letzte Verarbeitungsergebnis zu 0K.

Server konnte Lambda nicht authentifizieren

Dieser Fehler weist darauf hin, dass die Amazon-MSK-Kafka-Broker sich bei Lambda nicht authentifizieren konnten. Dieser Fehler kann aus folgenden Gründen auftreten:

- Sie haben kein Client-Zertifikat für die mTLS-Authentifizierung bereitgestellt.
- Sie haben ein Client-Zertifikat bereitgestellt, aber die Broker sind nicht für die Verwendung von mTLS konfiguriert.
- Die Broker vertrauen einem Client-Zertifikat nicht.

Bereitgestelltes Zertifikat oder bereitgestellter privater Schlüssel ist ungültig

Dieser Fehler weist darauf hin, dass der Amazon-MSK-Konsument das bereitgestellte Zertifikat oder den bereitgestellten privaten Schlüssel nicht verwenden konnte. Stellen Sie sicher, dass das Zertifikat und der Schlüssel das PEM-Format haben und die Verschlüsselung des privaten Schlüssels einen PBES1-Algorithmus nutzt.

Netzwerkkonfiguration

Damit Lambda Ihren Kafka-Cluster als Ereignisquelle verwenden kann, benötigt es Zugriff auf die Amazon VPC, in der sich Ihr Cluster befindet. Wir empfehlen, dass Sie AWS PrivateLink VPC-Endpunkte für Lambda bereitstellen, um auf Ihre VPC zuzugreifen. Stellen Sie Endpunkte für Lambda und AWS Security Token Service ()AWS STS bereit. Wenn der Broker Authentifizierung verwendet, stellen Sie auch einen VPC-Endpunkt für Secrets Manager bereit. Wenn Sie ein Ausfallziel konfiguriert haben, müssen Sie auch einen VPC-Endpunkt für den Ziel-Service bereitstellen.

Alternativ können Sie sicherstellen, dass die VPC, die Ihrem Kafka-Cluster zugeordnet ist, ein NAT-Gateway pro öffentlichem Subnetz enthält. Weitere Informationen finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Wenn Sie VPC-Endpunkte verwenden, müssen Sie sie auch so konfigurieren, dass private DNS-Namen aktiviert werden.

Wenn Sie eine Ereignisquellenzuordnung für einen MSK-Cluster erstellen, prüft Lambda, ob Elastic Network Interfaces (ENIs) bereits für die Subnetze und Sicherheitsgruppen der VPC Ihres Clusters vorhanden sind. Wenn Lambda vorhandene ENIs findet, versucht es, sie wiederzuverwenden. Andernfalls erstellt Lambda neue ENIs, um eine Verbindung zur Ereignisquelle herzustellen und Ihre Funktion aufzurufen.

> **Note**
>
> Lambda-Funktionen werden immer in VPCs ausgeführt, die dem Lambda-Service gehören. Diese VPCs werden automatisch vom Service verwaltet und sind für Kunden nicht sichtbar. Sie können Ihre Funktion auch mit einer Amazon VPC verbinden. In beiden Fällen hat die VPC-Konfiguration Ihrer Funktion keinen Einfluss auf die Zuordnung der Ereignisquelle. Nur die Konfiguration der VPC der Ereignisquelle bestimmt, wie Lambda eine Verbindung zu Ihrer Ereignisquelle herstellt.

Ihre Amazon-VPC-Konfiguration ist über die Amazon MSK API erkennbar. Sie müssen sie während der Einrichtung nicht mit dem Befehl create-event-source-mapping konfigurieren.

Weitere Informationen zur Konfiguration des Netzwerks finden Sie unter Einrichtung AWS Lambda eines Apache Kafka-Clusters innerhalb einer VPC im AWS Compute-Blog.

VPC-Sicherheitsgruppenregeln

Konfigurieren Sie die Sicherheitsgruppen für die Amazon VPC, die Ihren Cluster enthält, mit den folgenden Regeln (mindestens):

- Regeln für eingehenden Datenverkehr – Lassen Sie den gesamten Datenverkehr zum Amazon-MSK-Broker-Port (9092 für Klartext, 9094 für TLS, 9096 für SASL, 9098 für IAM) für die Sicherheitsgruppen zu, die für Ihre Ereignisquelle angegeben sind.
- Ausgehende Regeln - Erlauben Sie allen Datenverkehr auf Port 443 für alle Ziele. Lassen Sie den gesamten Datenverkehr für den Amazon-MSK-Broker-Port (9092 für Klartext, 9094 für TLS, 9096 für SASL, 9098 für IAM) für die Sicherheitsgruppen zu, die für Ihre Ereignisquelle angegeben sind.
- Wenn Sie VPC-Endpunkte anstelle eines NAT-Gateways verwenden, müssen die Sicherheitsgruppen, die mit den VPC-Endpunkten verknüpft sind, den gesamten eingehenden Datenverkehr für Port 443 von den Sicherheitsgruppen der Ereignisquelle zulassen.

Arbeiten mit VPC-Endpunkten

Wenn Sie VPC-Endpunkte verwenden, werden API-Aufrufe zum Aufrufen Ihrer Funktion mithilfe der ENIs über diese Endpunkte geleitet. Der Lambda-Serviceprinzipal muss alle Rollen `sts:AssumeRole` und `lambda:InvokeFunction` Funktionen aufrufen und aktivieren, die diese ENIs verwenden.

Standardmäßig haben VPC-Endpoints offene IAM-Richtlinien. Es hat sich bewährt, diese Richtlinien so einzuschränken, dass nur bestimmte Prinzipale die erforderlichen Aktionen über diesen Endpunkt ausführen können. Um sicherzustellen, dass Ihre Ereignisquellenzuordnung Ihre Lambda-Funktion aufrufen kann, muss die VPC-Endpunktrichtlinie zulassen, dass das Lambda-Serviceprinzip und aufruft. `sts:AssumeRole` `lambda:InvokeFunction` Wenn Sie Ihre VPC-Endpunktrichtlinien so einschränken, dass sie nur API-Aufrufe zulassen, die ihren Ursprung in Ihrer Organisation haben, verhindert, dass die Zuordnung der Ereignisquellen ordnungsgemäß funktioniert.

Die folgenden VPC-Endpunktrichtlinien zeigen, wie der erforderliche Zugriff auf den Lambda-Serviceprinzipal für die AWS STS und Lambda-Endpoints gewährt wird.

Example VPC-Endpunktrichtlinie — AWS STS Endpunkt

```
{
    "Statement": [
        {
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Example VPC-Endpunktrichtlinie — Lambda-Endpunkt

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Wenn Ihr Kafka-Broker Authentifizierung verwendet, können Sie auch die VPC-Endpunktrichtlinie für den Secrets Manager Manager-Endpunkt einschränken. Um die Secrets Manager Manager-API aufzurufen, verwendet Lambda Ihre Funktionsrolle, nicht den Lambda-Serviceprinzipal. Das folgende Beispiel zeigt eine Secrets Manager Manager-Endpunktrichtlinie.

Example VPC-Endpunktrichtlinie — Secrets Manager Manager-Endpunkt

```
{
    "Statement": [
        {
            "Action": "secretsmanager:GetSecretValue",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "customer_function_execution_role_arn"
                ]
            },
            "Resource": "customer_secret_arn"
        }
    ]
}
```

Wenn Sie ein Ziel für den Fall eines Fehlers konfiguriert haben, verwendet Lambda auch die Rolle Ihrer Funktion, um entweder `s3:PutObject`sns:Publish, oder `sqs:sendMessage` mithilfe der von Lambda verwalteten ENIs aufzurufen.

Hinzufügen von Amazon MSK als Ereignisquelle

Um ein Ereignisquellen-Mapping zu erstellen, fügen Sie Amazon MSK als Lambda-Funktionsauslöser mithilfe der Lambda-Konsole, eines AWS -SDKs oder AWS Command Line Interface (AWS CLI)

hinzu. Beachten Sie, dass Lambda beim Hinzufügen von Amazon MSK als Auslöser die VPC-Einstellungen des Amazon-MSK-Clusters annimmt, nicht die VPC-Einstellungen der Lambda-Funktion.

In diesem Abschnitt wird beschrieben, wie Sie mit der Lambda-Konsole und AWS CLI ein Ereignisquellen-Zuweisung erstellen.

Voraussetzungen

- Ein Amazon-MSK-Cluster und ein Kafka-Thema. Weitere Informationen finden Sie unter Erste Schritte mit Amazon MSK im Entwicklerhandbuch für Amazon Managed Streaming for Apache Kafka.
- Eine Ausführungsrolle mit der Berechtigung, auf die AWS Ressourcen zuzugreifen, die Ihr MSK-Cluster verwendet.

Anpassbare Konsumentengruppen-ID

Wenn Sie Kafka als Ereignisquelle einrichten, können Sie eine Konsumentengruppen-ID angeben. Diese Konsumentengruppen-ID ist eine vorhandene Kennung für die Kafka-Konsumentengruppe, der Ihre Lambda-Funktion beitreten soll. Mit diesem Feature können Sie alle laufenden Kafka-Datensatzverarbeitungs-Setups nahtlos von anderen Verbrauchern auf Lambda migrieren.

Wenn Sie eine Konsumentengruppen-ID angeben und sie innerhalb dieser Konsumentengruppe weitere aktive Poller gibt, verteilt Kafka Nachrichten an alle Konsumenten. Mit anderen Worten, Lambda erhält nicht alle Nachrichten zum Thema Kafka. Wenn Sie möchten, dass Lambda alle Nachrichten im Thema verarbeitet, deaktivieren Sie alle anderen Poller in dieser Konsumentengruppe.

Wenn Sie außerdem eine Konsumentengruppen-ID angeben und Kafka eine gültige vorhandene Konsumentengruppe mit derselben ID findet, ignoriert Lambda die `StartingPosition`-Parameter für Ihre Ereignisquellen-Zuweisung. Stattdessen beginnt Lambda mit der Verarbeitung von Datensätzen gemäß dem zugesagten Versatz der Konsumentengruppe. Wenn Sie eine Konsumentengruppen-ID angeben und Kafka keine vorhandene Konsumentengruppe finden kann, konfiguriert Lambda Ihre Ereignisquelle mit der angegebenen `StartingPosition`.

Die Konsumentengruppen-ID, die Sie angeben, muss unter all Ihren Kafka-Ereignisquellen eindeutig sein. Nachdem Sie eine Kafka-Ereignisquellenzuordnung mit der angegebenen Konsumentengruppen-ID erstellt haben, können Sie diesen Wert nicht aktualisieren.

Hinzufügen eines Amazon MSK-Auslösers (Konsole)

Befolgen Sie diese Schritte, um Ihren Amazon-MSK-Cluster und ein Kafka-Thema als Auslöser für Ihre Lambda-Funktion hinzuzufügen.

So fügen Sie Ihrer Lambda-Funktion (Konsole) einen Amazon-MSK-Auslöser hinzu

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen Ihrer Lambda-Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).
4. Führen Sie unter Auslöser-Konfiguration die folgenden Schritte aus:
    a. Wählen Sie den MSK-Auslösertyp.
    b. Wählen Sie für MSK-Cluster Ihren Cluster aus.
    c. Geben Sie für Batchgröße die maximale Anzahl von Nachrichten ein, die in einem einzelnen Batch empfangen werden sollen.
    d. Geben Sie für Batch window (Batch-Fenster) die maximale Zeit in Sekunden ein, die Lambda mit dem Sammeln von Datensätzen verbringt, bevor die Funktion aufgerufen wird.
    e. Geben Sie für Themenname den Namen eines Kafka-Themas ein.
    f. (Optional) Geben Sie für Konsumentengruppen-ID die ID einer Kafka-Konsumentengruppe ein, der Sie beitreten möchten.
    g. (Optional) Wählen Sie für Startposition die Option Neueste, um mit dem Lesen des Streams aus dem letzten Datensatz zu beginnen, Horizont trimmen, um mit dem frühesten verfügbaren Datensatz zu beginnen, oder Am Zeitstempel, um einen Zeitstempel anzugeben, ab dem mit dem Lesen begonnen werden soll.
    h. (Optional) Wählen Sie bei Authentication (Authentifizierung) den Geheimschlüssel zur Authentifizierung bei den Brokern in Ihrem MSK-Cluster aus.
    i. Um den Auslöser zu Testzwecken in einem deaktivierten Zustand zu erstellen (empfohlen), deaktivieren Sie Auslöser aktivieren. Um den Auslöser sofort zu aktivieren, wählen Sie Auslöser aktivieren.
5. Wählen Sie hinzufügen aus, um den Auslöser zu erstellen.

Hinzufügen eines Amazon-MSK-Auslösers (AWS CLI)

Verwenden Sie die folgenden AWS CLI Beispielbefehle, um einen Amazon MSK-Trigger für Ihre Lambda-Funktion zu erstellen und anzuzeigen.

Erstellen eines Triggers mit dem AWS CLI

Example – Erstellen Sie eine Zuordnung von Ereignisquellen für einen Cluster, der die IAM-Authentifizierung verwendet

Im folgenden Beispiel wird der `create-event-source-mapping` AWS CLI Befehl verwendet, um eine Lambda-Funktion mit dem Namen einem Kafka-Thema namens `my-kafka-function` zuzuordnen. `AWSKafkaTopic` Die Ausgangsposition des Themas ist auf `LATEST` festgelegt. Wenn der Cluster die rollenbasierte IAM-Authentifizierung verwendet, benötigen Sie kein Konfigurationsobjekt. SourceAccess Beispiel:

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
```

Example – Erstellen Sie eine Zuordnung von Ereignisquellen für einen Cluster, der die SASL/SCRAM-Authentifizierung verwendet

Wenn der Cluster die SASL/SCRAM-Authentifizierung verwendet, müssen Sie ein SourceAccessKonfigurationsobjekt, das spezifiziert, `SASL_SCRAM_512_AUTH` und einen geheimen Secrets Manager Manager-ARN ARN.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Example – Erstellen Sie eine Zuordnung von Ereignisquellen für einen Cluster, der die mTLS-Authentifizierung verwendet

Wenn der Cluster mTLS-Authentifizierung verwendet, müssen Sie ein SourceAccessKonfigurationsobjekt angeben, das einen geheimen Secrets Manager-ARN spezifiziert, `CLIENT_CERTIFICATE_TLS_AUTH` und einen geheimen Secrets Manager Manager-ARN ARN.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:cluster/my-cluster/fc2f5bdf-fd1b-45ad-85dd-15b4a5a6247e-2 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH","URI": "arn:aws:secretsmanager:us-east-1:111122223333:secret:my-secret"}]'
```

Weitere Informationen finden Sie in der CreateEventSourceMappingAPI-Referenzdokumentation.

Den Status mit dem anzeigen AWS CLI

Im folgenden Beispiel wird der `get-event-source-mapping` AWS CLI Befehl verwendet, um den Status der von Ihnen erstellten Ereignisquellenzuordnung zu beschreiben.

```
aws lambda get-event-source-mapping \
  --uuid 6d9bce8e-836b-442c-8070-74e77903c815
```

Erstellen von kontenübergreifenden Zuordnungen von Ereignisquellen

Sie können private Multi-VPC-Konnektivität verwenden, um eine Lambda-Funktion mit einem bereitgestellten MSK-Cluster in einem anderen AWS-Konto zu verbinden. Multi-VPC-Konnektivität verwendet AWS PrivateLink, wodurch der gesamte Datenverkehr im AWS Netzwerk bleibt.

> **Note**
>
> Sie können keine kontenübergreifenden Zuordnungen von Ereignisquellen für Serverless-MSK-Cluster erstellen.

Um eine kontenübergreifende Zuordnung von Ereignisquellen zu erstellen, müssen Sie zunächst die Multi-VPC-Konnektivität für den MSK-Cluster konfigurieren. Verwenden Sie beim Erstellen

der Zuordnung von Ereignisquellen den ARN der verwalteten VPC-Verbindung anstelle des Cluster-ARNs, wie in den folgenden Beispielen gezeigt. Der CreateEventSourceMappingVorgang unterscheidet sich auch je nachdem, welchen Authentifizierungstyp der MSK-Cluster verwendet.

Example – Erstellen Sie eine kontoübergreifende Zuordnung von Ereignisquellen für einen Cluster, der die IAM-Authentifizierung verwendet

Wenn der Cluster die rollenbasierte IAM-Authentifizierung verwendet, benötigen Sie kein Konfigurationsobjekt. SourceAccess Beispiel:

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function
```

Example – Erstellen Sie eine kontoübergreifende Zuordnung von Ereignisquellen für einen Cluster, der die SASL/SCRAM-Authentifizierung verwendet

Wenn der Cluster die SASL/SCRAM-Authentifizierung verwendet, müssen Sie ein SourceAccessKonfigurationsobjekt, das spezifiziert, `SASL_SCRAM_512_AUTH` und einen geheimen Secrets Manager Manager-ARN ARN.

Es gibt zwei Möglichkeiten, Secrets für kontenübergreifende Zuordnungen von Amazon-MSK-Ereignisquellen mit SASL/SCRAM-Authentifizierung zu verwenden:

- Erstellen Sie ein Secret im Lambda-Funktionskonto und synchronisieren Sie es mit dem Cluster-Secret. Erstellen Sie eine Rotation, um die beiden Secrets synchron zu halten. Mit dieser Option können Sie das Secret vom Funktionskonto aus kontrollieren.
- Verwenden Sie das Secret, das dem MSK-Cluster zugeordnet ist. Dieses Secret muss kontoübergreifenden Zugriff auf das Lambda-Funktionskonto ermöglichen. Weitere Informationen finden Sie unter Berechtigungen für AWS Secrets Manager geheime Daten für Benutzer mit einem anderen Konto.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
```

```
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "SASL_SCRAM_512_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Example – Erstellen Sie eine kontoübergreifende Zuordnung von Ereignisquellen für einen Cluster, der die mTLS-Authentifizierung verwendet

Wenn der Cluster mTLS-Authentifizierung verwendet, müssen Sie ein SourceAccessKonfigurationsobjekt angeben, das einen geheimen Secrets Manager-ARN spezifiziert, `CLIENT_CERTIFICATE_TLS_AUTH` und einen geheimen Secrets Manager Manager-ARN ARN. Das Secret kann im Clusterkonto oder im Lambda-Funktionskonto gespeichert werden.

```
aws lambda create-event-source-mapping \
  --event-source-arn arn:aws:kafka:us-east-1:111122223333:vpc-connection/444455556666/
my-cluster-name/51jn98b4-0a61-46cc-b0a6-61g9a3d797d5-7 \
  --topics AWSKafkaTopic \
  --starting-position LATEST \
  --function-name my-kafka-function \
  --source-access-configurations '[{"Type": "CLIENT_CERTIFICATE_TLS_AUTH","URI":
 "arn:aws:secretsmanager:us-east-1:444455556666:secret:my-secret"}]'
```

Ausfallziele

Um Datensätze zu fehlgeschlagenen Aufrufen zur Zuordnung von Ereignisquellen beizubehalten, fügen Sie der Zuordnung von Ereignisquellen Ihrer Funktion ein Ziel hinzu. Jeder an das Ziel gesendete Datensatz ist ein JSON-Dokument mit Metadaten über den fehlgeschlagenen Aufruf. Sie können jedes Amazon SNS SNS-Thema, jede Amazon SQS SQS-Warteschlange oder jeden S3-Bucket als Ziel konfigurieren. Ihre Ausführungsrolle muss über Berechtigungen für das Ziel verfügen:

- Für SQS-Ziele: sqs: SendMessage
- Für SNS-Ziele: sns:Publish
- Für S3-Bucket-Ziele: s3: und s3: PutObject ListBuckets

Wenn Sie einen KMS-Schlüssel für Ihr Ziel konfiguriert haben, benötigt Lambda außerdem je nach Zieltyp folgende Berechtigungen:

- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für ein S3-Ziel aktiviert haben, ist kms: GenerateData Key erforderlich. Wenn sich der KMS-Schlüssel und das S3-Bucket-Ziel

in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut, um kms: GenerateData Key zuzulassen.

- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für das SQS-Ziel aktiviert haben, sind kms:Decrypt und kms: Key erforderlich. GenerateData Wenn sich der KMS-Schlüssel und das SQS-Warteschlangenziel in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut und kms:Decrypt, kms: GenerateData Key, kms: und kms: zulässt. DescribeKey ReEncrypt
- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für das SNS-Ziel aktiviert haben, sind kms:Decrypt und kms: Key erforderlich. GenerateData Wenn sich der KMS-Schlüssel und das SNS-Themenziel in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut, sodass kms:Decrypt, kms: GenerateData Key, kms: und kms: zugelassen werden. DescribeKey ReEncrypt

Gehen Sie folgendermaßen vor, um ein Ausfallziel mit der Konsole zu konfigurieren:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add destination (Ziel hinzufügen).
4. Wählen Sie als Quelle die Option Aufruf der Zuordnung von Ereignisquellen aus.
5. Wählen Sie für die Zuordnung von Ereignisquellen eine Ereignisquelle aus, die für diese Funktion konfiguriert ist.
6. Wählen Sie für Bedingung die Option Bei Ausfall aus. Für Aufrufe zur Zuordnung von Ereignisquellen ist dies die einzig akzeptierte Bedingung.
7. Wählen Sie unter Zieltyp den Zieltyp aus, an den Lambda Aufrufdatensätze sendet.
8. Wählen Sie unter Destination (Ziel) eine Ressource aus.
9. Wählen Sie Save aus.

Sie können mit dem auch ein Ziel für den Fall eines Fehlers konfigurieren. AWS CLI Mit dem folgenden Befehl create-event-source-mapping wird beispielsweise eine Ereignisquellenzuordnung mit einem SQS-Ziel für den Fall eines Fehlers hinzugefügt: `MyFunction`

```
aws lambda create-event-source-mapping \
```

```
--function-name "MyFunction" \
--event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

Der folgende Befehl update-event-source-mapping fügt der mit der Eingabe verknüpften Ereignisquelle ein S3-Ziel für den Fall eines Fehlers hinzu: `uuid`

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": "arn:aws:s3:::dest-bucket"}}'
```

Um ein Ziel zu entfernen, geben Sie eine leere Zeichenfolge als Argument für den `destination-config`-Parameter an:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Beispielaufrufsdatensatz für SNS und SQS

Das folgende Beispiel zeigt, was Lambda bei einem fehlgeschlagenen Aufruf der Kafka-Ereignisquelle an ein SNS-Thema oder eine SQS-Warteschlange sendet. Jeder der Schlüssel unter `recordsInfo` enthält sowohl das Kafka-Thema als auch die Kafka-Partition, getrennt durch einen Bindestrich. Bei dem Schlüssel `"Topic-0"` handelt es sich beispielsweise bei `Topic` um das Kafka-Thema und bei `0` um die Partition. Für jedes Thema und jede Partition können Sie die Offsets und Zeitstempeldaten verwenden, um die ursprünglichen Aufrufdatensätze zu finden.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
```

```
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    }
}
```

Beispiel für einen S3-Zielaufrufdatensatz

Für S3-Ziele sendet Lambda den gesamten Aufrufdatensatz zusammen mit den Metadaten an das Ziel. Das folgende Beispiel zeigt, was Lambda bei einem fehlgeschlagenen Aufruf der Kafka-Ereignisquelle an ein S3-Bucket-Ziel sendet. Zusätzlich zu allen Feldern aus dem vorherigen Beispiel für SQS- und SNS-Ziele enthält das Feld `payload` den ursprünglichen Aufrufdatensatz als maskierte JSON-Zeichenfolge.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
```

```
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    },
    "payload": "<Whole Event>" // Only available in S3
}
```

> **Tip**
>
> Wir empfehlen außerdem, die S3-Versionsverwaltung in Ihrem Ziel-Bucket zu aktivieren.

Automatische Skalierung der Amazon-MSK-Ereignisquelle

Wenn Sie anfänglich eine Amazon-MSK-Ereignisquelle erstellen, weist Lambda einen Konsumenten zur Verarbeitung aller Partitionen im Kafka-Thema zu. Jeder Verbraucher hat mehrere Prozessoren, die parallel laufen, um erhöhte Workloads zu bewältigen. Lambda skaliert außerdem je nach Workload automatisch die Anzahl der Verbraucher nach oben oder unten. Um die Nachrichtenreihenfolge in jeder Partition beizubehalten, ist die maximale Anzahl von Verbrauchern pro Partition im Thema ein Verbraucher pro Partition.

In Intervallen von einer Minute wertet Lambda die Verbraucher-Offsetverzögerung aller Partitionen im Thema aus. Wenn die Verzögerung zu hoch ist, empfängt die Partition Nachrichten schneller als Lambda sie verarbeiten kann. Bei Bedarf fügt Lambda dem Thema Verbraucher hinzu oder entfernt sie. Der Skalierungsprozess zum Hinzufügen oder Entfernen von Verbrauchern erfolgt innerhalb von drei Minuten nach der Bewertung.

Wenn Ihre Lambda-Zielfunktion gedrosselt ist, verringert Lambda die Anzahl der Verbraucher. Diese Aktion reduziert die Workload für die Funktion, indem die Anzahl der Nachrichten reduziert wird, die Verbraucher abrufen und an die Funktion senden können.

Um den Durchsatz Ihres Kafka-Themas zu überwachen, sehen Sie sich die Offset-Verzögerungsmetrik an, die Lambda emittiert, während Ihre Funktion Datensätze verarbeitet.

Um zu überprüfen, wie viele Funktionsaufrufe parallel erfolgen, können Sie auch die Parallelitätsmetriken für Ihre Funktion überwachen.

Startpositionen für Abfragen und Streams

Beachten Sie, dass die Stream-Abfrage bei der Erstellung und Aktualisierung der Zuordnung von Ereignisquellen letztendlich konsistent ist.

- Bei der Erstellung der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis mit der Abfrage von Ereignissen aus dem Stream begonnen wird.
- Bei Aktualisierungen der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis die Abfrage von Ereignissen aus dem Stream gestoppt und neu gestartet wird.

Dieses Verhalten bedeutet, dass, wenn Sie `LATEST` als Startposition für den Stream angeben, die Zuordnung von Ereignisquellen bei der Erstellung oder Aktualisierung möglicherweise Ereignisse übersieht. Um sicherzustellen, dass keine Ereignisse übersehen werden, geben Sie die Startposition des Streams als `TRIM_HORIZON` oder `AT_TIMESTAMP` an.

CloudWatch Amazon-Metriken

Lambda gibt die Metrik `OffsetLag` aus, während Ihre Funktion Datensätze verarbeitet. Der Wert dieser Metrik ist die Differenz (der Versatz) zwischen dem letzten Datensatz, der ins Kafka-Ereignisquellen-Thema geschrieben wurde, und dem letzten Datensatz, den die Konsumentengruppe Ihrer Funktion verarbeitet hat. Sie können mit `OffsetLag` die Latenz zwischen dem Hinzufügen eines Datensatzes und der Verarbeitung des Datensatzes durch Ihre Konsumentengruppe abschätzen.

Ein zunehmender Trend in `OffsetLag` kann auf Probleme mit Pollern in der Konsumentengruppe Ihrer Funktion hinweisen. Weitere Informationen finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Amazon-MSK-Konfigurationsparameter

Alle Lambda-Ereignisquelltypen verwenden dieselben CreateEventSourceMappingUpdateEventSourceMappingAPI-Operationen. Allerdings gelten nur einige der Parameter für Amazon MSK.

Ereignisquellparameter, die für Amazon MSK gelten

Parameter	Erforderlich	Standard	Hinweise
AmazonManagedKafkaEventSourceConfig	N	Enthält das ConsumerGroupId Feld, das standardmäßig einen eindeutigen Wert hat.	Kann nur auf „Erstellen“ festgelegt werden
BatchSize	N	100	Höchstwert: 10 000.
Enabled	N	Aktiviert	
EventSourceArn	Y		Kann nur auf „Erstellen“ festgelegt werden
FunctionName	Y		
FilterCriteria	N		Lambda-Ereignisfilterung

Parameter	Erforderlich	Standard	Hinweise
MaximumBatchingWindowInSekunden	N	500 ms	Batching-Verhalten
SourceAccessKonfigurationen	N	Keine Anmeldedaten	Anmeldeinformationen zur SASL/SCRAM- oder CLIENT_CERTIFICATE_TLS_AUTH (MutualTLS)-Authentifizierung für Ihre Ereignisquelle
StartingPosition	Y		AT_TIMESTAMP, TRIM_HORIZON, oder LATEST Kann nur auf „Erstellen“ festgelegt werden
StartingPositionZeitstempel	N		Erforderlich, wenn auf StartingPosition AT_TIMESTAMP gesetzt ist
Themen	Y		Kafka-Thema-Name Kann nur auf „Erstellen“ festgelegt werden

Verwendung von Lambda mit selbstverwaltetem Apache Kafka

> **Note**
>
> Wenn Sie Daten an ein anderes Ziel als eine Lambda-Funktion senden oder die Daten vor dem Senden anreichern möchten, finden Sie weitere Informationen unter Amazon EventBridge Pipes.

Lambda unterstützt Apache Kafka als Ereignisquelle. Apache Kafka ist eine Open-Source-Event-Streaming-Plattform, die Workloads wie Datenpipelines und Streaming-Analysen unterstützt.

Sie können den AWS verwalteten Kafka-Service Amazon Managed Streaming for Apache Kafka (Amazon MSK) oder einen selbstverwalteten Kafka-Cluster verwenden. Weitere Informationen über die Verwendung von Lambda mit Amazon MSK finden Sie unter Verwenden von Lambda mit Amazon MSK.

In diesem Thema wird die Verwendung von Lambda mit einem selbstverwalteten Kafka-Cluster beschrieben. In der AWS Terminologie umfasst ein selbstverwalteter Cluster auch nicht gehostete Kafka-Cluster.AWS Sie können Ihren Kafka-Cluster beispielsweise bei einem Cloud-Anbieter wie Confluent Cloud hosten.

Apache Kafka als Ereignisquelle funktioniert ähnlich wie die Verwendung von Amazon Simple Queue Service (Amazon SQS) oder Amazon Kinesis. Lambda fragt intern neue Nachrichten von der Ereignisquelle ab und ruft dann synchron die Ziel-Lambda-Funktion auf. Lambda liest die Nachrichten in Batches und stellt diese Ihrer Funktion als Ereignisnutzlast zur Verfügung. Die maximale Batchgröße ist konfigurierbar. (Der Standardwert beträgt 100 Nachrichten.)

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Für Kafka-basierte Ereignisquellen unterstützt Lambda die Verarbeitung von Steuerungsparametern wie Batch-Fenster und -Größe. Weitere Informationen finden Sie unter Batching-Verhalten.

Ein Beispiel für die Verwendung von selbstverwaltetem Kafka als Ereignisquelle finden Sie im Compute-Blog unter Verwenden von selbst gehostetem Apache Kafka als Ereignisquelle für. AWS Lambda AWS

Themen

Beispielereignis

Lambda sendet den Batch von Nachrichten im Ereignisparameter, wenn es Ihre Lambda-Funktion aufruft. Die Ereignisquelle enthält ein Array von Nachrichten. Jedes Array-Element enthält Details zum Kafka-Thema und Kafka-Partitions-ID, zusammen mit einem Zeitstempel und einer base64-codierten Nachricht.

```
{
   "eventSource": "SelfManagedKafka",
   "bootstrapServers":"b-2.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092,b-1.demo-cluster-1.a1bcde.c1.kafka.us-
east-1.amazonaws.com:9092",
   "records":{
      "mytopic-0":[
         {
            "topic":"mytopic",
            "partition":0,
```

```
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "key":"abcDEFghiJKLmnoPQRstuVWXyz1234==",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[
               {
                  "headerKey":[
                     104,
                     101,
                     97,
                     100,
                     101,
                     114,
                     86,
                     97,
                     108,
                     117,
                     101
                  ]
               }
            ]
         }
      ]
   }
}
```

Authentifizierung für Kafka-Cluster

Lambda unterstützt mehrere Methoden zur Authentifizierung mit Ihrem selbstverwalteten Apache-Kafka-Cluster. Stellen Sie sicher, dass Sie den Kafka-Cluster für die Verwendung einer der folgenden unterstützten Authentifizierungsmethoden konfigurieren. Weitere Informationen zur Sicherheit von Kafka finden Sie unter Sicherheit in der Kafka-Dokumentation.

VPC-Zugriff

Wenn nur Kafka-Benutzer in Ihrer VPC auf Ihre Kafka-Broker zugreifen, müssen Sie die Kafka-Ereignisquelle für Zugriff auf Amazon Virtual Private Cloud (Amazon VPC) konfigurieren.

SASL/SCRAM-Authentifizierung

Lambda unterstützt die Authentifizierung mit Transport Layer Security (TLS)-Verschlüsselung (`SASL_SSL`) von Simple Authentication and Security Layer/Salted Challenge Response

Authentication Mechanism (SASL/SCRAM). Lambda sendet die verschlüsselten Anmeldeinformationen zur Authentifizierung mit dem Cluster. Lambda unterstützt SASL/SCRAM mit Klartext (`SASL_PLAINTEXT`) nicht. Weitere Informationen zur IAM-Authentifizierung finden Sie unter RFC 5802.

Lambda unterstützt auch die SASL/PLAIN-Authentifizierung. Da dieser Mechanismus Anmeldeinformationen im Klartext verwendet, muss die Verbindung zum Server TLS-Verschlüsselung verwenden, um sicherzustellen, dass die Anmeldeinformationen geschützt sind.

Für die SASL-Authentifizierung speichern Sie die Anmeldeinformationen als Secret in AWS Secrets Manager. Weitere Informationen zur Verwendung von Secrets Manager finden Sie im Tutorial: Erstellen und Abrufen eines Secrets im Benutzerhandbuch für AWS Secrets Manager .

> **Important**
>
> Um Secrets Manager für die Authentifizierung zu verwenden, müssen Geheimnisse in derselben AWS Region wie Ihre Lambda-Funktion gespeichert werden.

Gegenseitige TLS-Authentifizierung

Gegenseitige TLS (mTLS) bietet eine bidirektionale Authentifizierung zwischen Client und Server. Der Client sendet ein Zertifikat an den Server, damit der Server den Client überprüfen kann, und der Server sendet ein Zertifikat an den Client, damit der Client den Server überprüfen kann.

Im selbstverwalteten Apache Kafka fungiert Lambda als Client. Sie konfigurieren ein Client-Zertifikat (als Secret in Secrets Manager), um Lambda für Ihre Kafka-Broker zu authentifizieren. Das Client-Zertifikat muss von einer Zertifizierungsstelle im Trust Store des Servers signiert sein.

Der Kafka-Cluster sendet ein Serverzertifikat an Lambda, um die Kafka-Broker für Lambda zu authentifizieren. Das Serverzertifikat kann ein öffentliches CA-Zertifikat oder ein privates CA-Zertifikat/selbstsigniertes Zertifikat sein. Das öffentliche CA-Zertifikat muss von einer Zertifizierungsstelle (CA) signiert sein, die sich im Trust Store von Lambda befindet. Für ein privates CA-Zertifikat/selbstsigniertes Zertifikat konfigurieren Sie das Server-Root-CA-Zertifikat (als Secret in Secrets Manager). Lambda verwendet das Root-Zertifikat, um die Kafka-Broker zu verifizieren.

Weitere Informationen über mTLS finden Sie unter Vorstellung von gegenseitiger TLS-Authentifizierung für Amazon MSK als Ereignisquelle.

Konfigurieren des Client-Zertifikat-Secrets

Das Secret CLIENT_CERTIFICATE_TLS_AUTH erfordert ein Zertifikatfeld und ein Feld für einen privaten Schlüssel. Für einen verschlüsselten privaten Schlüssel erfordert das Secret ein Passwort für den privaten Schlüssel. Sowohl das Zertifikat als auch der private Schlüssel müssen im PEM-Format vorliegen.

> **Note**
>
> Lambda unterstützt die PBES1-Algorithmen (aber nicht PBES2) zur Verschlüsselung von privaten Schlüsseln.

Das Zertifikatfeld muss eine Liste von Zertifikaten enthalten, beginnend mit dem Client-Zertifikat, gefolgt von etwaigen Zwischenzertifikaten und endend mit dem Root-Zertifikat. Jedes Zertifikat muss in einer neuen Zeile mit der folgenden Struktur beginnen:

```
-----BEGIN CERTIFICATE-----
        <certificate contents>
-----END CERTIFICATE-----
```

Secrets Manager unterstützt Secrets von bis zu 65 536 Bytes, was genügend Platz für lange Zertifikatsketten bietet.

Der private Schlüssel muss im Format PKCS #8 mit folgender Struktur vorliegen:

```
-----BEGIN PRIVATE KEY-----
         <private key contents>
-----END PRIVATE KEY-----
```

Verwenden Sie für einen verschlüsselten privaten Schlüssel die folgende Struktur:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
          <private key contents>
-----END ENCRYPTED PRIVATE KEY-----
```

Im folgenden Beispiel sehen Sie den Inhalt eines Secrets für mTLS-Authentifizierung mit einem verschlüsselten privaten Schlüssel. Fügen Sie für einen verschlüsselten privaten Schlüssel das Passwort für den privaten Schlüssel in das Secret ein.

```
{"privateKeyPassword":"testpassword",
"certificate":"-----BEGIN CERTIFICATE-----
MIIE5DCCAsygAwIBAgIRAPJdwaFaNRrytHBto0j5BA0wDQYJKoZIhvcNAQELBQAw
...
j0Lh4/+1HfgyE2KlmII36dg4IMzNjAFEBZiCRoPimO40s1cRqtFHXoal0QQbIlxk
cmUuiAii9R0=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFgjCCA2qgAwIBAgIQdjNZd6uFf9hbNC5RdfmHrzANBgkqhkiG9w0BAQsFADBb
...
rQoiowbbk5wXCheYSANQIfTZ6weQTgiCHCCbuuMKNVS95FkXm0vqVD/YpXKwA/no
c8PH3PSoAaRwMMgOSA2ALJvbRz8mpg==
-----END CERTIFICATE-----",
"privateKey":"-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFKzBVBgkqhkiG9w0BBQ0wSDAnBgkqhkiG9w0BBQwwGgQUiAFcK5hT/X7Kjmgp
...
QrSekqF+kWzmB6nAfSzgO9IaoAaytLvNgGTckWeUkWn/V0Ck+LdGUXzAC4RxZnoQ
zp2mwJn2NYB7AZ7+imp0azDZb+8YG2aUCiyqb6PnnA==
-----END ENCRYPTED PRIVATE KEY-----"
}
```

Konfigurieren des Secrets des Server-Root-CA-Zertifikats

Sie erstellen dieses Secret, wenn Ihre Kafka-Broker TLS-Verschlüsselung mit Zertifikaten verwenden, die von einer privaten CA signiert wurden. Sie können die TLS-Verschlüsselung zur VPC-, SASL/SCRAM-, SASL/PLAIN- oder mTLS-Authentifizierung verwenden.

Das Secret des Server-Root-CA-Zertifikats erfordert ein Feld, das das Root-CA-Zertifikat des Kafka-Brokers im PEM-Format enthält. Das folgende Beispiel zeigt die Struktur des Secrets.

```
{"certificate":"-----BEGIN CERTIFICATE-----
MIID7zCCAtegAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxJTAjBgNVBAoT
HFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xOzA5BgNVBAMTMlN0YXJmaWVs
ZCBTZXJ2aWNlcyBSb290IENlcnRpZmljYXRlIEF1dG...
-----END CERTIFICATE-----"
}
```

Verwalten von API-Zugriff und -Berechtigungen

Neben dem Zugriff auf Ihren selbstverwalteten Kafka-Cluster benötigt Ihre Lambda-Funktion auch Berechtigungen, um verschiedene API-Aktionen auszuführen. Sie fügen diese Berechtigungen zur

Ausführungsrolle der Funktion hinzu. Wenn Ihre Benutzer Zugriff auf API-Aktionen benötigen, fügen Sie der Identitätsrichtlinie für den AWS Identity and Access Management (IAM-) Benutzer oder die Rolle die erforderlichen Berechtigungen hinzu.

Benötigte Lambda-Funktionsberechtigungen

Um Protokolle in einer Protokollgruppe in Amazon CloudWatch Logs zu erstellen und zu speichern, muss Ihre Lambda-Funktion in ihrer Ausführungsrolle über die folgenden Berechtigungen verfügen:

- Logs: Gruppe CreateLog
- Protokolle: CreateLog Stream
- Protokolle: PutLog Ereignisse

Optionale Lambda-Funktionsberechtigungen

Ihre Lambda-Funktion benötigt möglicherweise auch Berechtigungen für Folgendes:

- Beschreiben Ihres Secrets-Manager-Secrets
- Greifen Sie auf Ihren AWS Key Management Service (AWS KMS) vom Kunden verwalteten Schlüssel zu.
- Zugriff auf Ihre Amazon VPC
- Senden von Datensätzen zu fehlgeschlagenen Aufrufen an ein Ziel

Secrets Manager und AWS KMS Berechtigungen

Abhängig von der Art der Zugriffskontrolle, die Sie für Ihre Kafka-Broker konfigurieren, benötigt Ihre Lambda-Funktion möglicherweise die Erlaubnis, auf Ihr Secrets Manager-Geheimnis zuzugreifen oder Ihren vom AWS KMS Kunden verwalteten Schlüssel zu entschlüsseln. Um auf diese Ressourcen zuzugreifen, muss die Ausführungsrolle Ihrer Funktion die folgenden Berechtigungen besitzen:

- secretsmanager: Wert GetSecret
- kms:Decrypt

VPC-Berechtigungen

Wenn nur Benutzer innerhalb einer VPC auf Ihren selbstverwalteten Apache-Kafka-Cluster zugreifen können, muss Ihre Lambda-Funktion die Berechtigung zum Zugriff auf Ihre Amazon-VPC-

Ressourcen haben. Zu diesen Ressourcen gehören Ihre VPC, Subnetze, Sicherheitsgruppen und Netzwerkschnittstellen. Um auf diese Ressourcen zuzugreifen, muss die Ausführungsrolle Ihrer Funktion die folgenden Berechtigungen besitzen:

- ec2: Schnittstelle CreateNetwork
- ec2: Schnittstellen DescribeNetwork
- ec2: DescribeVpcs
- ec2: Schnittstelle DeleteNetwork
- ec2: DescribeSubnets
- ec2: Gruppen DescribeSecurity

Hinzufügen von Berechtigungen zu Ihrer Ausführungsrolle

Um auf andere AWS Dienste zuzugreifen, die Ihr selbstverwalteter Apache Kafka-Cluster verwendet, verwendet Lambda die Berechtigungsrichtlinien, die Sie in der Ausführungsrolle Ihrer Lambda-Funktion definieren.

Standardmäßig ist es Lambda nicht gestattet, die erforderlichen oder optionalen Aktionen für einen selbstverwalteten Apache-Kafka-Cluster durchzuführen. Sie müssen diese Aktionen in einer IAM-Vertrauensrichtlinie erstellen und definieren und die Richtlinie dann an Ihre Ausführungsrolle anhängen. In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, die Lambda den Zugriff auf Ihre Amazon-VPC-Ressourcen erlaubt.

```
{
        "Version":"2012-10-17",
        "Statement":[
           {
              "Effect":"Allow",
              "Action":[
                 "ec2:CreateNetworkInterface",
                 "ec2:DescribeNetworkInterfaces",
                 "ec2:DescribeVpcs",
                 "ec2:DeleteNetworkInterface",
                 "ec2:DescribeSubnets",
                 "ec2:DescribeSecurityGroups"
              ],
              "Resource":"*"
           }
        ]
```

```
    }
```

Informationen zum Erstellen eines JSON-Richtliniendokuments auf der IAM-Konsole finden Sie unter Erstellen von Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.

Gewähren von Benutzerzugriff mit einer IAM-Richtlinie

Standardmäßig haben Benutzer und Rollen keine Berechtigung zum Ausführen von Ereignisquellen-API-Vorgängen. Um Benutzern in Ihrem Unternehmen oder Ihrem Konto Zugriff zu gewähren, erstellen oder aktualisieren Sie eine identitätsbasierte Richtlinie. Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Richtlinien im IAM-Benutzerhandbuch.

Authentifizierungs- und Autorisierungsfehler

Wenn eine der für die Nutzung von Daten aus dem Kafka-Cluster erforderlichen Berechtigungen fehlt, zeigt Lambda in der Ereignisquellenzuordnung unter LastProcessing Ergebnis eine der folgenden Fehlermeldungen an.

Fehlermeldungen

- Cluster konnte Lambda nicht autorisieren
- SASL-Authentifizierung fehlgeschlagen
- Server konnte Lambda nicht authentifizieren
- Lambda konnte Server nicht authentifizieren
- Bereitgestelltes Zertifikat oder bereitgestellter privater Schlüssel ist ungültig

Cluster konnte Lambda nicht autorisieren

Bei SASL/SCRAM oder mTLS weist dieser Fehler darauf hin, dass der angegebene Benutzer nicht über alle nachfolgenden erforderlichen Berechtigungen für die Kafka-Zugriffskontrollliste (ACL) verfügt:

- DescribeConfigs Cluster
- Beschreiben von Gruppe
- Gruppe lesen
- Thema beschreiben
- Thema lesen

Wenn Sie Kafka-ACLs mit den erforderlichen `kafka-cluster`-Berechtigungen erstellen, geben Sie das Thema und die Gruppe als Ressourcen an. Der Themenname muss mit dem Thema in der Ereignisquellenzuordnung übereinstimmen. Der Gruppenname muss mit der UUID der Ereignisquellenzuordnung übereinstimmen.

Nachdem Sie der Ausführungsrolle die erforderlichen Berechtigungen hinzugefügt haben, kann es einige Minuten dauern, bis die Änderungen wirksam werden.

SASL-Authentifizierung fehlgeschlagen

Bei SASL/SCRAM oder SASL/PLAIN weist dieser Fehler darauf hin, dass die angegebenen Anmeldeinformationen ungültig sind.

Server konnte Lambda nicht authentifizieren

Dieser Fehler weist darauf hin, dass der Kafka-Broker Lambda nicht authentifizieren konnte. Dieser Fehler kann aus folgenden Gründen auftreten:

- Sie haben kein Client-Zertifikat für die mTLS-Authentifizierung bereitgestellt.
- Sie haben ein Client-Zertifikat bereitgestellt, aber die Kafka-Broker sind nicht für die Verwendung der mTLS-Authentifizierung konfiguriert.
- Die Kafka-Broker vertrauen einem Client-Zertifikat nicht.

Lambda konnte Server nicht authentifizieren

Dieser Fehler weist darauf hin, dass Lambda den Kafka-Broker nicht authentifizieren konnte. Dieser Fehler kann aus folgenden Gründen auftreten:

- Die Kafka-Broker verwenden selbstsignierte Zertifikate oder eine private Zertifizierungsstelle (CA), haben jedoch das Server-Root-CA-Zertifikat nicht bereitgestellt.
- Das Server-Root-CA-Zertifikat stimmt nicht mit der Root-CA überein, die das Zertifikat des Brokers signiert hat.
- Die Überprüfung des Hostnamens ist fehlgeschlagen, weil das Zertifikat des Brokers nicht den DNS-Namen oder die IP-Adresse des Brokers als alternativen Betreffnamen enthält.

Bereitgestelltes Zertifikat oder bereitgestellter privater Schlüssel ist ungültig

Dieser Fehler weist darauf hin, dass der Kafka-Konsument das bereitgestellte Zertifikat oder den bereitgestellten privaten Schlüssel nicht verwenden konnte. Stellen Sie sicher, dass das Zertifikat

und der Schlüssel das PEM-Format haben und die Verschlüsselung des privaten Schlüssels einen PBES1-Algorithmus nutzt.

Netzwerkkonfiguration

Damit Lambda Ihren Kafka-Cluster als Ereignisquelle verwenden kann, benötigt es Zugriff auf die Amazon VPC, in der sich Ihr Cluster befindet. Wir empfehlen, dass Sie AWS PrivateLink VPC-Endpunkte für Lambda bereitstellen, um auf Ihre VPC zuzugreifen. Stellen Sie Endpunkte für Lambda und AWS Security Token Service ()AWS STS bereit. Wenn der Broker Authentifizierung verwendet, stellen Sie auch einen VPC-Endpunkt für Secrets Manager bereit. Wenn Sie ein Ausfallziel konfiguriert haben, müssen Sie auch einen VPC-Endpunkt für den Ziel-Service bereitstellen.

Alternativ können Sie sicherstellen, dass die VPC, die Ihrem Kafka-Cluster zugeordnet ist, ein NAT-Gateway pro öffentlichem Subnetz enthält. Weitere Informationen finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Wenn Sie VPC-Endpunkte verwenden, müssen Sie sie auch so konfigurieren, dass private DNS-Namen aktiviert werden.

Wenn Sie eine Ereignisquellenzuordnung für einen selbstverwalteten Apache Kafka-Cluster erstellen, prüft Lambda, ob Elastic Network Interfaces (ENIs) bereits für die Subnetze und Sicherheitsgruppen der VPC Ihres Clusters vorhanden sind. Wenn Lambda vorhandene ENIs findet, versucht es, sie wiederzuverwenden. Andernfalls erstellt Lambda neue ENIs, um eine Verbindung zur Ereignisquelle herzustellen und Ihre Funktion aufzurufen.

> **Note**
>
> Lambda-Funktionen werden immer in VPCs ausgeführt, die dem Lambda-Service gehören. Diese VPCs werden automatisch vom Service verwaltet und sind für Kunden nicht sichtbar. Sie können Ihre Funktion auch mit einer Amazon VPC verbinden. In beiden Fällen hat die VPC-Konfiguration Ihrer Funktion keinen Einfluss auf die Zuordnung der Ereignisquelle. Nur die Konfiguration der VPC der Ereignisquelle bestimmt, wie Lambda eine Verbindung zu Ihrer Ereignisquelle herstellt.

Weitere Informationen zur Konfiguration des Netzwerks finden Sie unter Einrichtung AWS Lambda eines Apache Kafka-Clusters innerhalb einer VPC im AWS Compute-Blog.

VPC-Sicherheitsgruppenregeln

Konfigurieren Sie die Sicherheitsgruppen für die Amazon VPC, die Ihren Cluster enthält, mit den folgenden Regeln (mindestens):

- Regeln für eingehenden Datenverkehr – Lassen den gesamten Datenverkehr zum Port des Kafka-Brokers für die Sicherheitsgruppen zu, die für Ihre Ereignisquelle angegeben sind. Kafka verwendet standardmäßig Port 9092.
- Ausgehende Regeln - Erlauben Sie allen Datenverkehr auf Port 443 für alle Ziele. Lassen den gesamten Datenverkehr zum Port des Kafka-Brokers für die Sicherheitsgruppen zu, die für Ihre Ereignisquelle angegeben sind. Kafka verwendet standardmäßig Port 9092.
- Wenn Sie VPC-Endpunkte anstelle eines NAT-Gateways verwenden, müssen die Sicherheitsgruppen, die mit den VPC-Endpunkten verknüpft sind, den gesamten eingehenden Datenverkehr für Port 443 von den Sicherheitsgruppen der Ereignisquelle zulassen.

Arbeiten mit VPC-Endpunkten

Wenn Sie VPC-Endpunkte verwenden, werden API-Aufrufe zum Aufrufen Ihrer Funktion mithilfe der ENIs über diese Endpunkte geleitet. Der Lambda-Serviceprinzipal muss alle Rollen `sts:AssumeRole` und `lambda:InvokeFunction` Funktionen aufrufen und aktivieren, die diese ENIs verwenden.

Standardmäßig haben VPC-Endpoints offene IAM-Richtlinien. Es hat sich bewährt, diese Richtlinien so einzuschränken, dass nur bestimmte Prinzipale die erforderlichen Aktionen über diesen Endpunkt ausführen können. Um sicherzustellen, dass Ihre Ereignisquellenzuordnung Ihre Lambda-Funktion aufrufen kann, muss die VPC-Endpunktrichtlinie zulassen, dass das Lambda-Serviceprinzip und aufruft. `sts:AssumeRole` `lambda:InvokeFunction` Wenn Sie Ihre VPC-Endpunktrichtlinien so einschränken, dass sie nur API-Aufrufe zulassen, die ihren Ursprung in Ihrer Organisation haben, verhindert, dass die Zuordnung der Ereignisquellen ordnungsgemäß funktioniert.

Die folgenden VPC-Endpunktrichtlinien zeigen, wie der erforderliche Zugriff auf den Lambda-Serviceprinzipal für die AWS STS und Lambda-Endpoints gewährt wird.

Example VPC-Endpunktrichtlinie — AWS STS Endpunkt

```
{
    "Statement": [
        {
```

```
            "Action": "sts:AssumeRole",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Example VPC-Endpunktrichtlinie — Lambda-Endpunkt

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
            "Resource": "*"
        }
    ]
}
```

Wenn Ihr Kafka-Broker Authentifizierung verwendet, können Sie auch die VPC-Endpunktrichtlinie für den Secrets Manager Manager-Endpunkt einschränken. Um die Secrets Manager Manager-API aufzurufen, verwendet Lambda Ihre Funktionsrolle, nicht den Lambda-Serviceprinzipal. Das folgende Beispiel zeigt eine Secrets Manager Manager-Endpunktrichtlinie.

Example VPC-Endpunktrichtlinie — Secrets Manager Manager-Endpunkt

```
{
    "Statement": [
        {
            "Action": "secretsmanager:GetSecretValue",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": [
                    "customer_function_execution_role_arn"
                ]
            },
            "Resource": "customer_secret_arn"
        }
    ]
}
```

Wenn Sie ein Ziel für den Fall eines Fehlers konfiguriert haben, verwendet Lambda auch die Rolle Ihrer Funktion, um entweder `s3:PutObject`sns:Publish, oder `sqs:sendMessage` mithilfe der von Lambda verwalteten ENIs aufzurufen.

Hinzufügen eines Kafka-Clusters als Ereignisquelle

Um eine Ereignisquellenzuordnung zu erstellen, fügen Sie Ihren Kafka-Cluster als einen Lambda-Funktions-Auslöser hinzu und verwenden Sie dabei die Lambda-Konsole, ein AWS -SDK oder die AWS Command Line Interface (AWS CLI).

In diesem Abschnitt wird beschrieben, wie Sie mit der Lambda-Konsole und AWS CLI ein Ereignisquellen-Zuweisung erstellen.

Voraussetzungen

- Selbstverwaltetes Apache-Kafka-Cluster. Lambda unterstützt Apache Kafka Version 0.10.1.0 und höher.
- Eine Ausführungsrolle mit der Berechtigung, auf die AWS Ressourcen zuzugreifen, die Ihr selbstverwalteter Kafka-Cluster verwendet.

Anpassbare Konsumentengruppen-ID

Wenn Sie Kafka als Ereignisquelle einrichten, können Sie eine Konsumentengruppen-ID angeben. Diese Konsumentengruppen-ID ist eine vorhandene Kennung für die Kafka-Konsumentengruppe, der Ihre Lambda-Funktion beitreten soll. Mit diesem Feature können Sie alle laufenden Kafka-Datensatzverarbeitungs-Setups nahtlos von anderen Verbrauchern auf Lambda migrieren.

Wenn Sie eine Konsumentengruppen-ID angeben und sie innerhalb dieser Konsumentengruppe weitere aktive Poller gibt, verteilt Kafka Nachrichten an alle Konsumenten. Mit anderen Worten, Lambda erhält nicht alle Nachrichten zum Thema Kafka. Wenn Sie möchten, dass

Lambda alle Nachrichten im Thema verarbeitet, deaktivieren Sie alle anderen Poller in dieser Konsumentengruppe.

Wenn Sie außerdem eine Konsumentengruppen-ID angeben und Kafka eine gültige vorhandene Konsumentengruppe mit derselben ID findet, ignoriert Lambda die `StartingPosition`-Parameter für Ihre Ereignisquellen-Zuweisung. Stattdessen beginnt Lambda mit der Verarbeitung von Datensätzen gemäß dem zugesagten Versatz der Konsumentengruppe. Wenn Sie eine Konsumentengruppen-ID angeben und Kafka keine vorhandene Konsumentengruppe finden kann, konfiguriert Lambda Ihre Ereignisquelle mit der angegebenen `StartingPosition`.

Die Konsumentengruppen-ID, die Sie angeben, muss unter all Ihren Kafka-Ereignisquellen eindeutig sein. Nachdem Sie eine Kafka-Ereignisquellenzuordnung mit der angegebenen Konsumentengruppen-ID erstellt haben, können Sie diesen Wert nicht aktualisieren.

Hinzufügen eines selbstverwalteten Kafka-Clusters (Konsole)

Befolgen Sie diese Schritte, um Ihren selbstverwalteten Apache-Kafka-Cluster und ein Kafka-Thema als Auslöser für Ihre Lambda-Funktion hinzuzufügen.

So fügen Sie Ihrer Lambda-Funktion (Konsole) einen Apache-Kafka-Auslöser hinzu

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen Ihrer Lambda-Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).
4. Führen Sie unter Auslöser-Konfiguration die folgenden Schritte aus:

    a. Wählen Sie den Apache-Kafka-Auslösertyp.

    b. Geben Sie für Bootstrap-Server die Host- und Portpaaradresse eines Kafka-Brokers in Ihrem Cluster ein und wählen Sie dann Hinzufügen. Wiederholen Sie den Vorgang für jeden Kafka-Broker im Cluster.

    c. Geben Sie für Themenname den Namen des Kafka-Themas ein, das zum Speichern von Datensätzen im Cluster verwendet wird.

    d. (Optional) Geben Sie für Batchgröße die maximale Anzahl von Datensätzen ein, die in einem einzelnen Batch empfangen werden sollen.

    e. Geben Sie für Batch window (Batch-Fenster) die maximale Zeit in Sekunden ein, die Lambda mit dem Sammeln von Datensätzen verbringt, bevor die Funktion aufgerufen wird.

f. (Optional) Geben Sie für Konsumentengruppen-ID die ID einer Kafka-Konsumentengruppe ein, der Sie beitreten möchten.

g. (Optional) Wählen Sie für Startposition die Option Neueste, um mit dem Lesen des Streams aus dem letzten Datensatz zu beginnen, Horizont trimmen, um mit dem frühesten verfügbaren Datensatz zu beginnen, oder Am Zeitstempel, um einen Zeitstempel anzugeben, ab dem mit dem Lesen begonnen werden soll.

h. (Optional) Wählen Sie bei VPC die Amazon VPC für Ihren Kafka-Cluster aus. Wählen Sie dann VPC subnets (VPC-Subnetze) und VPC security groups (VPC-Sicherheitsgruppen) aus.

   Diese Einstellung ist erforderlich, wenn nur Benutzer innerhalb Ihrer VPC auf Ihre Broker zugreifen.

i. (Optional) Wählen Sie bei Authentication (Authentifizierung) die Option Add (Hinzufügen) aus und gehen Sie dann folgendermaßen vor:

   i. Wählen Sie das Zugriffs- oder Authentifizierungsprotokoll der Kafka-Broker in Ihrem Cluster aus.

      - Wenn Ihr Kafka-Broker eine SASL/PLAIN-Authentifizierung verwendet, wählen Sie BASIC_AUTH.
      - Wenn Ihr Broker die SASL/SCRAM-Authentifizierung verwendet, wählen Sie eines der SASL_SCRAM-Protokolle aus.
      - Falls Sie die mTLS-Authentifizierung konfigurieren, wählen Sie das Protokoll CLIENT_CERTIFICATE_TLS_AUTH aus.

   ii. Wählen Sie für SASL/SCRAM- oder mTLS-Authentifizierung den Secrets-Manager-Geheimschlüssel aus, der die Anmeldeinformationen für Ihren Kafka-Cluster enthält.

j. (Optional) Wählen Sie bei Encryption (Verschlüsselung) das Secrets-Manager-Secret aus, das das Root-CA-Zertifikat enthält, das Ihre Kafka-Broker zur TLS-Verschlüsselung verwenden, falls Ihre Kafka-Broker von einer privaten Zertifizierungsstelle signierte Zertifikate verwenden.

   Diese Einstellung gilt für die TLS-Verschlüsselung für SASL/SCRAM oder SASL/PLAIN sowie für die mTLS-Authentifizierung.

k. Um den Auslöser zu Testzwecken in einem deaktivierten Zustand zu erstellen (empfohlen), deaktivieren Sie Auslöser aktivieren. Um den Auslöser sofort zu aktivieren, wählen Sie Auslöser aktivieren.

5. Wählen Sie hinzufügen aus, um den Auslöser zu erstellen.

Selbstverwaltetes Apache-Kafka-Cluster hinzufügen (AWS CLI)

Verwenden Sie die folgenden AWS CLI Beispielbefehle, um einen selbstverwalteten Apache Kafka-Trigger für Ihre Lambda-Funktion zu erstellen und anzuzeigen.

Verwenden von SASL/SCRAM

Wenn Kafka-Benutzer über das Internet auf Ihre Kafka-Broker zugreifen, geben Sie das Secrets-Manager-Secret an, das Sie für die SASL/SCRAM-Authentifizierung erstellt haben. Im folgenden Beispiel wird der `create-event-source-mapping` AWS CLI Befehl verwendet, um eine Lambda-Funktion mit dem Namen einem Kafka-Thema namens `my-kafka-function` zuzuordnen. `AWSKafkaTopic`

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration Type=SASL_SCRAM_512_AUTH,URI=arn:aws:secretsmanager:us-
east-1:111122223333:secret:MyBrokerSecretName \
  --function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Verwenden einer VPC

Wenn nur Kafka-Benutzer in Ihrer VPC auf Ihre Kafka-Broker zugreifen, müssen Sie Ihre VPC, Subnetze und VPC-Sicherheitsgruppe angeben. Im folgenden Beispiel wird der `create-event-source-mapping` AWS CLI Befehl verwendet, um eine Lambda-Funktion mit dem Namen einem Kafka-Thema namens `my-kafka-function` zuzuordnen. `AWSKafkaTopic`

```
aws lambda create-event-source-mapping \
  --topics AWSKafkaTopic \
  --source-access-configuration '[{"Type": "VPC_SUBNET", "URI":
 "subnet:subnet-0011001100"}, {"Type": "VPC_SUBNET", "URI":
 "subnet:subnet-0022002200"}, {"Type": "VPC_SECURITY_GROUP", "URI":
 "security_group:sg-0123456789"}]' \
  --function-name arn:aws:lambda:us-east-1:111122223333:function:my-kafka-function \
  --self-managed-event-source '{"Endpoints":{"KAFKA_BOOTSTRAP_SERVERS":
["abc3.xyz.com:9092", "abc2.xyz.com:9092"]}}'
```

Den Status mit dem anzeigen AWS CLI

Im folgenden Beispiel wird der `get-event-source-mapping` AWS CLI Befehl verwendet, um den Status der von Ihnen erstellten Ereignisquellenzuordnung zu beschreiben.

```
aws lambda get-event-source-mapping
          --uuid dh38738e-992b-343a-1077-3478934hjkfd7
```

Ausfallziele

Um Datensätze zu fehlgeschlagenen Aufrufen zur Zuordnung von Ereignisquellen beizubehalten, fügen Sie der Zuordnung von Ereignisquellen Ihrer Funktion ein Ziel hinzu. Jeder an das Ziel gesendete Datensatz ist ein JSON-Dokument mit Metadaten über den fehlgeschlagenen Aufruf. Sie können jedes Amazon SNS SNS-Thema, jede Amazon SQS SQS-Warteschlange oder jeden S3-Bucket als Ziel konfigurieren. Ihre Ausführungsrolle muss über Berechtigungen für das Ziel verfügen:

- Für SQS-Ziele: sqs: SendMessage
- Für SNS-Ziele: sns:Publish
- Für S3-Bucket-Ziele: s3: und s3: PutObject ListBuckets

Wenn Sie einen KMS-Schlüssel für Ihr Ziel konfiguriert haben, benötigt Lambda außerdem je nach Zieltyp folgende Berechtigungen:

- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für ein S3-Ziel aktiviert haben, ist kms: GenerateData Key erforderlich. Wenn sich der KMS-Schlüssel und das S3-Bucket-Ziel in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut, um kms: GenerateData Key zuzulassen.
- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für das SQS-Ziel aktiviert haben, sind kms:Decrypt und kms: Key erforderlich. GenerateData Wenn sich der KMS-Schlüssel und das SQS-Warteschlangenziel in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut, sodass kms:Decrypt, kms: GenerateData Key, kms: und kms: zugelassen werden. DescribeKey ReEncrypt
- Wenn Sie die Verschlüsselung mit Ihrem eigenen KMS-Schlüssel für das SNS-Ziel aktiviert haben, sind kms:Decrypt und kms: Key erforderlich. GenerateData Wenn sich der KMS-Schlüssel und das SNS-Themenziel in einem anderen Konto als Ihre Lambda-Funktion und Ausführungsrolle

befinden, konfigurieren Sie den KMS-Schlüssel so, dass er der Ausführungsrolle vertraut, sodass kms:Decrypt, kms: GenerateData Key, kms: und kms: zugelassen werden. DescribeKey ReEncrypt

Gehen Sie folgendermaßen vor, um ein Ausfallziel mit der Konsole zu konfigurieren:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add destination (Ziel hinzufügen).
4. Wählen Sie als Quelle die Option Aufruf der Zuordnung von Ereignisquellen aus.
5. Wählen Sie für die Zuordnung von Ereignisquellen eine Ereignisquelle aus, die für diese Funktion konfiguriert ist.
6. Wählen Sie für Bedingung die Option Bei Ausfall aus. Für Aufrufe zur Zuordnung von Ereignisquellen ist dies die einzig akzeptierte Bedingung.
7. Wählen Sie unter Zieltyp den Zieltyp aus, an den Lambda Aufrufdatensätze sendet.
8. Wählen Sie unter Destination (Ziel) eine Ressource aus.
9. Wählen Sie Save aus.

Sie können mit dem auch ein Ziel für den Fall eines Fehlers konfigurieren. AWS CLI Mit dem folgenden Befehl create-event-source-mapping wird beispielsweise eine Ereignisquellenzuordnung mit einem SQS-Ziel für den Fall eines Fehlers hinzugefügt: `MyFunction`

```
aws lambda create-event-source-mapping \
--function-name "MyFunction" \
--event-source-arn arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2 \
--destination-config '{"OnFailure": {"Destination": "arn:aws:sqs:us-
east-1:123456789012:dest-queue"}}'
```

Der folgende Befehl update-event-source-mapping fügt der mit der Eingabe verknüpften Ereignisquelle ein S3-Ziel für den Fall eines Fehlers hinzu: `uuid`

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": "arn:aws:s3:::dest-bucket"}}'
```

Um ein Ziel zu entfernen, geben Sie eine leere Zeichenfolge als Argument für den `destination-config`-Parameter an:

```
aws lambda update-event-source-mapping \
--uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
--destination-config '{"OnFailure": {"Destination": ""}}'
```

Beispielaufrufsdatensatz für SNS und SQS

Das folgende Beispiel zeigt, was Lambda bei einem fehlgeschlagenen Aufruf der Kafka-Ereignisquelle an ein SNS-Thema oder eine SQS-Warteschlange sendet. Jeder der Schlüssel unter `recordsInfo` enthält sowohl das Kafka-Thema als auch die Kafka-Partition, getrennt durch einen Bindestrich. Bei dem Schlüssel `"Topic-0"` handelt es sich beispielsweise bei `Topic` um das Kafka-Thema und bei `0` um die Partition. Für jedes Thema und jede Partition können Sie die Offsets und Zeitstempeldaten verwenden, um die ursprünglichen Aufrufdatensätze zu finden.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
```

```
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    }
}
```

Beispiel für einen S3-Zielaufrufdatensatz

Für S3-Ziele sendet Lambda den gesamten Aufrufdatensatz zusammen mit den Metadaten an das Ziel. Das folgende Beispiel zeigt, was Lambda bei einem fehlgeschlagenen Aufruf der Kafka-Ereignisquelle an ein S3-Bucket-Ziel sendet. Zusätzlich zu allen Feldern aus dem vorherigen Beispiel für SQS- und SNS-Ziele enthält das Feld `payload` den ursprünglichen Aufrufdatensatz als maskierte JSON-Zeichenfolge.

```
{
    "requestContext": {
        "requestId": "316aa6d0-8154-xmpl-9af7-85d5f4a6bc81",
        "functionArn": "arn:aws:lambda:us-east-1:123456789012:function:myfunction",
        "condition": "RetryAttemptsExhausted" | "MaximumPayloadSizeExceeded",
        "approximateInvokeCount": 1
    },
    "responseContext": { // null if record is MaximumPayloadSizeExceeded
        "statusCode": 200,
        "executedVersion": "$LATEST",
        "functionError": "Unhandled"
    },
    "version": "1.0",
    "timestamp": "2019-11-14T00:38:06.021Z",
    "KafkaBatchInfo": {
        "batchSize": 500,
        "eventSourceArn": "arn:aws:kafka:us-east-1:123456789012:cluster/
vpc-2priv-2pub/751d2973-a626-431c-9d4e-d7975eb44dd7-2",
        "bootstrapServers": "...",
        "payloadSize": 2039086, // In bytes
```

```
        "recordsInfo": {
            "Topic-0": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            },
            "Topic-1": {
                "firstRecordOffset":
 "49601189658422359378836298521827638475320189012309704722",
                "lastRecordOffset":
 "49601189658422359378836298522902373528957594348623495186",
                "firstRecordTimestamp": "2019-11-14T00:38:04.835Z",
                "lastRecordTimestamp": "2019-11-14T00:38:05.580Z",
            }
        }
    },
    "payload": "<Whole Event>" // Only available in S3
}
```

> **Tip**
>
> Wir empfehlen außerdem, die S3-Versionsverwaltung in Ihrem Ziel-Bucket zu aktivieren.

Verwenden eines Kafka-Clusters als Ereignisquelle

Wenn Sie Ihren Apache Kafka-Cluster als Auslöser für Ihre Lambda-Funktion hinzufügen, wird der Cluster als Ereignisquelle verwendet.

Lambda liest Ereignisdaten aus den Kafka-Themen, die Sie wie `Topics` in einer CreateEventSourceMappingAnfrage angeben, basierend auf den `StartingPosition` von Ihnen angegebenen Themen. Nach erfolgreicher Verarbeitung wird Ihr Kafka-Thema Ihrem Kafka-Cluster zugeordnet.

Wenn Sie die `StartingPosition` als `LATEST` angeben, beginnt Lambda mit dem Lesen der neuesten Nachricht in jeder zum Thema gehörenden Partition. Da es nach der Auslöserkonfiguration eine gewisse Verzögerung geben kann, bevor Lambda mit dem Lesen der Nachrichten beginnt, liest Lambda keine Nachrichten, die innerhalb dieses Zeitraums erzeugt wurden.

Lambda verarbeitet Datensätze von einer oder mehreren Kafka-Themenpartitionen, die Sie angeben, und sendet eine JSON-Nutzlast an Ihre Funktion. Wenn mehr Datensätze verfügbar sind, setzt Lambda die Verarbeitung von Datensätzen stapelweise fort, basierend auf dem `BatchSize` Wert, den Sie in einer CreateEventSourceMappingAnfrage angeben, bis Ihre Funktion das Thema eingeholt hat.

Wenn Ihre Funktion einen Fehler für eine der Nachrichten in einem Batch zurückgibt, wiederholt Lambda den gesamten Nachrichtenbatch, bis die Verarbeitung erfolgreich ist oder die Nachrichten ablaufen. Sie können Datensätze, bei denen alle Wiederholungsversuche fehlschlagen, zur späteren Verarbeitung an ein Ziel senden, wenn ein Fehler aufgetreten ist.

> **Note**
>
> Während Lambda-Funktionen in der Regel ein maximales Timeout-Limit von 15 Minuten haben, unterstützen Ereignisquellenzuordnungen für Amazon MSK, selbstverwaltetes Apache Kafka, Amazon DocumentDB, Amazon MQ für ActiveMQ und RabbitMQ nur Funktionen mit einem maximalen Timeout-Limit von 14 Minuten. Diese Einschränkung stellt sicher, dass die Ereignisquellenzuordnung Funktionsfehler und Wiederholungsversuche ordnungsgemäß verarbeiten kann.

Startpositionen für Abfragen und Streams

Beachten Sie, dass die Stream-Abfrage bei der Erstellung und Aktualisierung der Zuordnung von Ereignisquellen letztendlich konsistent ist.

- Bei der Erstellung der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis mit der Abfrage von Ereignissen aus dem Stream begonnen wird.
- Bei Aktualisierungen der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis die Abfrage von Ereignissen aus dem Stream gestoppt und neu gestartet wird.

Dieses Verhalten bedeutet, dass, wenn Sie `LATEST` als Startposition für den Stream angeben, die Zuordnung von Ereignisquellen bei der Erstellung oder Aktualisierung möglicherweise Ereignisse übersieht. Um sicherzustellen, dass keine Ereignisse übersehen werden, geben Sie die Startposition des Streams als `TRIM_HORIZON` oder `AT_TIMESTAMP` an.

Automatische Skalierung der Kafka-Ereignisquelle

Wenn Sie anfänglich eine Apache-Kafka-Ereignisquelle erstellen, weist Lambda einen Konsumenten zur Verarbeitung aller Partitionen im Kafka-Thema zu. Jeder Verbraucher hat mehrere Prozessoren, die parallel laufen, um erhöhte Workloads zu bewältigen. Lambda skaliert außerdem je nach Workload automatisch die Anzahl der Verbraucher nach oben oder unten. Um die Nachrichtenreihenfolge in jeder Partition beizubehalten, ist die maximale Anzahl von Verbrauchern pro Partition im Thema ein Verbraucher pro Partition.

In Intervallen von einer Minute wertet Lambda die Verbraucher-Offsetverzögerung aller Partitionen im Thema aus. Wenn die Verzögerung zu hoch ist, empfängt die Partition Nachrichten schneller als Lambda sie verarbeiten kann. Bei Bedarf fügt Lambda dem Thema Verbraucher hinzu oder entfernt sie. Der Skalierungsprozess zum Hinzufügen oder Entfernen von Verbrauchern erfolgt innerhalb von drei Minuten nach der Bewertung.

Wenn Ihre Lambda-Zielfunktion überlastet ist, verringert Lambda die Anzahl der Verbraucher. Diese Aktion reduziert die Workload für die Funktion, indem die Anzahl der Nachrichten reduziert wird, die Verbraucher abrufen und an die Funktion senden können.

Um den Durchsatz Ihres Kafka-Themas zu überwachen, können Sie die Apache Kafka-Verbrauchermetriken wie `consumer_lag` und `consumer_offset` anzeigen. Um zu überprüfen, wie viele Funktionsaufrufe parallel erfolgen, können Sie auch die Parallelitätsmetriken für Ihre Funktion überwachen.

Fehler bei der Ereignisquellen-Zuweisung

Wenn Sie Ihren Apache-Kafka-Cluster als Ereignisquelle für Ihre Lambda-Funktion hinzufügen und Ihre Funktion auf einen Fehler stößt, beendet Ihr Kafka-Verbraucher die Verarbeitung von Datensätzen. Verbraucher einer Themenpartition sind diejenigen, die Ihre Datensätze abonnieren, lesen und verarbeiten. Ihre anderen Kafka-Verbraucher können weiterhin Datensätze verarbeiten, sofern sie nicht auf denselben Fehler stoßen.

Um die Ursache eines gestoppten Verbrauchers zu ermitteln, überprüfen Sie das `StateTransitionReason`-Feld in der Antwort von `EventSourceMapping`. In der folgenden Liste werden die Ereignisquellfehler beschrieben, die Sie erhalten können:

`ESM_CONFIG_NOT_VALID`

Die Konfiguration der Ereignisquellenzuordnung ist ungültig.

`EVENT_SOURCE_AUTHN_ERROR`

Lambda konnte die Ereignisquelle nicht authentifizieren.

`EVENT_SOURCE_AUTHZ_ERROR`

Lambda verfügt nicht über die erforderlichen Berechtigungen für den Zugriff auf die Ereignisquelle.

`FUNCTION_CONFIG_NOT_VALID`

Die Konfiguration der Funktion ist ungültig.

> **Note**
>
> Wenn Ihre Lambda-Ereignisdatensätze die zulässige Größenbeschränkung von 6 MB überschreiten, können sie unbearbeitet bleiben.

CloudWatch Amazon-Metriken

Lambda gibt die Metrik `OffsetLag` aus, während Ihre Funktion Datensätze verarbeitet. Der Wert dieser Metrik ist die Differenz (der Versatz) zwischen dem letzten Datensatz, der ins Kafka-Ereignisquellen-Thema geschrieben wurde, und dem letzten Datensatz, den die Konsumentengruppe Ihrer Funktion verarbeitet hat. Sie können mit `OffsetLag` die Latenz zwischen dem Hinzufügen eines Datensatzes und der Verarbeitung des Datensatzes durch Ihre Konsumentengruppe abschätzen.

Ein zunehmender Trend in `OffsetLag` kann auf Probleme mit Pollern in der Konsumentengruppe Ihrer Funktion hinweisen. Weitere Informationen finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Selbstverwalteter Apache-Kafka-Konfigurationsparameter

Alle Lambda-Ereignisquelltypen verwenden dieselben CreateEventSourceMappingUpdateEventSourceMappingAPI-Operationen. Allerdings gelten nur einige der Parameter für Apache Kafka.

Ereignisquellparameter, die für selbstverwaltete Apache Kafka gelten

Parameter	Erforderlich	Standard	Hinweise
BatchSize	N	100	Höchstwert: 10 000.

Parameter	Erforderlich	Standard	Hinweise
Enabled	N	Aktiviert	
FunctionName	Y		
FilterCriteria	N		Lambda-Ereignisfilterung
MaximumBatchingWindowInSekunden	N	500 ms	Batching-Verhalten
SelfManagedEventSource	Y		Liste der Kafka Broker. Kann nur auf „Erstellen“ festgelegt werden
SelfManagedKafkaEventSourceConfig	N	Enthält das ConsumerGroupId Feld, das standardmäßig einen eindeutigen Wert hat.	Kann nur auf „Erstellen“ festgelegt werden
SourceAccessKonfigurationen	N	Keine Anmeldeinformationen	VPC-Informationen oder Authentifizierungsanmeldeinformationen für den Cluster Für SASL_PLAIN auf BASIC_AUTH setzen
StartingPosition	Y		AT_TIMESTAMP, TRIM_HORIZON, oder LATEST Kann nur auf „Erstellen“ festgelegt werden

Parameter	Erforderlich	Standard	Hinweise
StartingPositionZeitstempel	N		Erforderlich, wenn auf StartingPosition AT_TIMESTAMP gesetzt ist
Themen	Y		Topic-Name Kann nur auf „Erstellen“ festgelegt werden

Verwenden von Lambda mit Amazon SQS

> **Note**
>
> Wenn Sie Daten an ein anderes Ziel als eine Lambda-Funktion senden oder die Daten vor dem Senden anreichern möchten, finden Sie weitere Informationen unter Amazon EventBridge Pipes.

Mit einer Lambda-Funktion können Sie Nachrichten in einer Amazon-SQS-Warteschlange (Amazon Simple Queue Service) verarbeiten. Lambda unterstützt sowohl Standardwarteschlangen als auch First-In-First-Out-Warteschlangen(FIFO) für die Zuordnung von Ereignisquellen.

Grundlegendes zum Abruf- und Batching-Verhalten für Amazon SQS SQS-Ereignisquellenzuordnungen

Mit Amazon SQS SQS-Ereignisquellenzuordnungen fragt Lambda die Warteschlange ab und ruft Ihre Funktion synchron mit einem Ereignis auf. Jedes Ereignis kann einen Stapel mehrerer Nachrichten aus der Warteschlange enthalten. Lambda empfängt diese Ereignisse einen Batch nach dem anderen und ruft Ihre Funktion einmal für jeden Batch auf. Wenn Ihre Funktion einen Batch erfolgreich verarbeitet, löscht Lambda deren Nachrichten aus der Warteschlange.

Wenn Lambda einen Batch empfängt, bleiben die Nachrichten in der Warteschlange, werden aber für die Dauer des Sichtbarkeits-Timeouts der Warteschlange ausgeblendet. Wenn Ihre Funktion alle Nachrichten im Batch erfolgreich verarbeitet, löscht Lambda die Nachrichten aus der

Warteschlange. Wenn Ihre Funktion bei der Verarbeitung eines Batches auf einen Fehler stößt, werden standardmäßig alle Nachrichten in diesem Batch nach Ablauf des Sichtbarkeits-Timeouts wieder in der Warteschlange sichtbar. Deshalb muss der Funktionscode in der Lage sein, dieselbe Nachricht mehrmals ohne unbeabsichtigte Begleiterscheinungen zu verarbeiten.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Um zu verhindern, dass Lambda eine Nachricht mehrfach verarbeitet, können Sie entweder Ihre Ereignisquellenzuordnung so konfigurieren, dass Batch-Elementfehler in Ihre Funktionsantwort aufgenommen werden, oder Sie können die DeleteMessageAPI verwenden, um Nachrichten aus der Warteschlange zu entfernen, wenn Ihre Lambda-Funktion sie erfolgreich verarbeitet.

Weitere Informationen zu Konfigurationsparametern, die Lambda für SQS-Ereignisquellenzuordnungen unterstützt, finden Sie unter. the section called “Eine SQS-Ereignisquellenzuordnung erstellen”

Beispiel für ein Standard-Warteschlangen-Nachrichtenereignis

Example Amazon-SQS-Nachrichtenereignis (Standardwarteschlange)

```
{
    "Records": [
        {
            "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
            "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082649183",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082649185"
            },
            "messageAttributes": {},
```

```
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
            "awsRegion": "us-east-2"
        },
        {
            "messageId": "2e1424d4-f796-459a-8184-9c92662be6da",
            "receiptHandle": "AQEBzWwaftRI0KuVm4tP+/7q1rGgNqicHq...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082650636",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082650649"
            },
            "messageAttributes": {},
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
            "awsRegion": "us-east-2"
        }
    ]
}
```

Lambda fragt standardmäßig bis zu 10 Nachrichten in Ihrer Warteschlange sofort ab und sendet diesen Batch an die Funktion. Um zu vermeiden, dass die Funktion mit einer geringen Anzahl von Datensätzen aufgerufen wird, können Sie die Ereignisquelle so konfigurieren, dass Datensätze für bis zu 5 Minuten zwischengespeichert werden, indem Sie ein Batchfenster konfigurieren. Vor dem Aufrufen der Funktion fragt Lambda weiterhin Nachrichten aus der Standardwarteschlange ab, bis das Batchfenster abläuft, das Kontingent für die Größe der Aufruf-Nutzlast erreicht ist oder die konfigurierte maximale Batchgröße erreicht ist.

Wenn Sie ein Batch-Fenster verwenden und Ihre SQS-Warteschlange sehr wenig Datenverkehr enthält, wartet Lambda möglicherweise bis zu 20 Sekunden, bevor Sie Ihre Funktion aufruft. Dies gilt auch, wenn Sie ein Batch-Fenster unter 20 Sekunden festlegen.

> **Note**
>
> In Java können beim Deserialisieren von JSON Nullzeigerfehler auftreten. Dies könnte daran liegen, dass die Groß- und Kleinschreibung von „Records“ und „eventSourceARN“ vom JSON-Objektmapper konvertiert wird.

Beispiel für ein FIFO-Warteschlangen-Nachrichtenereignis

Bei FIFO-Warteschlangen enthalten Datensätze zusätzliche Attribute, die mit der Deduplizierung und Sequenzierung zusammenhängen.

Example Amazon-SQS-Nachrichtenereignis (FIFO-Warteschlange)

```
{
    "Records": [
        {
            "messageId": "11d6ee51-4cc7-4302-9e22-7cd8afdaadf5",
            "receiptHandle": "AQEBBX8nesZEXmkhsmZeyIE8iQAMig7qw...",
            "body": "Test message.",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1573251510774",
                "SequenceNumber": "18849496460467696128",
                "MessageGroupId": "1",
                "SenderId": "AIDAIO23YVJENQZJOL4VO",
                "MessageDeduplicationId": "1",
                "ApproximateFirstReceiveTimestamp": "1573251510774"
            },
            "messageAttributes": {},
            "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:fifo.fifo",
            "awsRegion": "us-east-2"
        }
    ]
}
```

Erstellen und Konfigurieren einer Amazon SQS SQS-Ereignisquellenzuordnung

Um Amazon SQS SQS-Nachrichten mit Lambda zu verarbeiten, konfigurieren Sie Ihre Warteschlange mit den entsprechenden Einstellungen und erstellen Sie dann eine Lambda-Ereignisquellenzuordnung.

Konfigurieren einer Warteschlange zur Verwendung mit Lambda

Wenn Sie noch keine Amazon SQS SQS-Warteschlange haben, erstellen Sie eine, die als Ereignisquelle für Ihre Lambda-Funktion dient. Konfigurieren Sie dann die Warteschlange so, dass Ihre Lambda-Funktion genügend Zeit hat, um jeden Ereignisstapel zu verarbeiten.

Damit Ihre Funktion Zeit hat, jeden Datensatz zu verarbeiten, setzen Sie das Sichtbarkeits-Timeout der Quell-Warteschlange auf mindestens das Sechsfache des Konfigurations-Timeouts für Ihre Funktion. Die zusätzliche Zeit ermöglicht es Lambda, es erneut zu versuchen, wenn Ihre Funktion während der Verarbeitung eines vorherigen Batches gedrosselt wird.

Wenn Lambda zu irgendeinem Zeitpunkt während der Verarbeitung eines Batches auf einen Fehler stößt, kehren standardmäßig alle Nachrichten in diesem Batch in die Warteschlange zurück. Nach dem Sichtbarkeits-Timeout werden die Nachrichten wieder für Lambda sichtbar. Sie können Ihre Ereignisquellenzuordnung so konfigurieren, dass nur die fehlgeschlagenen Nachrichten mit partiellen Batch-Antworten in die Warteschlange zurückgesendet werden. Wenn Ihre Funktion eine Nachricht mehrmals nicht verarbeiten kann, kann Amazon SQS sie außerdem an eine Warteschlange für unzustellbare Nachrichten senden. Wir empfehlen, die Redrive-Richtlinie in Ihrer Quellwarteschlange `maxReceiveCount` auf mindestens 5 festzulegen. Dies gibt Lambda einige Möglichkeiten, es erneut zu versuchen, bevor fehlgeschlagene Nachrichten direkt an die Warteschlange für unzustellbare Briefe gesendet werden.

Berechtigungen für Lambda-Ausführungsrollen einrichten

Die AWSLambdaSQSQueueExecutionRole AWS verwaltete Richtlinie umfasst die Berechtigungen, die Lambda benötigt, um aus Ihrer Amazon SQS SQS-Warteschlange zu lesen. Sie können diese verwaltete Richtlinie der Ausführungsrolle Ihrer Funktion hinzufügen.

Wenn Sie optional eine verschlüsselte Warteschlange verwenden, müssen Sie Ihrer Ausführungsrolle auch die folgende Berechtigung hinzufügen:

- kms:Decrypt

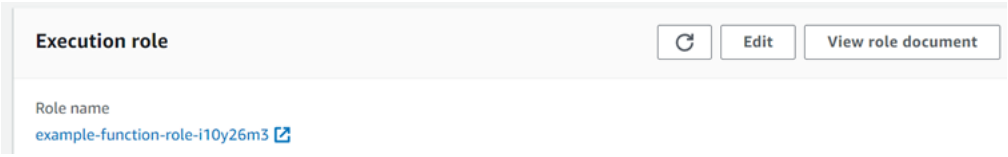
Eine SQS-Ereignisquellenzuordnung erstellen

Erstellen Sie ein Ereignisquellen-Mapping, um Lambda anzuweisen, Elemente aus Ihrer Warteschlange an eine Lambda-Funktion zu senden. Sie können mehrere Ereignisquellen-Zuweisungen zum Verarbeiten von Elementen aus mehreren Warteschlangen mit nur einer Funktion erstellen. Wenn Lambda die Zielfunktion aufruft, kann das Ereignis mehrere Elemente bis zu einer konfigurierbaren maximalen Batch-Größe enthalten.

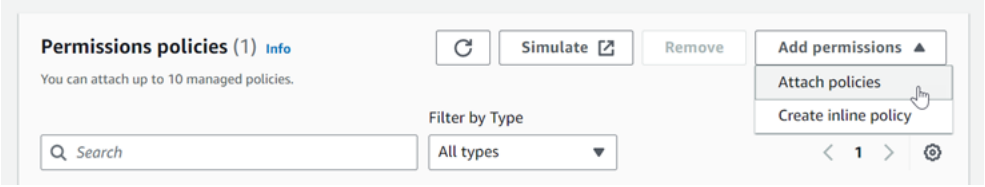
Um Ihre Funktion so zu konfigurieren, dass sie aus Amazon SQS liest, fügen Sie die AWSLambdaSQSQueueExecutionRole AWS verwaltete Richtlinie Ihrer Ausführungsrolle hinzu. Erstellen Sie dann mithilfe der folgenden Schritte von der Konsole aus eine Zuordnung der SQS-Ereignisquellen.

Um Berechtigungen hinzuzufügen und einen Trigger zu erstellen

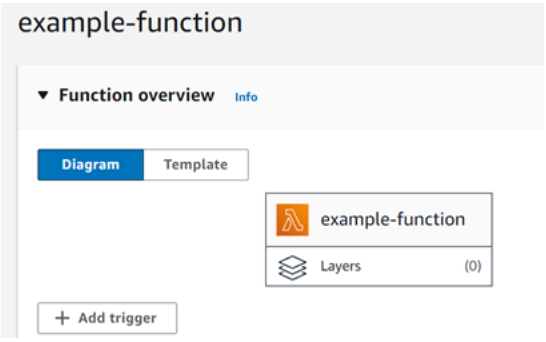
1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Berechtigungen aus.
4. Wählen Sie unter Rollenname den Link zu Ihrer Ausführungsrolle aus. Dieser Link öffnet die Rolle in der IAM-Konsole.



5. Wählen Sie Berechtigungen hinzufügen aus und wählen Sie dann Richtlinien direkt anhängen aus.



6. Geben Sie im Suchfeld `AWSLambdaSQSQueueExecutionRole` ein. Fügen Sie diese Richtlinie Ihrer Ausführungsrolle hinzu. Dies ist eine AWS verwaltete Richtlinie, die die Berechtigungen enthält, die Ihre Funktion zum Lesen aus einer Amazon SQS SQS-Warteschlange benötigt. Weitere Informationen zu dieser Richtlinie finden Sie AWSLambdaSQSQueueExecutionRolein der Referenz zu AWS verwalteten Richtlinien.
7. Kehren Sie zu Ihrer Funktion in der Lambda-Konsole zurück. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).



8. Wählen Sie einen Auslösertyp aus.
9. Konfigurieren Sie die erforderlichen Optionen und wählen Sie dann Add (Hinzufügen) aus.

Lambda unterstützt die folgenden Konfigurationsoptionen für Amazon SQS SQS-Ereignisquellen:

SQS Queue

Die Amazon-SQS-Warteschlange, aus der Datensätze gelesen werden sollen.

Aktivieren von Auslösern

Der Status der Zuordnung von Ereignisquellen. Enable trigger (Auslöser aktivieren) ist standardmäßig ausgewählt.

Batch-Größe

Die maximale Anzahl der Datensätze, die in jedem Stapel an die Funktion gesendet werden sollen. Bei einer Standardwarteschlange können dies bis zu 10.000 Datensätze sein. Bei einer FIFO-Warteschlange liegt der Höchstwert bei 10. Bei einer Stapelgröße über 10 müssen Sie das Stapelfenster (`MaximumBatchingWindowInSeconds`) zusätzlich auf mindestens 1 Sekunde festlegen.

Konfigurieren Sie Ihr Funktions-Timeout so, dass genügend Zeit für die Verarbeitung eines ganzen Stapels von Elementen zur Verfügung steht. Wenn die Verarbeitung bestimmter Elemente lange Zeit in Anspruch nimmt, wählen Sie eine kleinere Batch-Größe. Eine große Batchgröße kann die Effizienz für Workloads erhöhen, die sehr schnell sind oder viel Overhead aufweisen. Wenn Sie reservierte Nebenläufigkeit für Ihre Funktion konfigurieren, legen Sie mindestens fünf gleichzeitige Ausführungen fest, um das Risiko von Drosselungsfehlern zu senken, wenn Lambda die Funktion aufruft.

Lambda übergibt alle Datensätze im Batch in einem einzigen Aufruf an die Funktion, sofern die Gesamtgröße der Ereignisse das Kontingent für die Größe der Aufrufnutzlast für synchrone Aufrufe (6 MB) nicht überschreitet. Sowohl Lambda als auch Amazon SQS generieren Metadaten für jeden Datensatz. Diese zusätzlichen Metadaten werden auf die Gesamtnutzlastgröße angerechnet und können dazu führen, dass die Gesamtzahl der in einem Batch gesendeten Datensätze niedriger ist als die konfigurierte Batch-Größe. Die Metadatenfelder, die Amazon SQS sendet, können in der Länge variabel sein. Weitere Informationen zu den Amazon SQS-Metadatenfeldern finden Sie in der Dokumentation zum ReceiveMessageAPI-Betrieb in der Amazon Simple Queue Service API-Referenz.

Batchfenster

Die maximale Zeitspanne zur Erfassung von Datensätzen vor dem Aufruf der Funktion in Sekunden. Dies gilt nur für Standardwarteschlangen.

Wenn Sie ein Batchfenster von mehr als 0 Sekunden verwenden, müssen Sie die erhöhte Verarbeitungszeit im Sichtbarkeits-Timeout Ihrer Warteschlange berücksichtigen. Wir empfehlen, das Sichtbarkeits-Timeout Ihrer Warteschlange auf das Sechsfache Ihres Funktions-Timeouts plus den Wert von `MaximumBatchingWindowInSeconds` festzulegen. Dies gibt Ihrer Lambda-Funktion Zeit, jeden Ereignis-Batch zu verarbeiten und es im Falle eines Drosselungsfehlers erneut zu versuchen.

Wenn Nachrichten verfügbar werden, beginnt Lambda, Nachrichten stapelweise zu verarbeiten. Lambda beginnt mit der gleichzeitigen Verarbeitung von fünf Stapeln mit fünf gleichzeitigen Aufrufen Ihrer Funktion. Wenn weiterhin Nachrichten verfügbar sind, fügt Lambda Ihrer Funktion bis zu 300 weitere Instances pro Minute hinzu, bis zu einem Maximum von 1 000 Funktions-Instances. Informationen darüber, wie Gleichzeitigkeit mit der Skalierung interagiert, finden Sie unter Funktionsskalierung von Lambda.

Um mehr Nachrichten zu verarbeiten, können Sie Ihre Lambda-Funktion für einen höheren Durchsatz optimieren. Weitere Informationen finden Sie unter Grundlegendes zur AWS Lambda Skalierung mit Amazon SQS SQS-Standardwarteschlangen.

Maximale Gleichzeitigkeit

Die maximale Anzahl der gleichzeitigen Funktionen, die die Ereignisquelle aufrufen kann. Weitere Informationen finden Sie unter Konfigurieren der maximalen Gleichzeitigkeit für Amazon-SQS-Ereignisquellen.

Filterkriterien

Verwenden Sie Filterkriterien, um zu steuern, welche Ereignisse Lambda zur Verarbeitung an Ihre Funktion sendet. Weitere Informationen finden Sie unter Lambda-Ereignisfilterung.

Konfiguration des Skalierungsverhaltens für SQS-Ereignisquellenzuordnungen

Bei Standardwarteschlangen verwendet Lambda Long Polling, um eine Warteschlange abzufragen, bis sie aktiv wird. Wenn Nachrichten verfügbar sind, beginnt Lambda mit der gleichzeitigen Verarbeitung von fünf Stapeln mit fünf gleichzeitigen Aufrufen Ihrer Funktion. Wenn weiterhin Nachrichten verfügbar sind, erhöht Lambda die Anzahl der die Batches lesenden Prozesse um bis zu 300 weitere Instances pro Minute. Die maximale Anzahl von Batches, die eine Ereignisquellenzuordnung gleichzeitig verarbeiten kann, ist 1 000.

Bei FIFO-Warteschlangen sendet Lambda Nachrichten in der Reihenfolge, in der sie empfangen wurden, an Ihre Funktion. Wenn Sie eine Nachricht an eine FIFO-Warteschlange senden, geben Sie

eine Nachrichtengruppen-ID an. Amazon SQS stellt sicher, dass Nachrichten in derselben Gruppe in der Reihenfolge an Lambda übermittelt werden. Wenn Lambda Ihre Nachrichten in Batches liest, kann jeder Batch Nachrichten aus mehr als einer Nachrichtengruppe enthalten, aber die Reihenfolge der Nachrichten wird beibehalten. Wenn die Funktion einen Fehler zurückgibt, führt sie alle Wiederholungsversuche für die betroffenen Nachrichten aus, bevor Lambda weitere Nachrichten von derselben Gruppe erhält.

Konfigurieren der maximalen Gleichzeitigkeit für Amazon-SQS-Ereignisquellen

Sie können die Einstellung für maximale Parallelität verwenden, um das Skalierungsverhalten für Ihre SQS-Ereignisquellen zu steuern. Die Einstellung für die maximale Gleichzeitigkeit begrenzt die Anzahl der gleichzeitigen Instances der Funktion, die eine Amazon-SQS-Ereignisquelle aufrufen kann. Die maximale Gleichzeitigkeit ist eine Einstellung auf der Ebene der Ereignisquelle. Wenn Sie einer Funktion mehrere Amazon-SQS-Ereignisquellen zugeordnet haben, kann jede Ereignisquelle eine separate Einstellung für die maximale Gleichzeitigkeit haben. Sie können die maximale Parallelität verwenden, um zu verhindern, dass eine Warteschlange die gesamte reservierte Gleichzeitigkeit der Funktion oder den Rest des Gleichzeitigkeitskontingents des Kontos verwendet. Für die Konfiguration der maximalen Gleichzeitigkeit auf einer Amazon-SQS-Ereignisquelle fallen keine Gebühren an.

Wichtig ist, dass maximale und reservierte Parallelität zwei unabhängige Einstellungen sind. Setzen Sie die maximale Parallelität nicht höher als die reservierte Parallelität der Funktion. Wenn Sie maximale Parallelität konfigurieren, stellen Sie sicher, dass die reservierte Parallelität Ihrer Funktion größer oder gleich der gesamten maximalen Parallelität für alle Amazon SQS-Ereignisquellen auf der Funktion ist. Andernfalls könnte Lambda Ihre Nachrichten drosseln.

Wenn die maximale Parallelität nicht festgelegt ist, kann Lambda Ihre Amazon SQS-Ereignisquelle auf das Gesamtkontingent für Parallelität Ihres Kontos skalieren, das standardmäßig 1.000 beträgt.

> **Note**
>
> Bei FIFO-Warteschlangen sind gleichzeitige Aufrufe entweder durch die Anzahl der Nachrichtengruppen-IDs (`messageGroupId`) oder die maximale Gleichzeitigkeitseinstellung begrenzt, je nachdem, welcher Wert niedriger ist. Wenn Sie beispielsweise sechs Nachrichtengruppen-IDs haben und die maximale Gleichzeitigkeit auf 10 festgelegt ist, kann Ihre Funktion maximal sechs gleichzeitige Aufrufe haben.

Sie können die maximale Gleichzeitigkeit für neue und vorhandene Zuordnung von Ereignisquellen in Amazon SQS konfigurieren.

Konfigurieren der maximalen Gleichzeitigkeit mithilfe der Lambda-Konsole

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option SQS aus. Dadurch wird die Registerkarte Configuration (Konfiguration) geöffnet.
4. Wählen Sie den Amazon-SQS-Auslöser aus und klicken Sie auf Edit (Bearbeiten).
5. Geben Sie für Maximum concurrency (Maximale Gleichzeitigkeit) eine Zahl zwischen 2 und 1 000 ein. Um die maximale Gleichzeitigkeit zu deaktivieren, lassen Sie das Feld leer.
6. Wählen Sie Speichern.

Konfigurieren Sie die maximale Parallelität mit () AWS Command Line InterfaceAWS CLI

Verwenden Sie den update-event-source-mapping-Befehl mit der Option `--scaling-config`. Beispiel:

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --scaling-config '{"MaximumConcurrency":5}'
```

Um die maximale Gleichzeitigkeit zu deaktivieren, geben Sie einen leeren Wert für `--scaling-config` ein:

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --scaling-config "{}"
```

Konfigurieren der maximalen Gleichzeitigkeit mithilfe der Lambda-API

Verwenden Sie die UpdateEventSourceMappingAktion CreateEventSourceMappingoder mit einem ScalingConfigObjekt.

Behandlung von Fehlern für eine SQS-Ereignisquelle in Lambda

Um Fehler im Zusammenhang mit einer SQS-Ereignisquelle zu behandeln, verwendet Lambda automatisch eine Wiederholungsstrategie mit einer Backoff-Strategie. Sie können auch das Verhalten

bei der Fehlerbehandlung anpassen, indem Sie Ihre SQS-Ereignisquellenzuordnung so konfigurieren, dass teilweise Batch-Antworten zurückgegeben werden.

Backoff-Strategie für fehlgeschlagene Aufrufe

Wenn ein Aufruf fehlschlägt, versucht Lambda, den Aufruf zu wiederholen, während eine Backoff-Strategie implementiert wird. Die Backoff-Strategie unterscheidet sich geringfügig, je nachdem, ob Lambda den Fehler aufgrund eines Fehlers in Ihrem Funktionscode oder aufgrund einer Drosselung festgestellt hat.

- Wenn Ihr Funktionscode den Fehler verursacht hat, stoppt Lambda die Verarbeitung und versucht den Aufruf erneut. In der Zwischenzeit macht Lambda schrittweise einen Rückzieher und reduziert die Anzahl der Parallelität, die Ihrer Amazon SQS SQS-Ereignisquellenzuordnung zugewiesen ist. Wenn das Sichtbarkeits-Timeout Ihrer Warteschlange abgelaufen ist, erscheint die Nachricht wieder in der Warteschlange.
- Wenn der Aufruf aufgrund von Drosselung fehlschlägt, setzt Lambda schrittweise Wiederholungsversuche zurück, indem es die Menge der Gleichzeitigkeit reduziert, die Ihrer Zuordnung von Ereignisquellen in Amazon SQS zugewiesen ist. Lambda fährt fort, die Nachricht erneut zu versuchen, bis der Zeitstempel der Nachricht das Sichtbarkeits-Timeout Ihrer Warteschlange überschreitet, an welchem Punkt Lambda die Nachricht verwirft.

Implementierung von partiellen Batch-Antworten

Wenn die Lamda-Funktion während der Verarbeitung eines Batches auf einen Fehler stößt, werden standardmäßig alle Nachrichten in diesem Batch wieder in der Warteschlange sichtbar, einschließlich Nachrichten, die Lambda erfolgreich verarbeitet hat. Infolgedessen kann es passieren, dass die Funktion dieselbe Nachricht mehrmals verarbeitet.

Damit nicht erfolgreich bearbeiten Nachrichten in einem fehlgeschlagenen Batch erneut verarbeitet werden, können Sie die Zuordnung von Ereignisquellen so konfigurieren, dass nur die fehlgeschlagenen Nachrichten wieder sichtbar werden. Dies wird als partielle Batch-Antwort bezeichnet. Um partielle Batch-Antworten zu aktivieren, geben Sie dies bei der Konfiguration Ihrer Ereignisquellenzuordnung `ReportBatchItemFailures` für die Aktion FunctionResponseTypen an. Dadurch kann die Funktion einen Teilerfolg zurückgeben, was die Anzahl unnötiger Wiederholungsversuche für Datensätze reduzieren kann.

Wenn `ReportBatchItemFailures` aktiviert ist, skaliert Lambda die Nachrichtenabfrage nicht herunter, wenn Funktionsaufrufe fehlschlagen. Wenn Sie erwarten, dass einige Nachrichten ausfallen

– und Sie nicht möchten, dass sich diese Fehler auf die Nachrichtenverarbeitungsrate auswirken – verwenden Sie `ReportBatchItemFailures`.

> **Note**
>
> Berücksichtigen Sie bei Verwendung von partiellen Batch-Antworten Folgendes:
>
> - Wenn die Funktion eine Ausnahme ausgibt, gilt der gesamte Batch als fehlgeschlagen.
> - Wenn Sie dieses Feature mit einer FIFO-Warteschlange verwenden, sollte Ihre Funktion die Verarbeitung von Nachrichten nach dem ersten Fehler beenden und alle fehlgeschlagenen und nicht verarbeiteten Nachrichten in `batchItemFailures` zurückgeben. Das hilft, die Reihenfolge der Nachrichten in der Warteschlange beizubehalten.

So aktivieren Sie partielle Batchberichterstattung

1. Sehen Sie sich die bewährten Methoden für die Implementierung von partiellen Batch-Antworten an.
2. Führen Sie den folgenden Befehl aus, um `ReportBatchItemFailures` für Ihre Funktion zu aktivieren. Um die UUID Ihrer Ereignisquellenzuordnung abzurufen, führen Sie den Befehl AWS CLI list-event-source-mappings aus.

   ```
   aws lambda update-event-source-mapping \
   --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
   --function-response-types "ReportBatchItemFailures"
   ```

3. Aktualisieren Sie Ihren Funktionscode, um alle Ausnahmen abzufangen und fehlgeschlagene Nachrichten in einer `batchItemFailures`-JSON-Antwort zurückzugeben. Die `batchItemFailures`-Antwort muss eine Liste von Nachrichten-IDs als `itemIdentifier`-JSON-Werte enthalten.

   Angenommen, Sie haben einen Batch von fünf Nachrichten mit den Nachrichten-IDs `id1`, `id2`, `id3`, `id4` und `id5`. Die Funktion verarbeitet erfolgreich `id1`, `id3` und `id5`. Damit die Nachrichten `id2` und `id4` in der Warteschlange wieder sichtbar werden, sollte Ihre Funktion folgende Antwort zurückgeben:

   ```
   {
     "batchItemFailures": [
   ```

```
        {
            "itemIdentifier": "id2"
        },
        {
            "itemIdentifier": "id4"
        }
    ]
}
```

Hier sind einige Beispiele für Funktionscodes, die die Liste der fehlgeschlagenen Nachrichten-IDs im Batch zurückgeben:

.NET

AWS SDK for .NET

> **Note**
>
> Es GitHub gibt noch mehr dazu. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von SQS-Batchelementfehlern mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be
 converted into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
 ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 List<SQSBatchResponse.BatchItemFailure>();
```

```
        foreach(var message in evnt.Records)
        {
            try
            {
                //process your message
                await ProcessMessageAsync(message, context);
            }
            catch (System.Exception)
            {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.Add(new
 SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        if (String.IsNullOrEmpty(message.Body))
        {
            throw new Exception("No Body in SQS Message.");
        }
        context.Logger.LogInformation($"Processed message {message.Body}");
        // TODO: Do interesting work based on the new message
        await Task.CompletedTask;
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batch-Elementen mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "encoding/json"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, sqsEvent events.SQSEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, message := range sqsEvent.Records {

  if /* Your message processing condition here */ {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": message.MessageId})
  }
 }

 sqsBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return sqsBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;

import java.util.ArrayList;
import java.util.List;

public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,
 SQSBatchResponse> {
    @Override
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context)
 {

        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<SQSBatchResponse.BatchItemFailure>();
        String messageId = "";
        for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
            try {
                //process your message
                messageId = message.getMessageId();
            } catch (Exception e) {
                //Add failed message identifier to the batchItemFailures
 list
                batchItemFailures.add(new
 SQSBatchResponse.BatchItemFailure(messageId));
            }
```

```
        }
        return new SQSBatchResponse(batchItemFailures);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von SQS-Batch-Elementfehlern mit Lambda unter Verwendung von. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event, context) => {
    const batchItemFailures = [];

    for (const record of event.Records) {
        try {
            await processMessageAsync(record, context);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }

    return { batchItemFailures };
};

async function processMessageAsync(record, context) {
    if (record.body && record.body.includes("error")) {
        throw new Error("There is an error in the SQS Message.");
    }
    console.log(`Processed message: ${record.body}`);
}
```

Melden von SQS-Batch-Elementfehlern mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure,
 SQSRecord } from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
 Promise<SQSBatchResponse> => {
    const batchItemFailures: SQSBatchItemFailure[] = [];

    for (const record of event.Records) {
        try {
            await processMessageAsync(record);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }

    return {batchItemFailures: batchItemFailures};
};

async function processMessageAsync(record: SQSRecord): Promise<void> {
    if (record.body && record.body.includes("error")) {
        throw new Error('There is an error in the SQS Message.');
    }
    console.log(`Processed message ${record.body}`);
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batch-Elementen mit Lambda mithilfe von PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        $this->logger->info("Processing SQS records");
        $records = $event->getRecords();

        foreach ($records as $record) {
            try {
                // Assuming the SQS message is in JSON format
                $message = json_decode($record->getBody(), true);
                $this->logger->info(json_encode($message));
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $this->markAsFailed($record);
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords SQS
 records");
```

```
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event, context):
    if event:
        batch_item_failures = []
        sqs_batch_response = {}

        for record in event["Records"]:
            try:
                # process message
            except Exception as e:
                batch_item_failures.append({"itemIdentifier":
 record['messageId']})

        sqs_batch_response["batchItemFailures"] = batch_item_failures
        return sqs_batch_response
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
  if event
    batch_item_failures = []
    sqs_batch_response = {}

    event["Records"].each do |record|
      begin
        # process message
      rescue StandardError => e
        batch_item_failures << {"itemIdentifier" => record['messageId']}
      end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
    return sqs_batch_response
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}

async fn function_handler(event: LambdaEvent<SqsEvent>) ->
 Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }

    Ok(SqsBatchResponse {
        batch_item_failures,
    })
}
```

```
#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(function_handler)).await
}
```

Wenn die fehlgeschlagenen Ereignisse nicht in die Warteschlange zurückkehren, finden Sie weitere Informationen unter Wie behebe ich Probleme mit der Lambda-Funktion ReportBatchItemFailures SQS? im AWS Knowledge Center.

Erfolgs- und Misserfolgsbedingungen

Lambda behandelt einen Batch als komplett erfolgreich, wenn die Funktion eines der folgenden Elemente zurückgibt:

- Eine leere `batchItemFailures`-Liste
- Eine ungültige `batchItemFailures`-Liste
- Ein leeres `EventResponse`
- Ein ungültiges `EventResponse`

Lambda behandelt einen Batch als komplett fehlgeschlagen, wenn die Funktion eines der folgenden Elemente zurückgibt:

- Eine ungültige JSON-Antwort
- Eine leere Zeichenfolge `itemIdentifier`
- Ein ungültiges `itemIdentifier`
- Ein `itemIdentifier` mit einem falschen Schlüsselnamen
- Einen `itemIdentifier`-Wert mit einer Nachrichten-ID, die nicht existiert

CloudWatch Metriken

Um festzustellen, ob Ihre Funktion Fehler bei Chargenartikeln korrekt meldet, können Sie die Amazon SQS-Metriken `NumberOfMessagesDeleted` und die `ApproximateAgeOfOldestMessage` Amazon SQS-Metriken in Amazon CloudWatch überwachen.

- `NumberOfMessagesDeleted` verfolgt die Anzahl der Nachrichten, die aus der Warteschlange entfernt wurden. Wenn der Wert auf 0 sinkt, ist dies ein Zeichen dafür, dass die Funktionsantwort fehlgeschlagene Nachrichten nicht korrekt zurückgibt.
- `ApproximateAgeOfOldestMessage` verfolgt, wie lange die älteste Nachricht in der Warteschlange geblieben ist. Ein starker Anstieg dieser Metrik kann darauf hinweisen, dass die Funktion fehlgeschlagene Nachrichten nicht korrekt zurückgibt.

Lambda-Parameter für Amazon SQS SQS-Ereignisquellenzuordnungen

Alle Lambda-Ereignisquelltypen verwenden dieselben CreateEventSourceMappingUpdateEventSourceMappingAPI-Operationen. Allerdings gelten nur einige der Parameter für Amazon SQS.

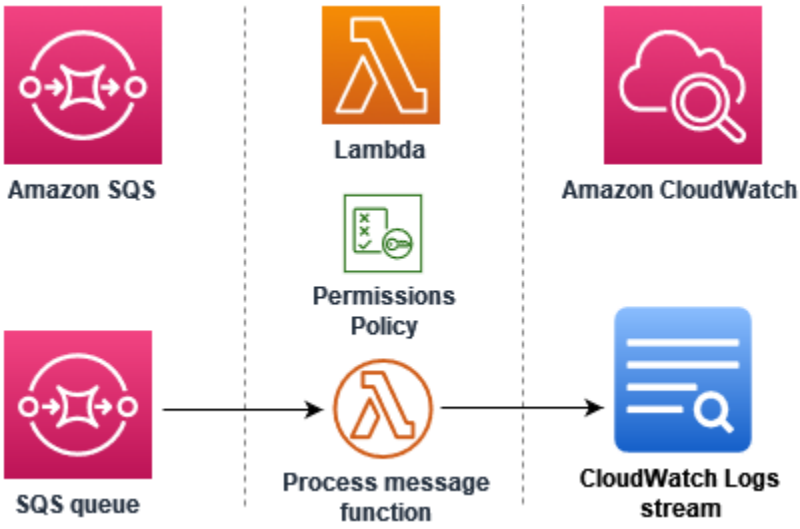
Ereignisquellparameter, die für Amazon SQS gelten

Parameter	Erforderlich	Standard	Hinweise
BatchSize	N	10	Bei Standardw arteschlangen beträgt der Maximalwert 10 000. Bei FIFO-Warteschlange n beträgt der Maximalwert 10.
Aktiviert	N	true	
EventSourceArn	Y		Der ARN des Datenstroms oder eines Stream-Ko nsumenten
FunctionName	Y		
FilterCriteria	N		Lambda-Ereignisfil terung
FunctionResponseTy pen	N		Damit Ihre Funktion bestimmte Fehler in

Parameter	Erforderlich	Standard	Hinweise
			einem Batch meldet, beziehen Sie den Wert `ReportBatchItemFailures` in `FunctionResponseTypes` ein. Weitere Informationen finden Sie unter Implementierung von partiellen Batch-Antworten.
MaximumBatchingWindowInSekunden	N	0	
ScalingConfig	N		Konfigurieren der maximalen Gleichzeitigkeit für Amazon-SQS-Ereignisquellen

Tutorial: Verwenden von Lambda mit Amazon SQS

In diesem Tutorial erstellen Sie eine Lambda-Funktion, die Nachrichten aus einer Warteschlange von Amazon Simple Queue Service (Amazon SQS) verarbeitet. Die Lambda-Funktion wird ausgeführt, wenn der Warteschlange eine neue Nachricht hinzugefügt wird. Die Funktion schreibt die Nachrichten in einen Amazon CloudWatch Logs-Stream. Das folgende Diagramm zeigt die AWS -Ressourcen, die Sie zur Durchführung des Tutorials verwenden.



Führen Sie für dieses Tutorial die folgenden Schritte aus:

1. Erstellen Sie eine Lambda-Funktion, die Nachrichten in CloudWatch Logs schreibt.
2. Erstellen einer Amazon SQS-Warteschlange
3. Erstellen Sie eine Zuordnung von Ereignisquellen in Lambda. Die Zuordnung von Ereignisquellen liest die Amazon-SQS-Warteschlange und ruft Ihre Lambda-Funktion auf, wenn eine neue Nachricht hinzugefügt wird.
4. Testen Sie das Setup, indem Sie Nachrichten zu Ihrer Warteschlange hinzufügen und die Ergebnisse in CloudWatch Logs überwachen.

Voraussetzungen

Melde dich an für eine AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

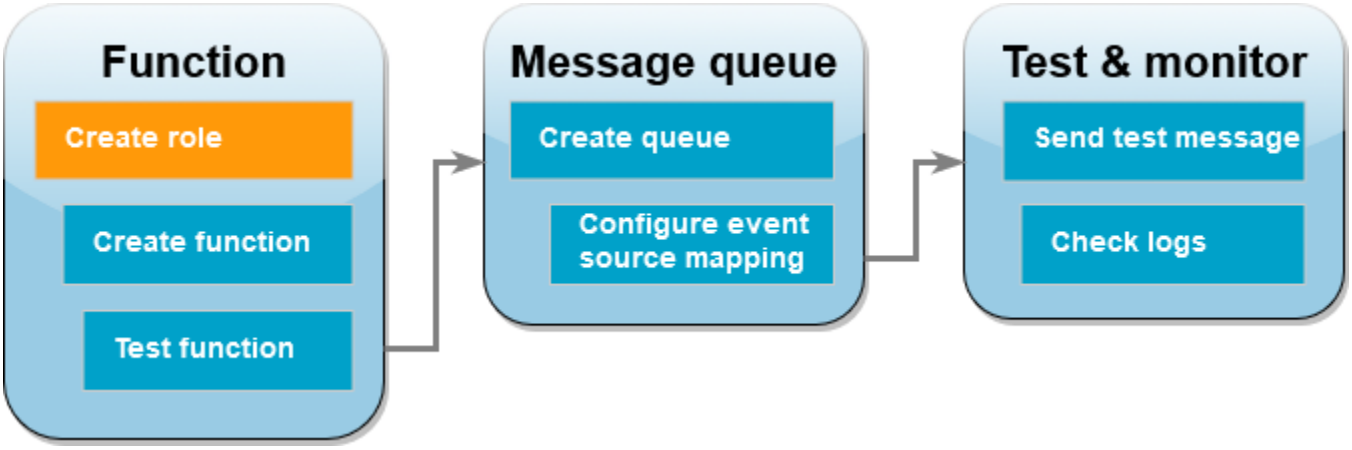
Installieren Sie das AWS Command Line Interface

Wenn Sie das noch nicht installiert haben AWS Command Line Interface, folgen Sie den Schritten unter Installieren oder Aktualisieren der neuesten Version von AWS CLI, um es zu installieren.

Das Tutorial erfordert zum Ausführen von Befehlen ein Befehlszeilenterminal oder eine Shell. Verwenden Sie unter Linux und macOS Ihre bevorzugte Shell und Ihren bevorzugten Paketmanager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux.

Erstellen der Ausführungsrolle



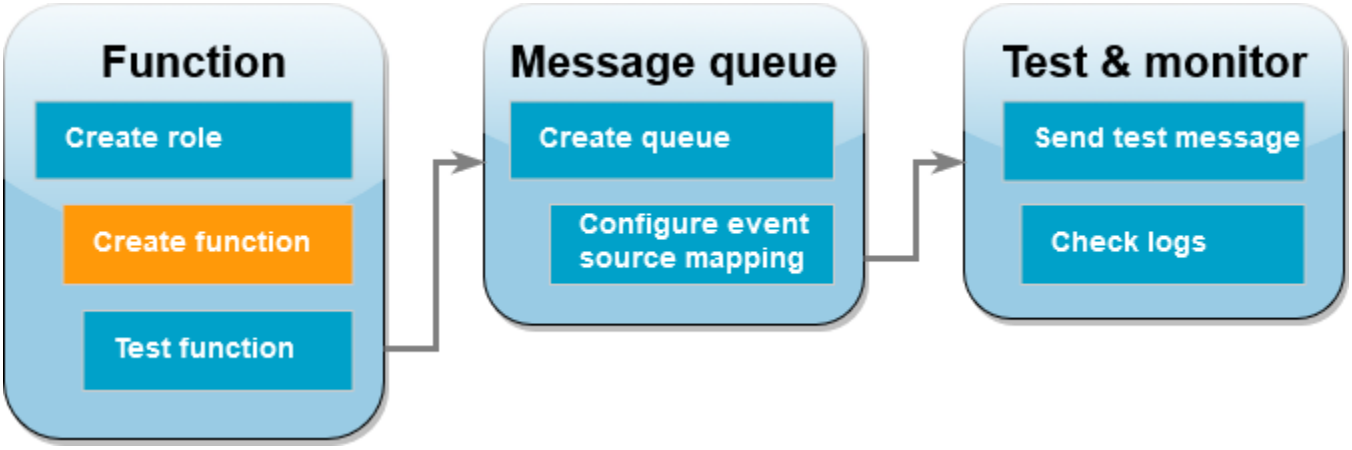
Eine Ausführungsrolle ist eine AWS Identity and Access Management (IAM-) Rolle, die einer Lambda-Funktion die Berechtigung zum Zugriff auf AWS Dienste und Ressourcen gewährt. Damit Ihre Funktion Elemente aus Amazon SQS lesen kann, fügen Sie die AWSLambdaSQSQueueExecutionRoleBerechtigungsrichtlinie bei.

So erstellen Sie eine Ausführungsrolle und fügen eine Amazon-SQS-Berechtigungsrichtlinie hinzu

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
4. Wählen Sie unter Anwendungsfall die Option Lambda aus.
5. Wählen Sie Weiter aus.
6. Geben Sie im Suchfeld Berechtigungsrichtlinien die Zeichenfolge **`AWSLambdaSQSQueueExecutionRole`** ein.
7. Wählen Sie die AWSLambdaSQSQueueExecutionRoleRichtlinie aus und klicken Sie dann auf Weiter.
8. Geben Sie unter Rollendetails für Rollenname den Namen **`lambda-sqs-role`** ein und wählen Sie anschließend Rolle erstellen aus.

Schreiben Sie sich nach der Erstellung der Rolle den Amazon-Ressourcennamen (ARN) Ihrer Ausführungsrolle auf. Sie werden ihn in späteren Schritten noch benötigen.

Erstellen der Funktion



Erstellen Sie eine Lambda-Funktion, die Ihre Amazon-SQS-Nachrichten verarbeitet. Der Funktionscode protokolliert den Hauptteil der Amazon SQS-Nachricht in CloudWatch Logs.

In diesem Tutorial wird die Node.js 18.x-Laufzeit verwendet. Es stehen aber auch Beispielcodes für andere Laufzeitensprachen zur Verfügung. Sie können die Registerkarte im folgenden Feld auswählen, um Code für die gewünschte Laufzeit anzusehen. Der JavaScript Code, den Sie in diesem Schritt verwenden, befindet sich im ersten Beispiel, das auf der JavaScriptRegisterkarte angezeigt wird.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }

    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
 for _, record := range event.Records {
  err := processMessage(record)
  if err != nil {
   return err
  }
 }
 fmt.Println("done")
 return nil
}

func processMessage(record events.SQSMessage) error {
 fmt.Printf("Processed message %s\n", record.Body)
 // TODO: Do interesting work based on the new message
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
            throw e;
        }
```

```
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines SQS-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message) {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Konsumieren eines SQS-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";
```

```
export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein SQS-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
```

```
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].each do |message|
    process_message(message)
  end
  puts "done"
end

def process_message(message)
  begin
    puts "Processed message #{message['body']}"
    # TODO: Do interesting work based on the new message
```

```
  rescue StandardError => err
    puts "An error occurred"
    raise err
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein SQS-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
    event.payload.records.iter().for_each(|record| {
        // process the record
        tracing::info!("Message body: {}",
 record.body.as_deref().unwrap_or_default())
    });

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
```

```
        .init();

    run(service_fn(function_handler)).await
}
```

So erstellen Sie eine Node.js-Lambda-Funktion

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir sqs-tutorial
cd sqs-tutorial
```

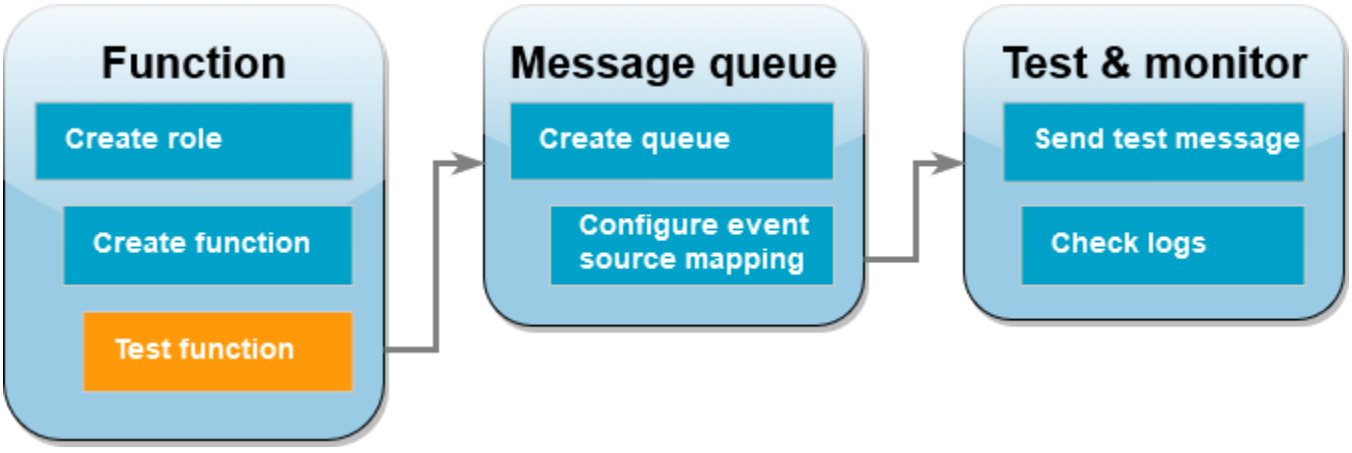
2. Kopieren Sie den JavaScript Beispielcode in eine neue Datei mit dem Namen. `index.js`
3. Erstellen Sie ein Bereitstellungspaket mit dem folgenden `zip`-Befehl.

```
zip function.zip index.js
```

4. Erstellen Sie eine Lambda-Funktion mithilfe des AWS CLI -Befehls create-function. Geben Sie für den `role`-Parameter den ARN der Ausführungsrolle ein, die Sie zuvor erstellt haben.

```
aws lambda create-function --function-name ProcessSQSRecord \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
--role arn:aws:iam::111122223333:role/lambda-sqs-role
```

Testen der Funktion



Rufen Sie Ihre Lambda-Funktion manuell mit dem `invoke` AWS CLI Befehl und einem Amazon SQS SQS-Beispielereignis auf.

So rufen Sie die Lambda-Funktion mit einem Beispielereignis auf

1. Speichern Sie die folgende JSON als Datei mit dem Namen `input.json`. Dieser JSON-Code simuliert ein Ereignis, das so ggf. von Amazon SQS an Ihre Lambda-Funktion gesendet wird, wobei `"body"` die tatsächliche Nachricht aus der Warteschlange enthält. In diesem Beispiel lautet die Nachricht `"test"`.

   Example Amazon-SQS-Ereignis

   Dies ist ein Testereignis. Nachricht und Kontonummer müssen nicht geändert werden.

   ```
   {
       "Records": [
           {
               "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
               "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
               "body": "test",
               "attributes": {
                   "ApproximateReceiveCount": "1",
                   "SentTimestamp": "1545082649183",
                   "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                   "ApproximateFirstReceiveTimestamp": "1545082649185"
               },
               "messageAttributes": {},
               "md5OfBody": "098f6bcd4621d373cade4e832627b4f6",
               "eventSource": "aws:sqs",
               "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:my-queue",
               "awsRegion": "us-east-1"
           }
       ]
   }
   ```

2. Führen Sie den folgenden Invoke-Befehl aus. AWS CLI Dieser Befehl gibt CloudWatch Logs in der Antwort zurück. Weitere Informationen über das Abrufen von Protokollen finden Sie unter Zugreifen auf Protokolle mit dem AWS CLI.

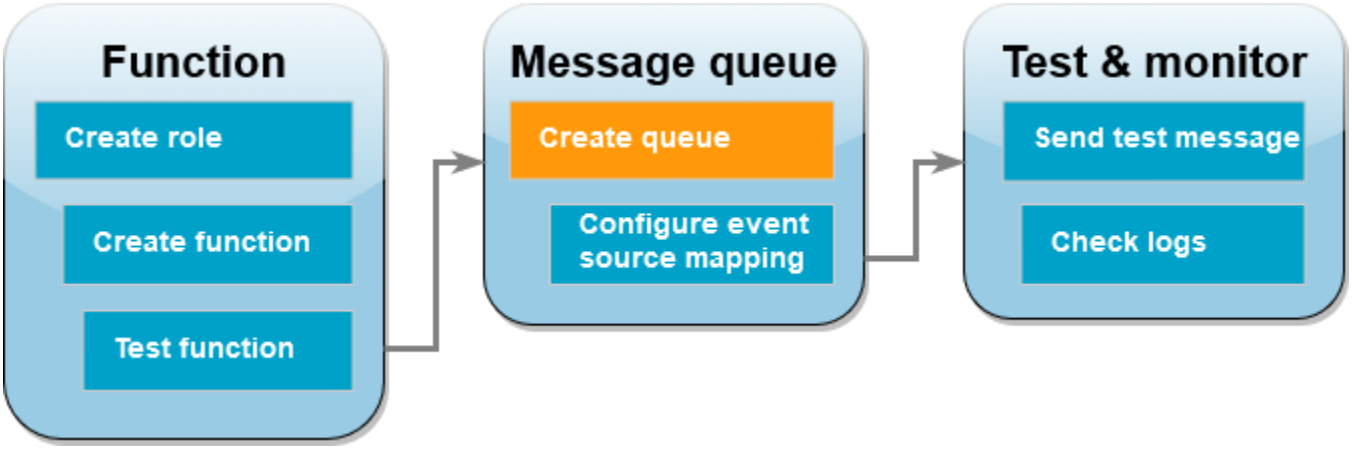
   ```
   aws lambda invoke --function-name ProcessSQSRecord --payload file://input.json out
    --log-type Tail \
   --query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
   decode
   ```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

3. Suchen Sie in der Antwort nach dem Protokoll `INFO`. Dort protokolliert die Lambda-Funktion den Nachrichtentext. Sie sollten Protokolle sehen, die wie folgt aussehen:

```
2023-09-11T22:45:04.271Z 348529ce-2211-4222-9099-59d07d837b60 INFO Processed
 message test
2023-09-11T22:45:04.288Z 348529ce-2211-4222-9099-59d07d837b60 INFO done
```

Erstellen einer Amazon-SQS-Warteschlange



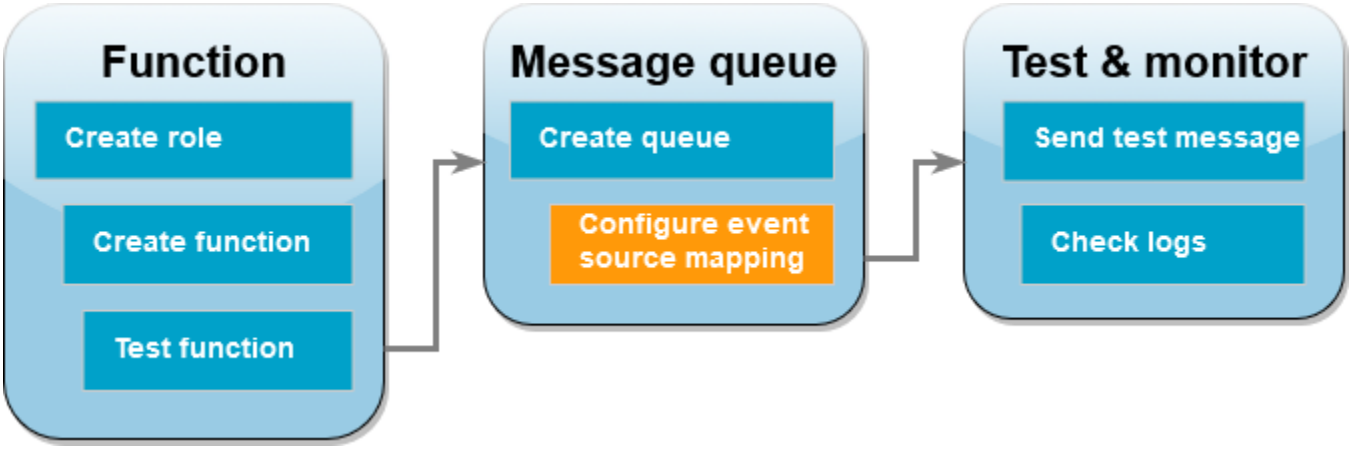
Erstellen Sie eine Amazon-SQS-Warteschlange, die die Lambda-Funktion als Ereignisquelle verwenden kann.

So erstellen Sie eine Warteschlange

1. Öffnen Sie die Amazon-SQS-Konsole.
2. Wählen Sie Create queue (Warteschlange erstellen) aus.
3. Geben Sie einen Namen für die Warteschlange ein. Übernehmen Sie bei allen anderen Optionen die Standardeinstellungen.
4. Wählen Sie Create queue (Warteschlange erstellen) aus.

Notieren Sie sich nach dem Erstellen der Warteschlange ihren ARN. Sie benötigen ihn im nächsten Schritt, um die Warteschlange Ihrer Lambda-Funktion zuzuordnen.

Konfigurieren der Ereignisquelle



Verbinden Sie die Amazon-SQS-Warteschlange mit Ihrer Lambda-Funktion, indem Sie eine Zuordnung von Ereignisquellen erstellen. Die Zuordnung von Ereignisquellen liest die Amazon-SQS-Warteschlange und ruft Ihre Lambda-Funktion auf, wenn eine neue Nachricht hinzugefügt wird.

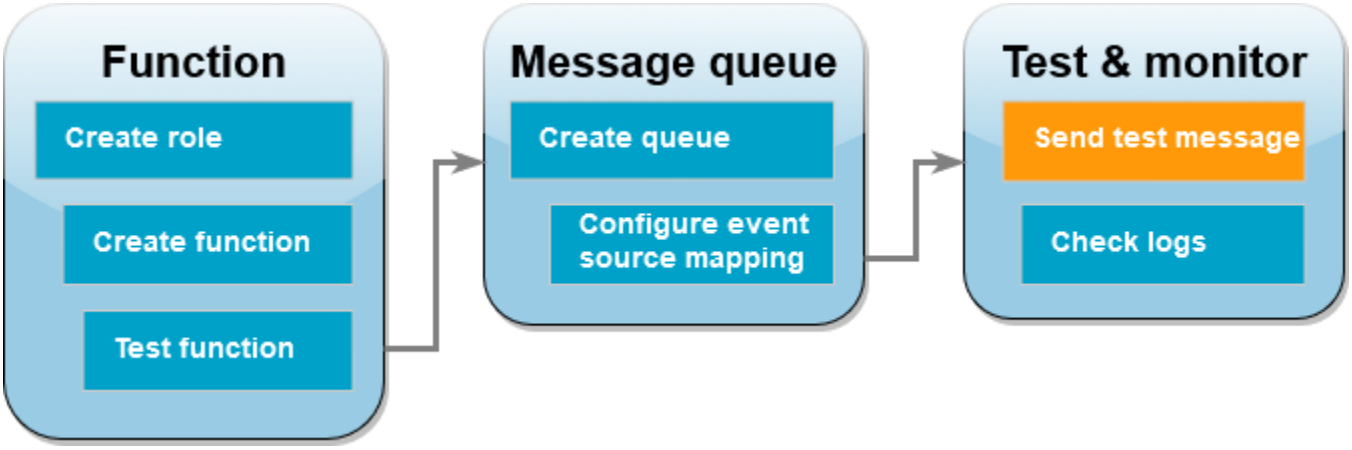
Verwenden Sie den Befehl, um eine Zuordnung zwischen Ihrer Amazon SQS SQS-Warteschlange und Ihrer Lambda-Funktion zu erstellen. create-event-source-mapping AWS CLI Beispiel:

```
aws lambda create-event-source-mapping --function-name ProcessSQSRecord  --batch-size
 10 \
--event-source-arn arn:aws:sqs:us-east-1:111122223333:my-queue
```

Verwenden Sie den Befehl, um eine Liste Ihrer Ereignisquellenzuordnungen abzurufen. list-event-source-mappings Beispiel:

```
aws lambda list-event-source-mappings --function-name ProcessSQSRecord
```

Senden einer Testnachricht

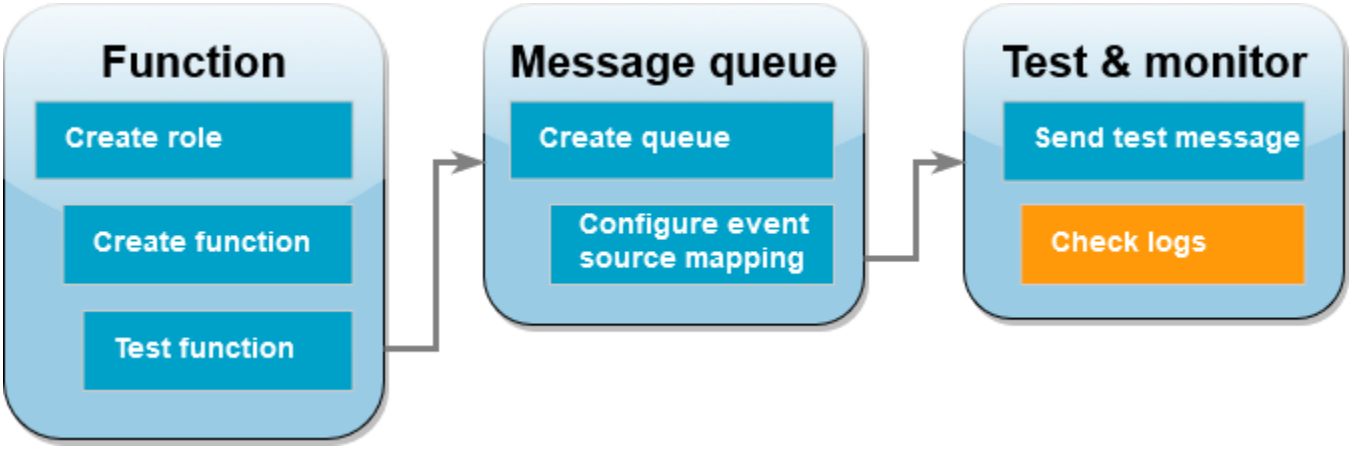


So senden Sie eine Amazon-SQS-Nachricht an die Lambda-Funktion

1. Öffnen Sie die Amazon-SQS-Konsole.
2. Wählen Sie die Warteschlange aus, die Sie zuvor erstellt haben.
3. Wählen Sie Nachrichten senden und empfangen.
4. Geben Sie unter Nachrichtentext eine Testnachricht ein (z. B. „Dies ist eine Testnachricht.“).
5. Klicken Sie auf Send Message (Nachricht senden).

Lambda fragt die Warteschlange nach Aktualisierungen ab. Wenn eine neue Nachricht vorliegt, ruft Lambda Ihre Funktion mit diesen neuen Ereignisdaten aus der Warteschlange auf. Wenn der Funktions-Handler ohne Ausnahmen zurückgegeben wird, betrachtet Lambda die Nachricht als erfolgreich verarbeitet und beginnt mit dem Lesen neuer Nachrichten in der Warteschlange. Nach erfolgreicher Verarbeitung einer Nachricht löscht Lambda diese automatisch aus der Warteschlange. Wenn der Handler eine Ausnahme auslöst, betrachtet Lambda den Nachrichten-Batch als nicht erfolgreich verarbeitet und Lambda ruft die Funktion mit demselben Nachrichten-Batch auf.

Überprüfen Sie die Protokolle CloudWatch



So vergewissern Sie sich, dass die Funktion die Nachricht verarbeitet hat

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion ProcessSQSRecord aus.
3. Wählen Sie Überwachen aus.
4. Wählen Sie CloudWatch Protokolle anzeigen.
5. Wählen Sie in der CloudWatch Konsole den Protokollstream für die Funktion aus.
6. Suchen Sie das Protokoll `INFO`. Dort protokolliert die Lambda-Funktion den Nachrichtentext. Sie sollten die Nachricht sehen, die Sie über die Amazon-SQS-Warteschlange gesendet haben. Beispiel:

```
2023-09-11T22:49:12.730Z b0c41e9c-0556-5a8b-af83-43e59efeec71 INFO Processed
 message this is a test message.
```

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.

4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Amazon-SQS-Warteschlange

1. Melden Sie sich bei der Amazon SQS SQS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/sqs/.
2. Wählen Sie die Warteschlange aus, die Sie erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie **`confirm`** in das Texteingabefeld ein.
5. Wählen Sie Löschen.

Tutorial: Verwenden einer kontoübergreifenden Amazon SQS SQS-Warteschlange als Ereignisquelle

In diesem Tutorial erstellen Sie eine Lambda-Funktion, die Nachrichten aus einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange in einem anderen Konto verarbeitet. AWS Dieses Tutorial umfasst zwei AWS Konten: Konto A bezieht sich auf das Konto, das Ihre Lambda-Funktion enthält, und Konto B bezieht sich auf das Konto, das die Amazon SQS SQS-Warteschlange enthält.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen der Ausführungsrolle (Konto A)

Erstellen Sie in Konto A eine Ausführungsrolle, die Ihrer Funktion die Erlaubnis erteilt, auf die erforderlichen AWS Ressourcen zuzugreifen.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Rollen in der AWS Identity and Access Management (IAM-) Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.
   - Vertrauenswürdige Entität – AWS Lambda.
   - Berechtigungen — AWSLambdaSQSQueueExecutionRole
   - Role name (Name der Rolle – **`cross-account-lambda-sqs-role`**

Die AWSLambdaSQSQueueExecutionRoleRichtlinie verfügt über die Berechtigungen, die die Funktion zum Lesen von Elementen aus Amazon SQS und zum Schreiben von Protokollen in Amazon CloudWatch Logs benötigt.

Erstellen Sie die Funktion (Account A)

Erstellen Sie in Konto A eine Lambda-Funktion, die Ihre Amazon SQS-Nachrichten verarbeitet. Das folgende Codebeispiel für Node.js 18 schreibt jede Nachricht in ein Protokoll in CloudWatch Logs.

Example index.mjs

```
export const handler = async function(event, context) {
  event.Records.forEach(record => {
    const { body } = record;
    console.log(body);
  });
  return {};
}
```

So erstellen Sie die Funktion

> **Note**
>
> Mit diesen Schritten wird eine Funktion in Node.js 18 erstellt. Für andere Sprachen sind die Schritte ähnlich, aber einige Details unterscheiden sich.

1. Speichern Sie das Codebeispiel als Datei mit dem Namen `index.mjs`.
2. Erstellen Sie ein Bereitstellungspaket.

   ```
   zip function.zip index.mjs
   ```

3. Erstellen Sie die Funktion mit dem Befehl `create-function` AWS Command Line Interface (AWS CLI).

   ```
   aws lambda create-function --function-name CrossAccountSQSExample \
   --zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
   --role arn:aws:iam::<AccountA_ID>:role/cross-account-lambda-sqs-role
   ```

Testen Sie die Funktion (Konto A)

Testen Sie in Konto A Ihre Lambda-Funktion manuell mithilfe des `invoke` AWS CLI Befehls und eines Amazon SQS SQS-Beispielereignisses.

Wenn der Handler normal und ohne Ausnahmen zurückkehrt, betrachtet Lambda die Nachricht als erfolgreich verarbeitet und beginnt mit dem Lesen neuer Nachrichten in der Warteschlange. Nach erfolgreicher Verarbeitung einer Nachricht löscht Lambda diese automatisch aus der Warteschlange. Wenn der Handler eine Ausnahme auslöst, betrachtet Lambda den Nachrichten-Batch als nicht erfolgreich verarbeitet und Lambda ruft die Funktion mit demselben Nachrichten-Batch auf.

1. Speichern Sie die folgende JSON als Datei mit dem Namen `input.txt`.

```
{
    "Records": [
        {
            "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
            "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
            "body": "test",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1545082649183",
                "SenderId": "AIDAIENQZJOLO23YVJ4VO",
                "ApproximateFirstReceiveTimestamp": "1545082649185"
            },
            "messageAttributes": {},
            "md5OfBody": "098f6bcd4621d373cade4e832627b4f6",
            "eventSource": "aws:sqs",
            "eventSourceARN": "arn:aws:sqs:us-east-1:111122223333:example-queue",
            "awsRegion": "us-east-1"
        }
    ]
}
```

   Das vorangehende JSON simuliert ein Ereignis, das Amazon SQS an Ihre Lambda-Funktion senden könnte, wobei `"body"` die tatsächliche Nachricht aus der Warteschlange enthält.

2. Führen Sie den Befehl `invoke` AWS CLI aus.

```
aws lambda invoke --function-name CrossAccountSQSExample \
--cli-binary-format raw-in-base64-out \
--payload file://input.txt outputfile.txt
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

3. Überprüfen Sie die Ausgabe in der Datei `outputfile.txt`.

Erstellen einer Amazon SQS-Warteschlange (Konto B)

Erstellen Sie in Konto B eine Amazon SQS-Warteschlange, die die Lambda-Funktion in Konto A als Ereignisquelle verwenden kann.

So erstellen Sie eine Warteschlange

1. Öffnen Sie die Amazon-SQS-Konsole.
2. Wählen Sie Create queue (Warteschlange erstellen) aus.
3. Erstellen Sie eine Warteschlange mit den folgenden Eigenschaften.
   - Typ – Standard
   - Name — LambdaCrossAccountQueue
   - Konfiguration – Behalten Sie die Standardeinstellungen bei.
   - Zugriffsrichtlinie – Wählen Sie Advanced (Erweitert). Fügen Sie die folgende JSON-Richtlinie ein:

```
{
   "Version": "2012-10-17",
   "Id": "Queue1_Policy_UUID",
   "Statement": [{
      "Sid":"Queue1_AllActions",
      "Effect": "Allow",
      "Principal": {
         "AWS": [
            "arn:aws:iam::<AccountA_ID>:role/cross-account-lambda-sqs-role"
         ]
      },
      "Action": "sqs:*",
      "Resource": "arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue"
    }
```

```
  ]
}
```

Diese Richtlinie gewährt der Lambda-Ausführungsrolle in Konto A Berechtigungen zur Nutzung von Nachrichten aus dieser Amazon-SQS-Warteschlange.

4. Zeichnen Sie nach dem Erstellen der Warteschlange ihren Amazon-Ressourcennamen (ARN) auf. Sie benötigen ihn im nächsten Schritt, um die Warteschlange Ihrer Lambda-Funktion zuzuordnen.

Konfigurieren Sie die Ereignisquelle (Konto A)

Erstellen Sie in Konto A eine Ereignisquellenzuordnung zwischen der Amazon SQS SQS-Warteschlange in Konto B und Ihrer Lambda-Funktion, indem Sie den folgenden `create-event-source-mapping` AWS CLI Befehl ausführen.

```
aws lambda create-event-source-mapping --function-name CrossAccountSQSExample --batch-size 10 \
--event-source-arn arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue
```

Führen Sie den folgenden Befehl aus, um eine Liste Ihrer Ereignisquellen-Zuweisung abzurufen.

```
aws lambda list-event-source-mappings --function-name CrossAccountSQSExample \
--event-source-arn arn:aws:sqs:us-east-1:<AccountB_ID>:LambdaCrossAccountQueue
```

Testen der Einrichtung

Sie können die Einrichtung nun wie folgt testen:

1. In Konto B öffnen Sie die Amazon-SQS-Konsole.
2. Wählen Sie LambdaCrossAccountQueue, was Sie zuvor erstellt haben.
3. Wählen Sie Nachrichten senden und empfangen.
4. Geben Sie unter Nachrichtentext eine Testnachricht ein.
5. Klicken Sie auf Send Message (Nachricht senden).

Ihre Lambda-FunktionKonto Asollte die Nachricht erhalten. Lambda wird die Warteschlange weiterhin nach Updates abfragen. Wenn eine neue Nachricht vorliegt, ruft Lambda Ihre Funktion mit diesen

neuen Ereignisdaten aus der Warteschlange auf. Ihre Funktion wird in Amazon ausgeführt und erstellt Protokolle CloudWatch. Sie können die Protokolle in der CloudWatch Konsole einsehen.

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

In :Konto ABereinigen Sie Ihre Ausführungsrolle und Lambda-Funktion.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

In :Konto BBereinigen Sie die Amazon SQS SQS-Warteschlange.

So löschen Sie die Amazon-SQS-Warteschlange

1. Melden Sie sich bei der Amazon SQS SQS-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/sqs/.
2. Wählen Sie die Warteschlange aus, die Sie erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie **`confirm`** in das Texteingabefeld ein.
5. Wählen Sie Löschen.

Amazon DocumentDB DocumentDB-Ereignisse mit Lambda verarbeiten

Sie können eine Lambda-Funktion verwenden, um Ereignisse in einem Änderungsstream von Amazon DocumentDB (mit MongoDB-Kompatibilität) zu verarbeiten, indem Sie einen Amazon-DocumentDB-Cluster als Ereignisquelle konfigurieren. Anschließend können Sie ereignisgesteuerte Workloads automatisieren, indem Sie Ihre Lambda-Funktion jedes Mal aufrufen, wenn sich Daten in Ihrem Amazon-DocumentDB-Cluster ändern.

> **Note**
>
> Lambda unterstützt nur die Versionen 4.0 und 5.0 von Amazon DocumentDB. Lambda unterstützt Version 3.6 nicht.
> Für die Zuordnung von Ereignisquellen unterstützt Lambda außerdem nur Instance-basierte Cluster und regionale Cluster. Lambda unterstützt keine elastischen Cluster oder globalen Cluster. Diese Einschränkung gilt nicht, wenn Lambda als Client verwendet wird, um eine Verbindung mit Amazon DocumentDB herzustellen. Lambda kann eine Verbindung mit allen Clustertypen herstellen, um CRUD-Vorgänge auszuführen.

Lambda verarbeitet Ereignisse aus Amazon-DocumentDB-Änderungsstreams sequentiell in der Reihenfolge, in der sie ankommen. Aus diesem Grund kann Ihre Funktion jeweils nur einen Aufruf von DocumentDB gleichzeitig verarbeiten. Sie können Ihre Funktion anhand ihrer Gleichzeitigkeitsmetriken überwachen.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Themen

- Erstellen einer Zuordnung von Ereignisquellen von Amazon DocumentDB (Konsole)
- Erstellen einer Zuordnung von Ereignisquellen von Amazon DocumentDB (SDK oder CLI)
- Startpositionen für Abfragen und Streams
- Überwachen Ihrer Amazon-DocumentDB-Ereignisquelle
- Tutorial: Verwendung AWS Lambda mit Amazon DocumentDB DocumentDB-Streams

Beispiel für Amazon-DocumentDB-Ereignis


```
{
    "eventSourceArn": "arn:aws:rds:us-
east-1:123456789012:cluster:canaryclusterb2a659a2-qo5tcmqkcl03",
    "events": [
        {
            "event": {
                "_id": {
                    "_data": "0163eeb6e7000000090100000009000041e1"
                },
                "clusterTime": {
                    "$timestamp": {
                        "t": 1676588775,
                        "i": 9
                    }
                },
                "documentKey": {
                    "_id": {
                        "$oid": "63eeb6e7d418cd98afb1c1d7"
                    }
                },
                "fullDocument": {
                    "_id": {
                        "$oid": "63eeb6e7d418cd98afb1c1d7"
                    },
                    "anyField": "sampleValue"
                },
                "ns": {
                    "db": "test_database",
                    "coll": "test_collection"
                },
                "operationType": "insert"
            }
        }
```

```
    ],
    "eventSource": "aws:docdb"
}
```

Weitere Informationen zu den Ereignissen in diesem Beispiel und den zugehörigen Formen finden Sie unter Änderungsereignisse auf der MongoDB-Dokumentationswebsite.

Voraussetzungen und Berechtigungen

Bevor Sie Amazon DocumentDB als Ereignisquelle für Ihre Lambda-Funktion verwenden können, beachten Sie die folgenden Voraussetzungen. Folgendes muss zutreffen:

- Haben Sie einen vorhandenen Amazon DocumentDB-Cluster in derselben AWS-Konto und AWS-Region wie Ihre Funktion. Wenn Sie über keinen bestehenden Cluster verfügen, können Sie anhand der Anleitung in Erste Schritte mit Amazon DocumentDB im Amazon-DocumentDB-Entwicklerhandbuch einen erstellen. Alternativ dazu führen Sie die ersten Schritte in Tutorial: Verwendung AWS Lambda mit Amazon DocumentDB DocumentDB-Streams durch die Erstellung eines DocumentDB-Clusters mit allen erforderlichen Voraussetzungen.
- Sie müssen Lambda den Zugriff auf die Ressourcen von Amazon Virtual Private Cloud (Amazon VPC) erlauben, die Ihrem Amazon-DocumentDB-Cluster zugeordnet sind. Weitere Informationen finden Sie unter Netzwerkkonfiguration.
- Aktivieren Sie TLS in Ihrem Amazon-DocumentDB-Cluster. Dies ist die Standardeinstellung. Wenn Sie TLS deaktivieren, kann Lambda nicht mit Ihrem Cluster kommunizieren.
- Aktivieren Sie Änderungsstreams in Ihrem Amazon-DocumentDB-Cluster. Weitere Informationen finden Sie unter Verwenden von Änderungsstreams mit Amazon DocumentDB im Amazon-DocumentDB-Entwicklerhandbuch.
- Stellen Sie Lambda Anmeldeinformationen für den Zugriff auf Ihren Amazon-DocumentDB-Cluster zur Verfügung. Geben Sie bei der Einrichtung der Ereignisquelle den AWS Secrets Manager-Schlüssel mit den Authentifizierungsdetails (Benutzername und Passwort) an, die für den Zugriff auf Ihren Cluster erforderlich sind. Um diesen Schlüssel während der Einrichtung bereitzustellen, haben Sie die folgenden Möglichkeiten:
  - Wenn Sie die Lambda-Konsole für die Einrichtung verwenden, geben Sie diesen Schlüssel in das Feld Secrets-Manager-Schlüssel ein.
  - Wenn Sie AWS Command Line Interface (AWS CLI) für die Einrichtung verwenden, geben Sie diesen Schlüssel in der `source-access-configurations` Option an. Sie können diese Option entweder in den `create-event-source-mapping`-Befehl oder in den `update-event-source-mapping`-Befehl einschließen. Beispielsweise:

```
aws lambda create-event-source-mapping \
    ...
    --source-access-configurations
 '[{"Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-
west-2:123456789012:secret:DocDBSecret-AbC4E6"}]' \
    ...
```

- Sie müssen Lambda Berechtigungen zur Verwaltung von Ressourcen gewähren, die zu Ihrem Amazon-DocumentDB-Stream gehören. Fügen Sie der zu der Ausführungsrolle Ihrer Funktion manuell die folgenden Berechtigungen hinzu:
  - rds:DescribeDBClusters
  - rds: DescribeDB ClusterParameters
  - rds: DescribeDB SubnetGroups
  - ec2: Schnittstelle CreateNetwork
  - ec2: Schnittstellen DescribeNetwork
  - ec2: DescribeVpcs
  - ec2: Schnittstelle DeleteNetwork
  - ec2: DescribeSubnets
  - ec2: Gruppen DescribeSecurity
  - kms:Decrypt
  - secretsmanager: Wert GetSecret
- Halten Sie die Größe der Amazon-DocumentDB-Änderungsstream-Ereignisse, die Sie an Lambda senden, bei unter 6 MB. Lambda unterstützt Nutzlasten mit einer Größe von bis zu 6 MB. Wenn Ihr Änderungsstream versucht, Lambda ein Ereignis zu senden, das größer als 6 MB ist, löscht Lambda die Nachricht und gibt die `OversizedRecordCount`-Metrik aus. Lambda gibt alle Metriken auf die bestmögliche Weise aus.

> **Note**
>
> Während Lambda-Funktionen in der Regel ein maximales Timeout-Limit von 15 Minuten haben, unterstützen Ereignisquellenzuordnungen für Amazon MSK, selbstverwaltetes Apache Kafka, Amazon DocumentDB, Amazon MQ für ActiveMQ und RabbitMQ nur Funktionen mit einem maximalen Timeout-Limit von 14 Minuten. Diese Einschränkung stellt sicher, dass

die Ereignisquellenzuordnung Funktionsfehler und Wiederholungsversuche ordnungsgemäß verarbeiten kann.

Netzwerkkonfiguration

Damit Lambda Ihren Amazon DocumentDB-Cluster als Ereignisquelle verwenden kann, benötigt es Zugriff auf die Amazon VPC, in der sich Ihr Cluster befindet. Wir empfehlen, dass Sie AWS PrivateLink VPC-Endpunkte für Lambda bereitstellen, um auf Ihre VPC zuzugreifen. Stellen Sie einen VPC-Endpunkt für Lambda bereit und, falls der Cluster Authentifizierung verwendet, auch einen VPC-Endpunkt für Secrets Manager.

Oder stellen Sie sicher, dass die VPC, die Ihrem Amazon-DocumentDB-Cluster zugeordnet ist, ein NAT-Gateway pro öffentliches Subnetz enthält. Weitere Informationen finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Wenn Sie VPC-Endpunkte verwenden, müssen Sie sie auch so konfigurieren, dass private DNS-Namen aktiviert werden.

Wenn Sie eine Ereignisquellenzuordnung für einen Amazon DocumentDB-Cluster erstellen, prüft Lambda, ob Elastic Network Interfaces (ENIs) bereits für die Subnetze und Sicherheitsgruppen der VPC Ihres Clusters vorhanden sind. Wenn Lambda vorhandene ENIs findet, versucht es, sie wiederzuverwenden. Andernfalls erstellt Lambda neue ENIs, um eine Verbindung zur Ereignisquelle herzustellen und Ihre Funktion aufzurufen.

> **Note**
>
> Lambda-Funktionen werden immer in VPCs ausgeführt, die dem Lambda-Service gehören. Diese VPCs werden automatisch vom Service verwaltet und sind für Kunden nicht sichtbar. Sie können Ihre Funktion auch mit einer Amazon VPC verbinden. In beiden Fällen hat die VPC-Konfiguration Ihrer Funktion keinen Einfluss auf die Zuordnung der Ereignisquelle. Nur die Konfiguration der VPC der Ereignisquelle bestimmt, wie Lambda eine Verbindung zu Ihrer Ereignisquelle herstellt.

VPC-Sicherheitsgruppenregeln

Konfigurieren Sie die Sicherheitsgruppen für die Amazon VPC, die Ihren Cluster enthält, mit den folgenden Regeln (mindestens):

- Regeln für eingehenden Datenverkehr — Erlauben Sie den gesamten Datenverkehr auf dem Amazon DocumentDB-Cluster-Port für die Sicherheitsgruppen, die für Ihre Ereignisquelle angegeben sind. Amazon DocumentDB verwendet standardmäßig Port 27017.
- Ausgehende Regeln - Erlauben Sie allen Datenverkehr auf Port 443 für alle Ziele. Lassen Sie den gesamten Verkehr auf dem Amazon DocumentDB-Cluster-Port zu. Amazon DocumentDB verwendet standardmäßig Port 27017.
- Wenn Sie VPC-Endpunkte anstelle eines NAT-Gateways verwenden, müssen die Sicherheitsgruppen, die mit den VPC-Endpunkten verknüpft sind, den gesamten eingehenden Datenverkehr für Port 443 von den Sicherheitsgruppen der Ereignisquelle zulassen.

Arbeiten mit VPC-Endpunkten

Wenn Sie VPC-Endpunkte verwenden, werden API-Aufrufe zum Aufrufen Ihrer Funktion mithilfe der ENIs über diese Endpunkte geleitet. Der Lambda-Serviceprinzipal muss alle Funktionen aufrufen`lambda:InvokeFunction`, die diese ENIs verwenden.

Standardmäßig haben VPC-Endpoints offene IAM-Richtlinien. Es hat sich bewährt, diese Richtlinien so einzuschränken, dass nur bestimmte Prinzipale die erforderlichen Aktionen über diesen Endpunkt ausführen können. Um sicherzustellen, dass Ihre Ereignisquellenzuordnung Ihre Lambda-Funktion aufrufen kann, muss die VPC-Endpunktrichtlinie den Aufruf des Lambda-Serviceprinzips zulassen. `lambda:InvokeFunction` Wenn Sie Ihre VPC-Endpunktrichtlinien so einschränken, dass sie nur API-Aufrufe zulassen, die ihren Ursprung in Ihrer Organisation haben, verhindert, dass die Zuordnung der Ereignisquellen ordnungsgemäß funktioniert.

Die folgenden VPC-Endpunktrichtlinien zeigen, wie der erforderliche Zugriff für Lambda-Endpunkte gewährt wird.

Example VPC-Endpunktrichtlinie — Lambda-Endpunkt

```
{
    "Statement": [
        {
            "Action": "lambda:InvokeFunction",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "lambda.amazonaws.com"
                ]
            },
```

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

Wenn Ihr Amazon DocumentDB-Cluster Authentifizierung verwendet, können Sie auch die VPC-Endpunktrichtlinie für den Secrets Manager Manager-Endpunkt einschränken. Um die Secrets Manager Manager-API aufzurufen, verwendet Lambda Ihre Funktionsrolle, nicht den Lambda-Serviceprinzipal. Das folgende Beispiel zeigt eine Secrets Manager Manager-Endpunktrichtlinie.

Example VPC-Endpunktrichtlinie — Secrets Manager Manager-Endpunkt

```
{
    "Statement": [
        {
            "Action": "secretsmanager:GetSecretValue",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "customer_function_execution_role_arn"
                ]
            },
            "Resource": "customer_secret_arn"
        }
    ]
}
```

Erstellen einer Zuordnung von Ereignisquellen von Amazon DocumentDB (Konsole)

Erstellen Sie für eine Funktion zum Lesen aus dem Änderungsstream eines Amazon-DocumentDB-Clusters eine Zuordnung von Ereignisquellen. In diesem Abschnitt wird die entsprechende Vorgehensweise über die Lambda-Konsole beschrieben. AWS SDK und AWS CLI Anweisungen finden Sie unterthe section called “Erstellen einer Zuordnung von Ereignisquellen von Amazon DocumentDB (SDK oder CLI)”.

So erstellen Sie eine Zuordnung von Ereignisquellen von Amazon DocumentDB (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).

4. Wählen Sie unter Auslöserkonfiguration in der Dropdown-Liste die Option DocumentDB aus.
5. Konfigurieren Sie die erforderlichen Optionen und wählen Sie dann Add (Hinzufügen) aus.

Lambda unterstützt die folgenden Optionen für Amazon-DocumentDB-Ereignisquellen:

- DocumentDB-Cluster – Wählen Sie einen Amazon-DocumentDB-Cluster aus.
- Auslöser aktivieren – Wählen Sie aus, ob Sie den Auslöser sofort aktivieren möchten. Wenn Sie dieses Kontrollkästchen aktivieren, beginnt Ihre Funktion sofort, Datenverkehr aus dem angegebenen Amazon-DocumentDB-Änderungsstream zu empfangen, sobald die Zuordnung von Ereignisquellen erstellt wurde. Wir empfehlen, das Kontrollkästchen zu deaktivieren, um die Zuordnung von Ereignisquellen zu Testzwecken in einem deaktivierten Zustand zu erstellen. Nach der Erstellung können Sie die Zuordnung von Ereignisquellen jederzeit aktivieren.
- Datenbankname – Geben Sie den Namen einer Datenbank innerhalb des Clusters ein, die verwendet werden soll.
- (Optional) Sammlungsname – Geben Sie den Namen einer Sammlung in der Datenbank ein, die verwendet werden soll. Wenn Sie keine Sammlung angeben, hört Lambda auf alle Ereignisse aus jeder Sammlung in der Datenbank.
- Batchgröße – Legen Sie die maximale Anzahl von Nachrichten fest, die in einem einzelnen Batch abgerufen werden sollen bis zu 10 000. Die Standardgröße beträgt 100.
- Startposition – Wählen Sie die Position im Stream aus, von der aus das Lesen von Datensätzen beginnen.
  - Neueste – Verarbeiten Sie Datensätze, die neu zum Stream hinzugefügt wurden. Ihre Funktion beginnt erst mit der Verarbeitung von Datensätzen, nachdem Lambda die Erstellung Ihrer Ereignisquelle abgeschlossen hat. Das bedeutet, dass einige Datensätze gelöscht werden können, bis Ihre Ereignisquelle erfolgreich erstellt wurde.
  - Horizont trimmen – Verarbeiten Sie alle Datensätze im Stream. Lambda verwendet die Protokollspeicherdauer Ihres Clusters, um zu bestimmen, ab wo mit dem Lesen von Ereignissen begonnen werden soll. Insbesondere beginnt Lambda mit dem Lesen von `current_time - log_retention_duration`. Ihr Änderungsstream muss bereits vor diesem Zeitstempel aktiv sein, damit Lambda alle Ereignisse korrekt lesen kann.
  - Am Zeitstempel – Verarbeiten Sie Datensätze ab einem bestimmten Zeitpunkt. Ihr Änderungsstream muss bereits vor dem angegebenen Zeitstempel aktiv sein, damit Lambda alle Ereignisse korrekt lesen kann.

- Authentifizierung – Wählen Sie unter Authentifizierungsmethode den Zugriff auf den Broker in Ihrem Cluster aus.
  - BASIC_AUTH – Bei der Standardauthentifizierung müssen Sie den Secrets-Manager-Schlüssel angeben, der die Anmeldeinformationen für den Zugriff auf Ihren Cluster enthält.
- Secrets-Manager-Schlüssel – Wählen Sie den Secrets-Manager-Schlüssel aus, der die Authentifizierungsdetails (Benutzername und Passwort) enthält, die für den Zugriff auf Ihren Amazon-DocumentDB-Cluster erforderlich sind.
- (Optional) Batch-Fenster – Legen Sie die maximale Zeitspanne zur Erfassung von Datensätzen vor dem Aufruf der Funktion in Sekunden fest (bis zu 300).
- (Optional) Vollständige Dokumentkonfiguration – Wählen Sie für Dokumentaktualisierungsvorgänge aus, was Sie an den Stream senden möchten. Der Standardwert ist `Default`, was bedeutet, dass Amazon DocumentDB für jedes Änderungsstream-Ereignis nur ein Delta sendet, das die vorgenommenen Änderungen beschreibt. Weitere Informationen zu diesem Feld finden Sie FullDocumentin der MongoDB Javadoc-API-Dokumentation.
  - Standard – Lambda sendet nur ein Teildokument, das die vorgenommenen Änderungen beschreibt.
  - UpdateLookup— Lambda sendet ein Delta, das die Änderungen beschreibt, zusammen mit einer Kopie des gesamten Dokuments.

Erstellen einer Zuordnung von Ereignisquellen von Amazon DocumentDB (SDK oder CLI)

Um eine Zuordnung von Ereignisquellen von Amazon DocumentDB mit einem AWS SDK zu verwalten, können Sie die folgenden API-Operationen verwenden:

- CreateEventSourceMapping
- ListEventSourceMappings
- GetEventSourceMapping
- UpdateEventSourceMapping
- DeleteEventSourceMapping

Verwenden Sie den `create-event-source-mapping`Befehl, um die Zuordnung der AWS CLI Ereignisquelle mit dem zu erstellen. Im folgenden Beispiel wird dieser Befehl verwendet, um eine Funktion namens `my-function` einem Amazon-DocumentDB-Änderungsstream zuzuordnen. Der

Ereignisquelle wird mit dem Amazon-Ressourcennamen (ARN) angegeben, mit einer Batchgröße von 500, beginnend ab dem Zeitstempel in Unix-Zeit. Der Befehl gibt auch den Secrets-Manager-Schlüssel an, den Lambda verwendet, um eine Verbindung zu Amazon DocumentDB herzustellen. Darüber hinaus enthält er `document-db-event-source-config`-Parameter, die die Datenbank und die Sammlung angeben, aus der gelesen werden soll.

```
aws lambda create-event-source-mapping --function-name my-function \
    --event-source-arn arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy
    --batch-size 500 \
    --starting-position AT_TIMESTAMP \
    --starting-position-timestamp 1541139109 \
    --source-access-configurations
 '[{"Type":"BASIC_AUTH","URI":"arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocDBSecret-BAtjxi"}]' \
    --document-db-event-source-config '{"DatabaseName":"test_database",
 "CollectionName": "test_collection"}' \
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "BatchSize": 500,
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "MaximumBatchingWindowInSeconds": 0,
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541348195.412,
    "LastProcessingResult": "No records processed",
    "State": "Creating",
    "StateTransitionReason": "User action"
}
```

Nach der Erstellung können Sie den `update-event-source-mapping`-Befehl verwenden, um die Einstellungen für Ihre Amazon-DocumentDB-Ereignisquelle zu aktualisieren. Im folgenden Beispiel werden die Batchgröße auf 1 000 und das Batchfenster auf 10 Sekunden aktualisiert. Für diesen

Befehl benötigen Sie die UUID Ihrer Zuordnung von Ereignisquellen, die Sie über den `list-event-source-mapping`-Befehl oder die Lambda-Konsole abrufen können.

```
aws lambda update-event-source-mapping --function-name my-function \
    --uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b \
    --batch-size 1000 \
    --batch-window 10
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "BatchSize": 500,
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "MaximumBatchingWindowInSeconds": 0,
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541359182.919,
    "LastProcessingResult": "OK",
    "State": "Updating",
    "StateTransitionReason": "User action"
}
```

Da Lambda die Einstellungen asynchron aktualisiert, werden Sie diese Änderungen möglicherweise erst nach Abschluss des Vorgangs in der Ausgabe sehen. Verwenden Sie den `get-event-source-mapping`-Befehl, um die aktuellen Einstellungen Ihrer Zuordnung von Ereignisquellen anzuzeigen.

```
aws lambda get-event-source-mapping --uuid f89f8514-cdd9-4602-9e1f-01a5b77d449b
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "UUID": "2b733gdc-8ac3-cdf5-af3a-1827b3b11284",
    "DocumentDBEventSourceConfig": {
        "CollectionName": "test_collection",
```

```
        "DatabaseName": "test_database",
        "FullDocument": "Default"
    },
    "BatchSize": 1000,
    "MaximumBatchingWindowInSeconds": 10,
    "EventSourceArn": "arn:aws:rds:us-west-2:123456789012:cluster:privatecluster7de2-
epzcyvu4pjoy",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "LastModified": 1541359182.919,
    "LastProcessingResult": "OK",
    "State": "Enabled",
    "StateTransitionReason": "User action"
}
```

Um Ihre Zuordnung von Ereignisquellen von Amazon DocumentDB zu löschen, verwenden Sie den `delete-event-source-mapping`-Befehl.

```
aws lambda delete-event-source-mapping \
    --uuid 2b733gdc-8ac3-cdf5-af3a-1827b3b11284
```

Startpositionen für Abfragen und Streams

Beachten Sie, dass die Stream-Abfrage bei der Erstellung und Aktualisierung der Zuordnung von Ereignisquellen letztendlich konsistent ist.

- Bei der Erstellung der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis mit der Abfrage von Ereignissen aus dem Stream begonnen wird.
- Bei Aktualisierungen der Zuordnung von Ereignisquellen kann es mehrere Minuten dauern, bis die Abfrage von Ereignissen aus dem Stream gestoppt und neu gestartet wird.

Dieses Verhalten bedeutet, dass, wenn Sie `LATEST` als Startposition für den Stream angeben, die Zuordnung von Ereignisquellen bei der Erstellung oder Aktualisierung möglicherweise Ereignisse übersieht. Um sicherzustellen, dass keine Ereignisse übersehen werden, geben Sie die Startposition des Streams als `TRIM_HORIZON` oder `AT_TIMESTAMP` an.

Überwachen Ihrer Amazon-DocumentDB-Ereignisquelle

Um Sie bei der Überwachung Ihrer Amazon-DocumentDB-Ereignisquelle zu unterstützen, gibt Lambda die Metrik `IteratorAge` aus, wenn die Funktion das Verarbeiten von Datensätzen abgeschlossen hat. Das Iterator-Alter ist der Unterschied zwischen dem Zeitstempel des letzten

Ereignisses und dem aktuellen Zeitstempel. Im Wesentlichen gibt die Metrik `IteratorAge` an, wie alt der letzte Datensatz im Batch bei Fertigstellung der Verarbeitung war. Wenn Ihre Funktion derzeit neue Ereignisse verarbeitet, können Sie mit dem Iterator-Alter die Latenz zwischen dem Zeitpunkt, zu dem ein Datensatz hinzugefügt wird, und dem Zeitpunkt, zu dem die Funktion verarbeitet wird, schätzen. Eine ansteigende Tendenz bei `IteratorAge` kann auf Probleme mit Ihrer Funktion hindeuten. Weitere Informationen finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Amazon DocumentDB DocumentDB-Change-Streams sind nicht für die Bewältigung großer Zeitlücken zwischen Ereignissen optimiert. Wenn Ihre Amazon DocumentDB DocumentDB-Ereignisquelle über einen längeren Zeitraum keine Ereignisse empfängt, kann Lambda die Zuordnung der Ereignisquellen deaktivieren. Die Länge dieses Zeitraums kann je nach Clustergröße und anderen Workloads zwischen einigen Wochen und einigen Monaten variieren.

Lambda unterstützt Nutzlasten von bis zu 6 MB. Änderungsstream-Ereignisse von Amazon DocumentDB können jedoch bis zu 16 MB groß sein. Wenn Ihr Änderungsstream versucht, Lambda ein Änderungsstream-Ereignis zu senden, das größer als 6 MB ist, löscht Lambda die Nachricht und gibt die Metrik `OversizedRecordCount` aus. Lambda gibt alle Metriken auf die bestmögliche Weise aus.

Tutorial: Verwendung AWS Lambda mit Amazon DocumentDB DocumentDB-Streams

In diesem Tutorial erstellen Sie eine einfache Lambda-Funktion, die Ereignisse aus einem Amazon DocumentDB (mit MongoDB-Kompatibilität) Change-Stream konsumiert. Um dieses Tutorial abzuschließen, werden Sie die folgenden Phasen durchlaufen:

- Richten Sie Ihren Amazon-DocumentDB-Cluster ein, stellen Sie eine Verbindung zu ihm her und aktivieren Sie Change-Streams darauf.
- Erstellen Sie Ihre Lambda-Funktion und konfigurieren Sie Ihren Amazon-DocumentDB-Cluster als Ereignisquelle für Ihre Funktion.
- Testen Sie das end-to-end Setup, indem Sie Elemente in Ihre Amazon DocumentDB DocumentDB-Datenbank einfügen.

Themen

- Erstellen des Secrets in Secrets Manager
- Installieren der mongo-Shell
- Mit dem DocumentDB-Cluster verbinden
- Change-Streams aktivieren
- Schnittstellen-VPC-Endpunkte erstellen
- Erstellen der Ausführungsrolle
- So erstellen Sie die Lambda-Funktion:
- Erstellen Sie die Zuordnung von Ereignisquellen in Lambda
- Testen Sie Ihre -Funktion – manueller Aufruf
- Testen Sie Ihre Funktion – fügen Sie einen Datensatz ein
- Testen Sie Ihre Funktion – aktualisieren Sie einen Datensatz
- Testen Sie Ihre Funktion – löschen Sie einen Datensatz
- Bereinigen Ihrer Ressourcen

Voraussetzungen

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

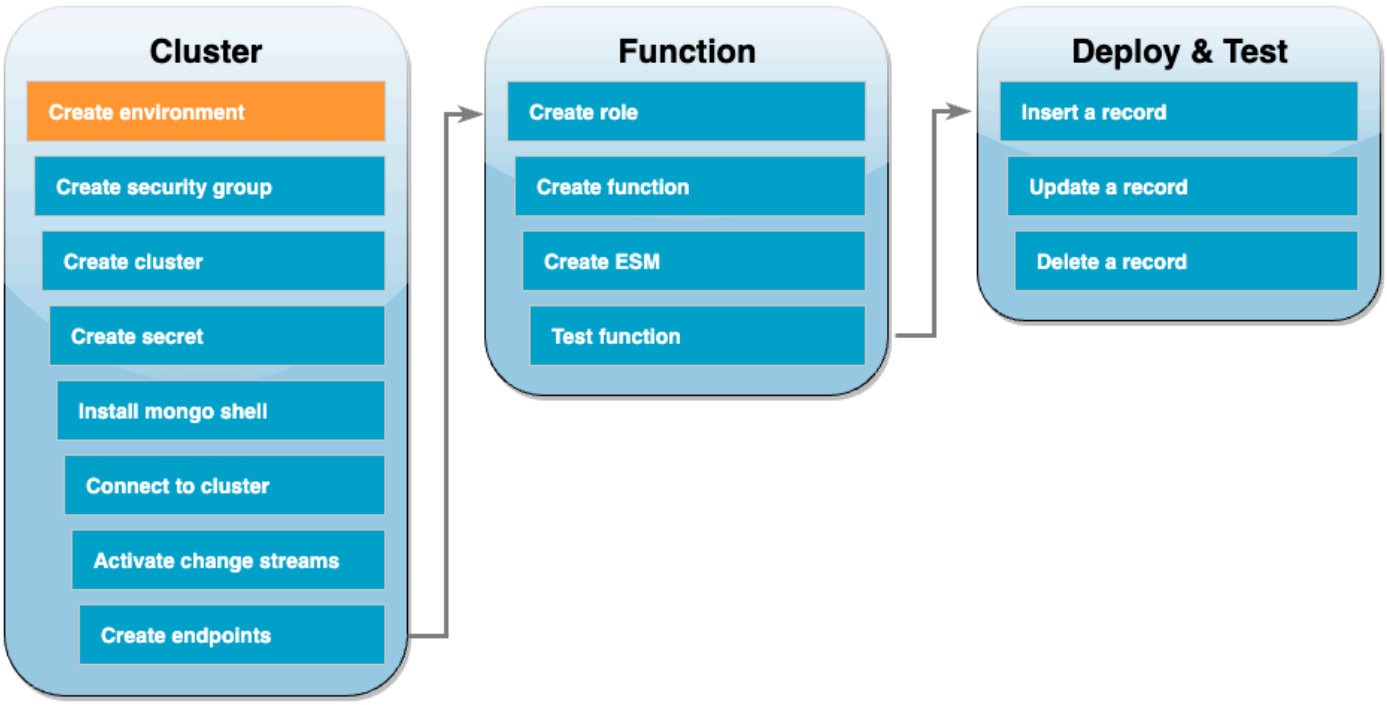
Installieren Sie das AWS Command Line Interface

Wenn Sie das noch nicht installiert haben AWS Command Line Interface, folgen Sie den Schritten unter Installieren oder Aktualisieren der neuesten Version von AWS CLI, um es zu installieren.

Das Tutorial erfordert zum Ausführen von Befehlen ein Befehlszeilenterminal oder eine Shell. Verwenden Sie unter Linux und macOS Ihre bevorzugte Shell und Ihren bevorzugten Paketmanager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux.

Erstellen Sie die AWS Cloud9 Umgebung



Bevor Sie die Lambda-Funktion erstellen, müssen Sie Ihren Amazon-DocumentDB-Cluster erstellen und konfigurieren. Die Schritte zum Einrichten Ihres Clusters in diesem Tutorial basieren auf dem Verfahren unter Erste Schritte mit Amazon DocumentDB.

> **Note**
>
> Wenn Sie bereits einen Amazon-DocumentDB-Cluster eingerichtet haben, stellen Sie sicher, dass Sie Change-Streams aktivieren und die erforderlichen Schnittstellen-VPC-Endpunkte erstellen. Anschließend können Sie direkt mit den Schritten zur Funktionserstellung fortfahren.

Erstellen Sie zunächst eine AWS Cloud9 Umgebung. Sie werden diese Umgebung in diesem Tutorial verwenden, um eine Verbindung zu Ihrem DocumentDB-Cluster herzustellen und ihn abzufragen.

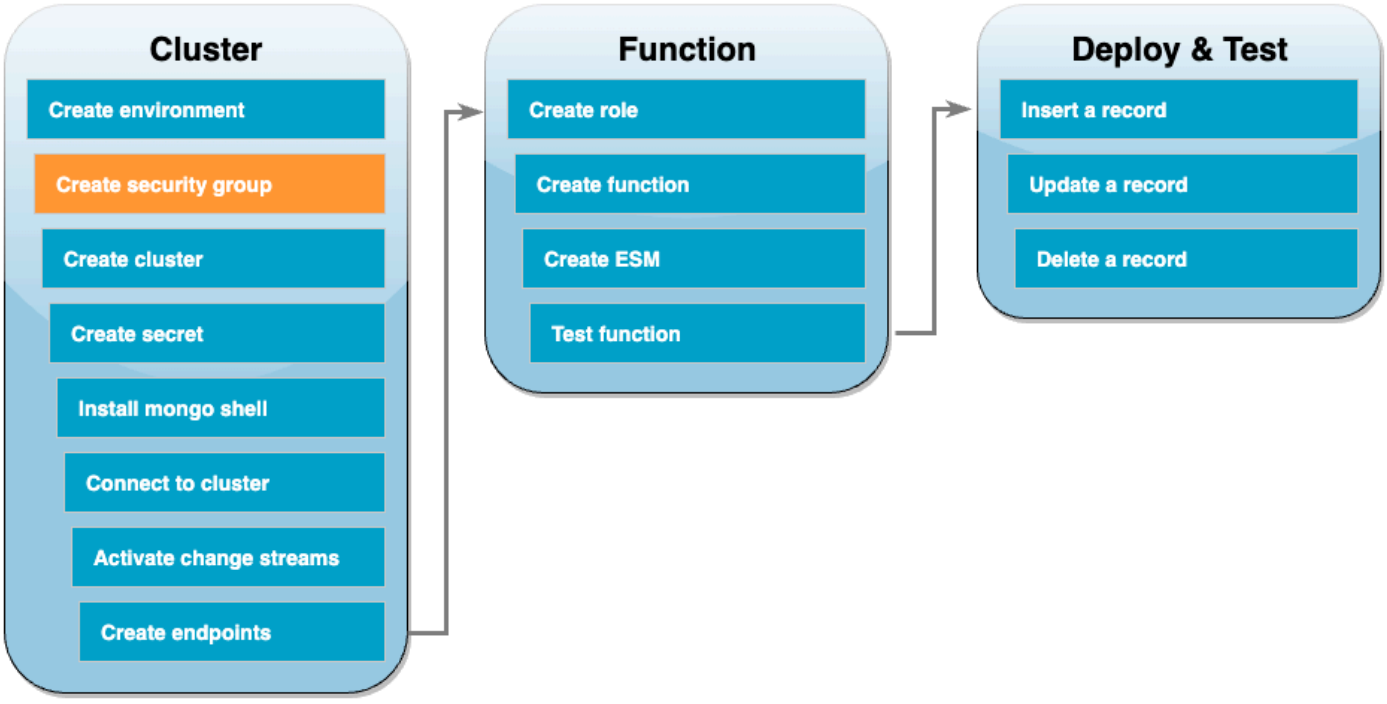
Um eine AWS Cloud9 Umgebung zu schaffen

1. Öffnen Sie die Cloud9-Konsole und wählen Sie Umgebung erstellen.
2. Erstellen Sie eine Umgebung mit der folgenden Konfiguration:

- Unter Details:
  - Name (Name – `DocumentDBCloud9Environment`
  - Umgebungstyp – Neue EC2-Instance
- Unter Neue EC2-Instance:
  - Instance-Typ – `t2.micro` (1 GiB RAM + 1 vCPU)
  - Plattform – Amazon Linux 2
  - Timeout – 30 Minuten
- Unter Netzwerkeinstellungen:
  - Verbindung — AWS Systems Manager (SSM)
  - Erweitern Sie das Dropdown-Menü für VPC-Einstellungen.
  - Amazon Virtual Private Cloud (VPC) – Wählen Sie Ihre Standard-VPC.
  - Subnetz – Keine Präferenz
- Behalten Sie die alle Standardeinstellung bei.

3. Wählen Sie Erstellen. Die Bereitstellung Ihrer neuen AWS Cloud9 Umgebung kann mehrere Minuten dauern.

Erstellen der EC2-Sicherheitsgruppe

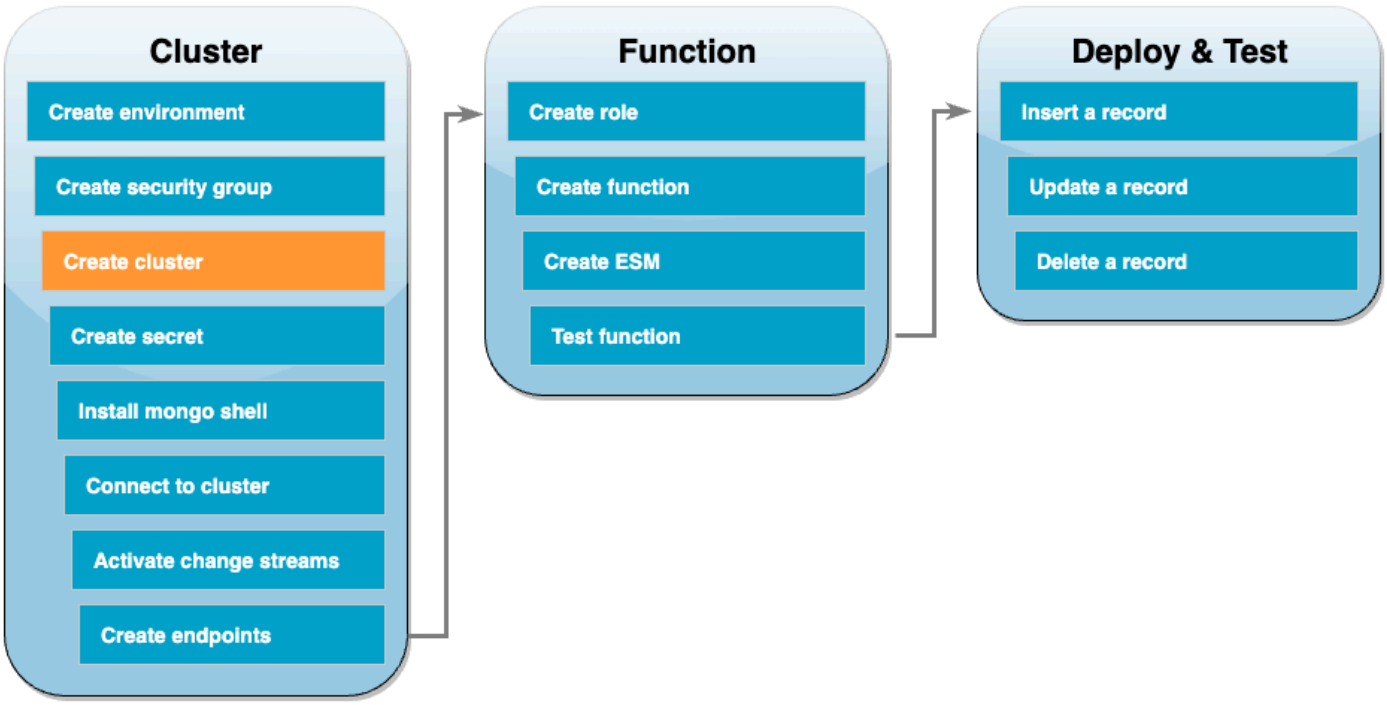


Erstellen Sie als Nächstes eine EC2-Sicherheitsgruppe mit Regeln, die den Datenverkehr zwischen Ihrem DocumentDB-Cluster und Ihrer Cloud9-Umgebung zulassen.

Um eine EC2-Sicherheitsgruppe zu erstellen

1. Öffnen Sie die EC2-Konsole. Wählen Sie unter Netzwerk und Sicherheit die Option Sicherheitsgruppen aus.
2. Wählen Sie Sicherheitsgruppe erstellen aus.
3. Erstellen Sie eine Sicherheitsgruppe mit der folgenden Konfiguration:
   - Unter Grundlegende Details:
     - Name der Sicherheitsgruppe – `DocDBTutorial`
     - Beschreibung – Sicherheitsgruppe für den Datenverkehr zwischen Cloud9 und DocumentDB.
     - VPC – Wählen Sie Ihre Standard-VPC aus.
   - Wählen Sie unter Inbound rules (Regeln für eingehenden Datenverkehr) die Option Add rule (Regel hinzufügen). Erstellen Sie eine Regel mit der folgenden Konfiguration:
     - Typ – Benutzerdefiniertes TCP
     - Portbereich – 27017
     - Quelle – Benutzerdefiniert
     - Wählen Sie im Suchfeld neben Quelle die Sicherheitsgruppe für die AWS Cloud9 Umgebung aus, die Sie im vorherigen Schritt erstellt haben. Um eine Liste der verfügbaren Sicherheitsgruppen anzuzeigen, geben Sie `cloud9` in das Suchfeld ein. Wählen Sie die Sicherheitsgruppe mit dem Namen `aws-cloud9-<environment_name>` aus.
   - Behalten Sie die alle Standardeinstellung bei.
4. Wählen Sie Sicherheitsgruppe erstellen aus.

Erstellen Sie den DocumentDB-Cluster



In diesem Schritt erstellen Sie einen DocumentDB-Cluster mithilfe der Sicherheitsgruppe aus dem vorigen Schritt.

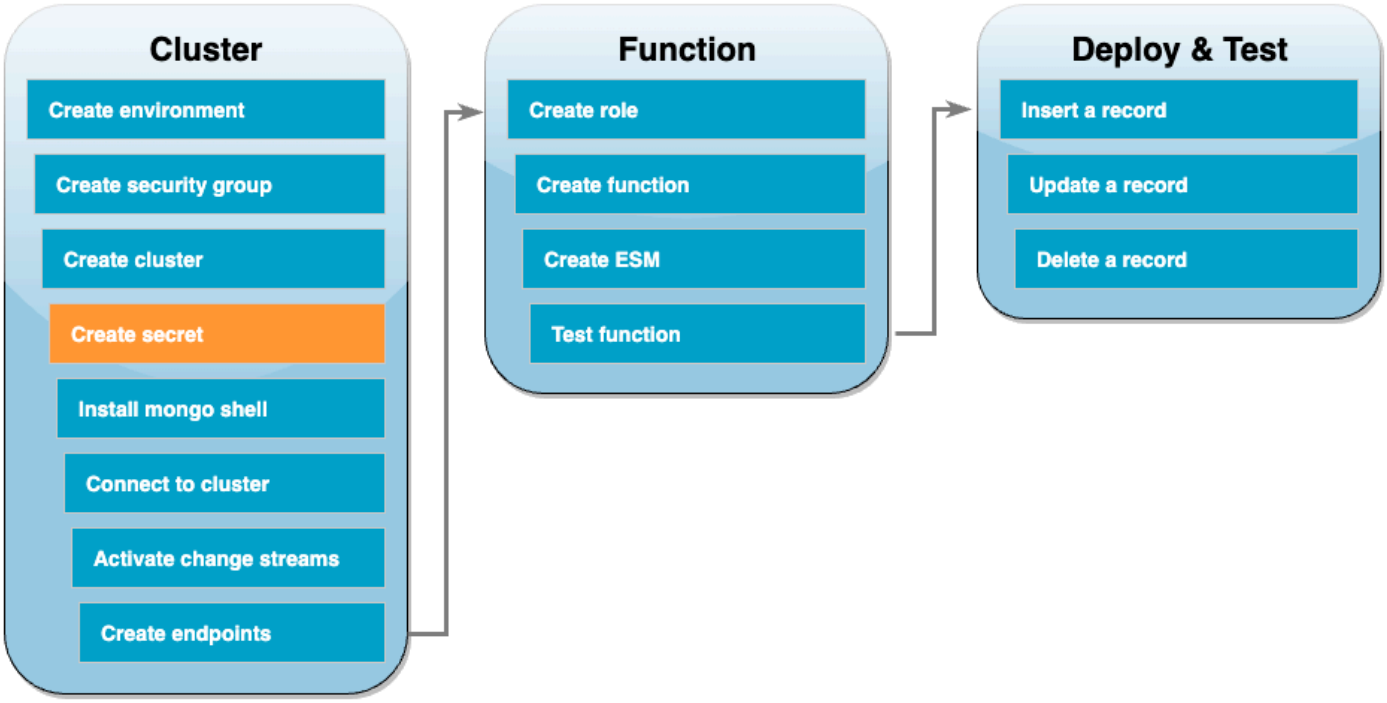
Um einen DocumentDB-Cluster zu erstellen

1. Öffnen Sie die DocumentDB-Konsole. Wählen Sie unter Cluster die Option Erstellen aus.
2. Erstellen Sie einen Cluster mit der folgenden Konfiguration:
   - Wählen Sie als Cluster-Typ die Option Instance-basierter Cluster aus.
   - Unter Konfiguration:
     - Engine-Version — 5.0.0
     - Instanzklasse — db.t3.medium (für eine kostenlose Testversion geeignet)
     - Anzahl der Instances – 1.
   - Unter Authentifizierung:
     - Geben Sie den Benutzernamen und das Passwort ein, die für die Verbindung zu Ihrem Cluster erforderlich sind (dieselben Anmeldeinformationen, mit denen Sie das Geheimnis im vorherigen Schritt erstellt haben). Bestätigen Sie unter Passwort bestätigen Ihr Passwort.
   - Aktivieren Sie Erweiterte Einstellungen anzeigen.

- Unter Netzwerkeinstellungen:
  - Virtual Private Cloud (VPC) – Wählen Sie Ihre Standard-VPC.
  - Subnetz-Gruppe – standard
  - VPC-Sicherheitsgruppen – Wählen Sie neben der `default (VPC)` auch die `DocDBTutorial (VPC)`-Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.
- Behalten Sie die alle Standardeinstellung bei.

3. Wählen Sie Cluster erstellen. Die Bereitstellung Ihres DocumentDB-Clusters kann einige Minuten dauern.

Erstellen des Secrets in Secrets Manager



Um manuell auf Ihren DocumentDB-Cluster zuzugreifen, müssen Sie den Benutzernamen und das Passwort angeben. Damit Lambda auf Ihren Cluster zugreifen kann, müssen Sie bei der Einrichtung Ihrer Zuordnung von Ereignisquellen ein Secret in Secrets Manager angeben, das die gleichen Anmeldeinformationen enthält. In diesem Schritt erstellen Sie dieses Secret.

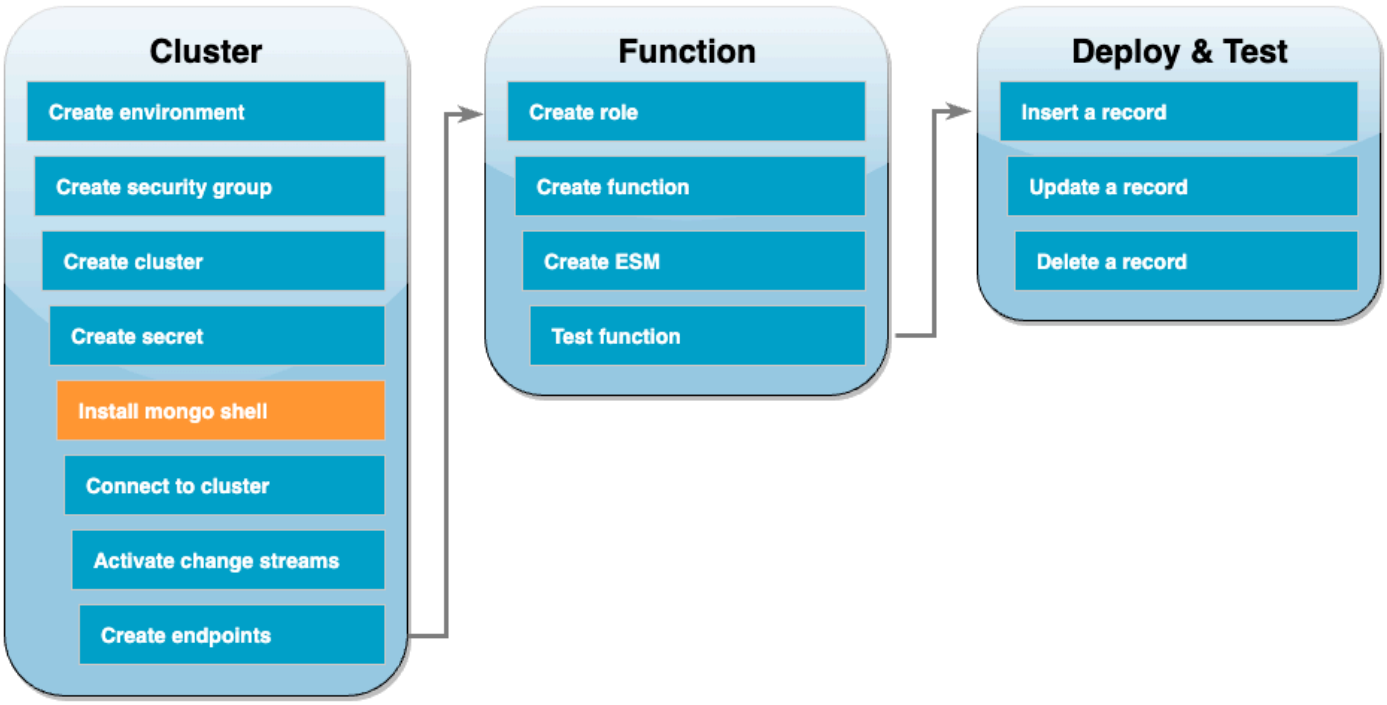
Um das Secret in Secrets Manager zu erstellen

1. Öffnen Sie die Secrets-Manager-Konsole und wählen Sie Neues Secret speichern.

2. Wählen Sie für Secret-Typ auswählen eine der folgenden Optionen aus:
    - Unter Grundlegende Details:
        - Secret-Typ – Anmeldeinformationen für die Amazon-DocumentDB-Datenbank
        - Geben Sie unter Anmeldeinformationen den Benutzernamen und das Passwort ein, die Sie für den Zugriff auf Ihren DocumentDB-Cluster verwenden werden.
        - Datenbank – Wählen Sie Ihren DocumentDB-Cluster aus.
        - Wählen Sie Weiter aus.
3. Wählen Sie unter Secret konfigurieen eine der folgenden Optionen aus:
    - Secret-Name – `DocumentDBSecret`
    - Wählen Sie Weiter.
4. Wählen Sie Weiter.
5. Wählen Sie Store (Speichern) aus.
6. Aktualisieren Sie die Konsole, um zu überprüfen, ob Sie das `DocumentDBSecret`-Secret erfolgreich gespeichert haben.

Notieren Sie sich den Secret ARN Ihres Geheimnisses. Sie werden es in einem späteren Schritt noch benötigen.

Installieren der mongo-Shell



In diesem Schritt installieren Sie die mongo-Shell in Ihrer Cloud9-Umgebung. Die mongo-Shell ist ein Befehlszeilenprogramm, mit dem Sie eine Verbindung zu Ihrem DocumentDB-Cluster herstellen und ihn abfragen können.

Um die mongo-Shell in Ihrer Cloud9-Umgebung zu installieren

1. Öffnen Sie die Cloud9-Konsole. Klicken Sie neben der `DocumentDBCloud9Environment`-Umgebung, die Sie zuvor erstellt haben, auf den Link Öffnen unter der Spalte Cloud9 IDE.
2. Erstellen Sie im Terminal-Fenster die MongoDB-Repository-Datei mit dem folgenden Befehl:

```
echo -e "[mongodb-org-5.0] \nname=MongoDB Repository\nbaseurl=https://
repo.mongodb.org/yum/amazon/2/mongodb-org/5.0/x86_64/\ngpgcheck=1 \nenabled=1
 \ngpgkey=https://www.mongodb.org/static/pgp/server-5.0.asc" | sudo tee /etc/
yum.repos.d/mongodb-org-5.0.repo
```

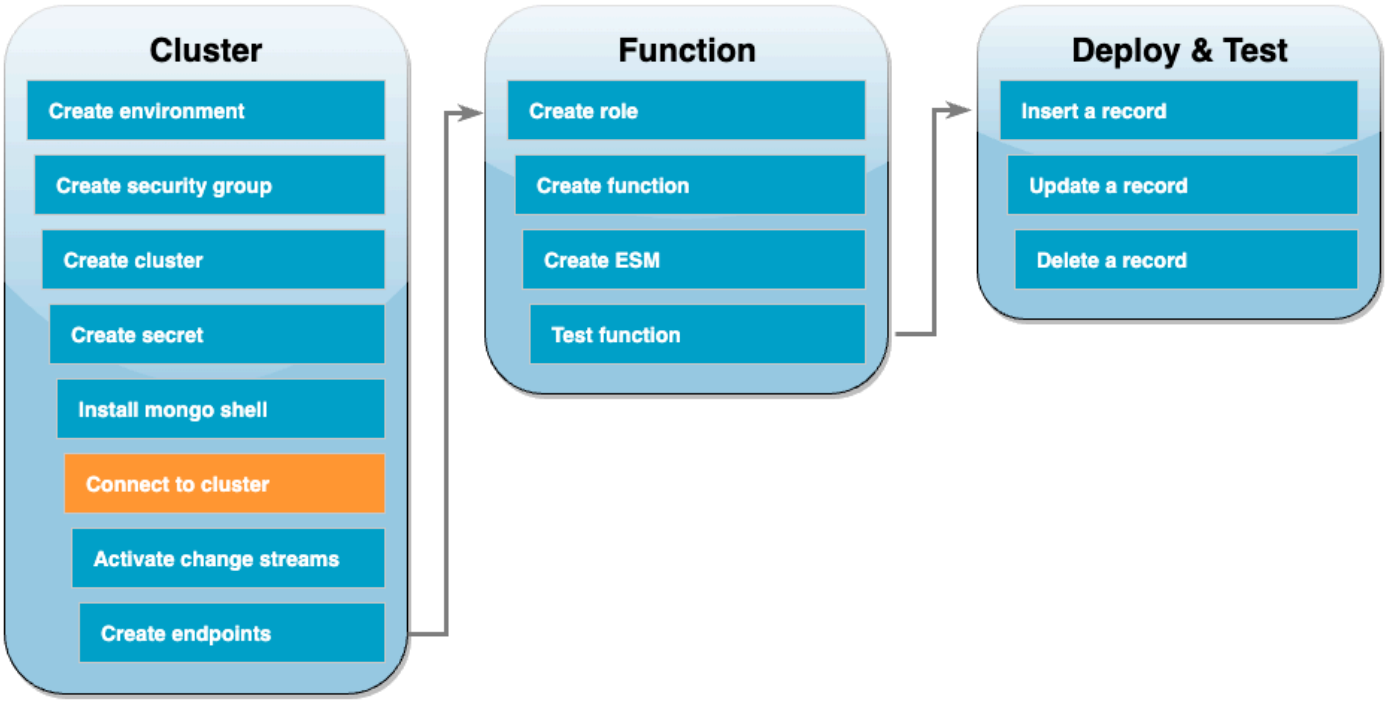
3. Installieren Sie daraufhin die mongo-Shell mit dem folgenden Befehl:

```
sudo yum install -y mongodb-org-shell
```

4. Um Daten während der Übertragung zu verschlüsseln, laden Sie den öffentlichen Schlüssel für Amazon DocumentDB. Der folgende Befehl lädt eine Datei mit dem Namen `global-bundle.pem` herunter:

```
wget https://truststore.pki.rds.amazonaws.com/global/global-bundle.pem
```

Mit dem DocumentDB-Cluster verbinden



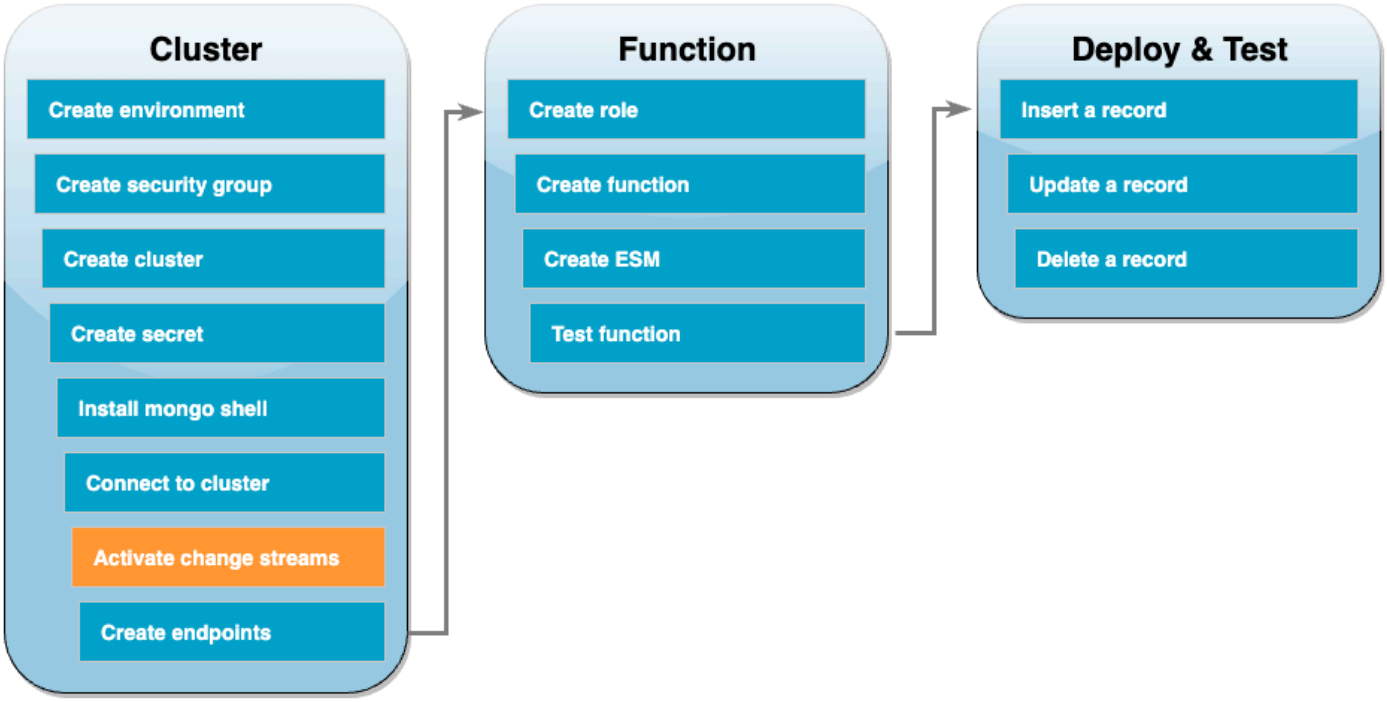
Sie sind jetzt bereit, mithilfe der mongo-Shell eine Verbindung zu Ihrem DocumentDB-Cluster herzustellen.

So stellen Sie eine Verbindung zu Ihrem DocumentDB-Cluster her

1. Öffnen Sie die DocumentDB-Konsole. Wählen Sie unter Cluster Ihren Cluster aus, indem Sie seine Cluster-ID auswählen.
2. Wählen Sie auf der Registerkarte Konnektivität und Sicherheit unter Mit der mongo-Shell mit diesem Cluster verbinden die Option Kopieren aus.
3. In Ihrer Cloud9-Umgebung fügen Sie diesen Befehl in das Terminal ein. Ersetzen Sie `<insertYourPassword>` durch das richtige Passwort.

Wenn nach der Eingabe dieses Befehls die Eingabeaufforderung auf `rs0:PRIMARY>` gesetzt wird, sind Sie mit Ihrem Amazon DocumentDB-Cluster verbunden.

Change-Streams aktivieren



In diesem Tutorial verfolgen Sie Änderungen an der `products`-Sammlung der `docdbdemo`-Datenbank in Ihrem DocumentDB-Cluster. Sie tun dies, indem Sie Change-Streams aktivieren. Erstellen Sie zunächst die `docdbdemo`-Datenbank und testen Sie sie, indem Sie einen Datensatz einfügen.

Um eine neue Datenbank in Ihrem Cluster zu erstellen

1. Stellen Sie in Ihrer Cloud9-Umgebung sicher, dass Sie immer noch mit Ihrem DocumentDB-Cluster verbunden sind.
2. Erstellen Sie mit dem folgenden Befehl im Terminal-Fenster eine neue Datenbank mit dem Namen `docdbdemo`:

   ```
   use docdbdemo
   ```

3. Verwenden Sie dann den folgenden Befehl, um einen Datensatz einzufügen `docdbdemo`:

   ```
   db.products.insert({"hello":"world"})
   ```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
WriteResult({ "nInserted" : 1 })
```

4. Verwenden Sie den folgenden Befehl, um alle Datenbanken aufzulisten:

```
show dbs
```

Stellen Sie sicher, dass Ihre Ausgabe die `docdbdemo`-Datenbank enthält:

```
docdbdemo  0.000GB
```

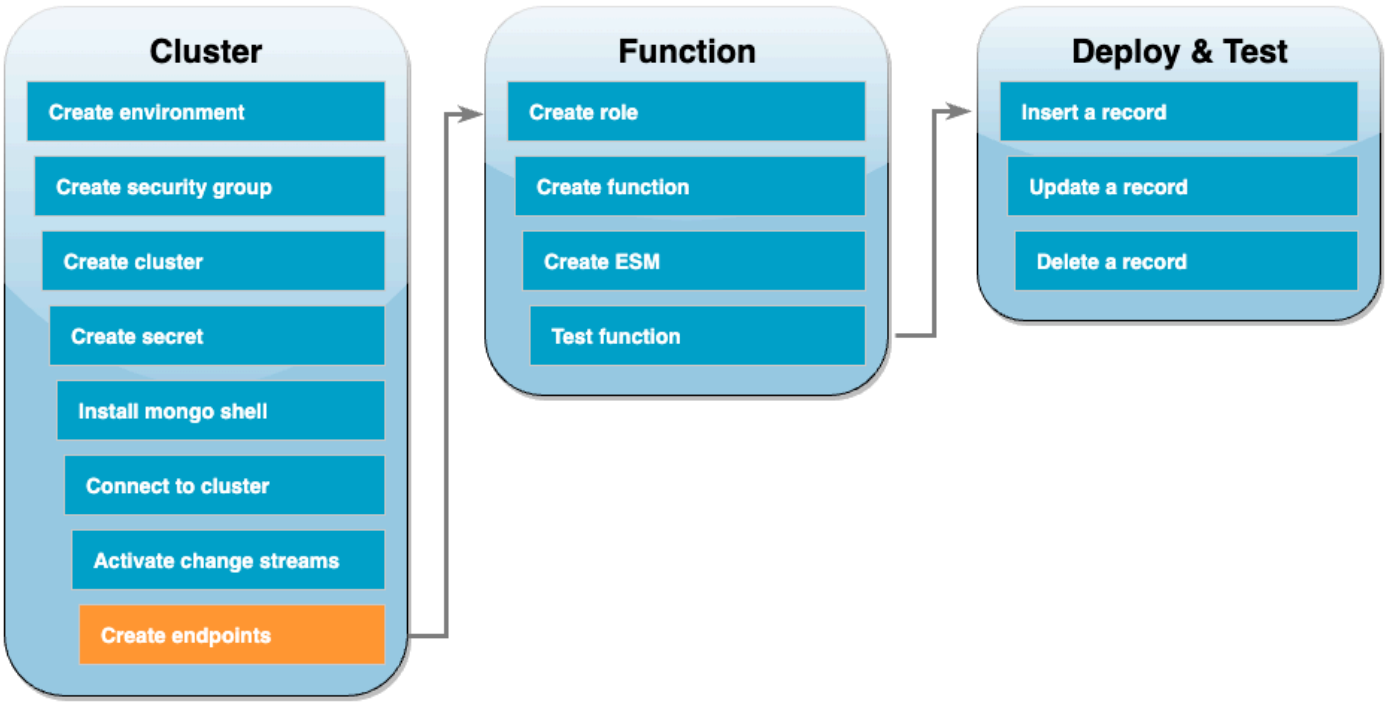
Dann aktivieren Sie mit dem folgenden Befehl Change-Streams für die `products`-Sammlung der `docdbdemo`-Datenbank:

```
db.adminCommand({modifyChangeStreams: 1,
    database: "docdbdemo",
    collection: "products",
    enable: true});
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{ "ok" : 1, "operationTime" : Timestamp(1680126165, 1) }
```

Schnittstellen-VPC-Endpunkte erstellen



Erstellen Sie als Nächstes Schnittstellen-VPC-Endpunkte, um sicherzustellen, dass Lambda und Secrets Manager (der später zum Speichern unserer Cluster-Anmeldeinformationen verwendet wird) eine Verbindung zu Ihrer Standard-VPC herstellen können.

Um Schnittstellen-VPC-Endpunkte zu erstellen

1. Öffnen Sie die VPC;-Konsole. Wählen Sie im linken Menü unter Virtual Private Cloud die Option Endpunkte aus.
2. Wählen Sie Endpunkt erstellen aus. Erstellen Sie einen Endpunkt mit der folgenden Konfiguration:

   - Geben Sie für Name Tag `lambda-default-vpc` ein.
   - Wählen Sie als Dienstkategorie die Option AWS Dienste aus.
   - Geben Sie unter Services `lambda` in das Suchfeld ein. Wählen Sie den Service im Format `com.amazonaws.<region>.lambda`.
   - Wählen Sie bei VPC Ihre Standard-VPC aus.
   - Aktivieren Sie für Subnetze die Kästchen neben jeder Availability Zone. Wählen Sie die richtige Subnetz-ID für jede Availability Zone.

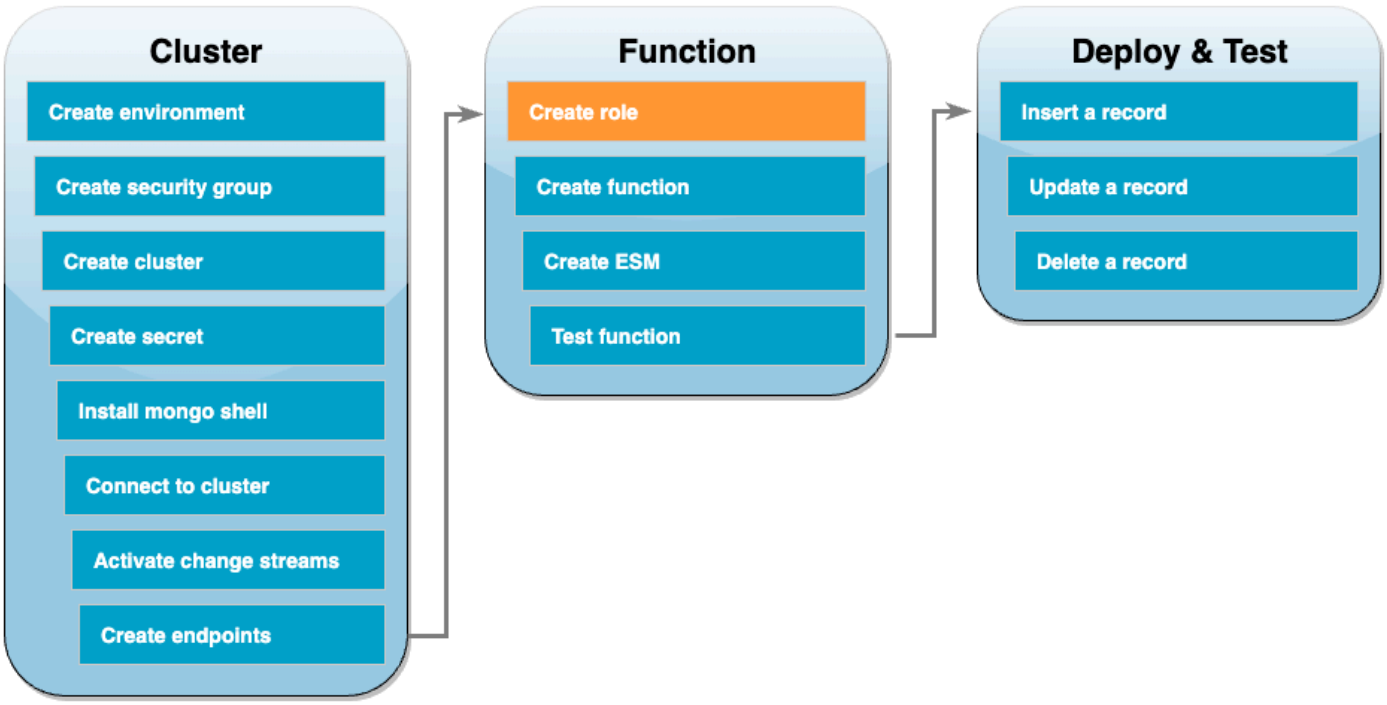
- Wählen Sie unter IP-Adresstyp IPv4 aus.
- Wählen Sie für Sicherheitsgruppen die Standard-VPC-Sicherheitsgruppe (Gruppenname von `default`) und die Sicherheitsgruppe, die Sie zuvor erstellt haben (Gruppenname von `DocDBTutorial`).
- Behalten Sie die alle Standardeinstellung bei.
- Wählen Sie Endpunkt erstellen aus.

3. Wählen Sie erneut Endpunkt erstellen. Erstellen Sie einen Endpunkt mit der folgenden Konfiguration:

   - Geben Sie für Name Tag `secretsmanager-default-vpc` ein.
   - Wählen Sie als Servicekategorie die Option AWS Dienste aus.
   - Geben Sie unter Services `secretsmanager` in das Suchfeld ein. Wählen Sie den Service im Format `com.amazonaws.<region>.secretsmanager`.
   - Wählen Sie bei VPC Ihre Standard-VPC aus.
   - Aktivieren Sie für Subnetze die Kästchen neben jeder Availability Zone. Wählen Sie die richtige Subnetz-ID für jede Availability Zone.
   - Wählen Sie unter IP-Adresstyp IPv4 aus.
   - Wählen Sie für Sicherheitsgruppen die Standard-VPC-Sicherheitsgruppe (Gruppenname von `default`) und die Sicherheitsgruppe, die Sie zuvor erstellt haben (Gruppenname von `DocDBTutorial`).
   - Behalten Sie die alle Standardeinstellung bei.
   - Wählen Sie Endpunkt erstellen aus.

Damit ist der Abschnitt zur Einrichtung eines Clusters in diesem Tutorial abgeschlossen.

Erstellen der Ausführungsrolle



In den nächsten Schritten erstellen Sie Ihre Lambda-Funktion. Zunächst müssen Sie die Ausführungsrolle erstellen, die Ihrer Funktion die Berechtigung zum Zugriff auf Ihren Cluster gibt. Dazu erstellen Sie zunächst eine IAM-Richtlinie und verknüpfen diese dann mit einer IAM-Rolle.

So erstellen Sie eine IAM-Richtlinie

1. Öffnen Sie in der IAM-Konsole die Seite Richtlinien und wählen Sie dann Richtlinie erstellen aus.
2. Wählen Sie den Tab JSON. Ersetzen Sie in der folgenden Richtlinie den ARN der Secrets-Manager-Ressource in der letzten Zeile der Anweisung durch Ihren geheimen ARN von zuvor, und kopieren Sie die Richtlinie in den Editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LambdaESMNetworkingAccess",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
```

```
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kms:Decrypt"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LambdaDocDBESMAccess",
            "Effect": "Allow",
            "Action": [
                "rds:DescribeDBClusters",
                "rds:DescribeDBClusterParameters",
                "rds:DescribeDBSubnetGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LambdaDocDBESMGetSecretValueAccess",
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:us-
east-1:123456789012:secret:DocumentDBSecret"
        }
    ]
}
```

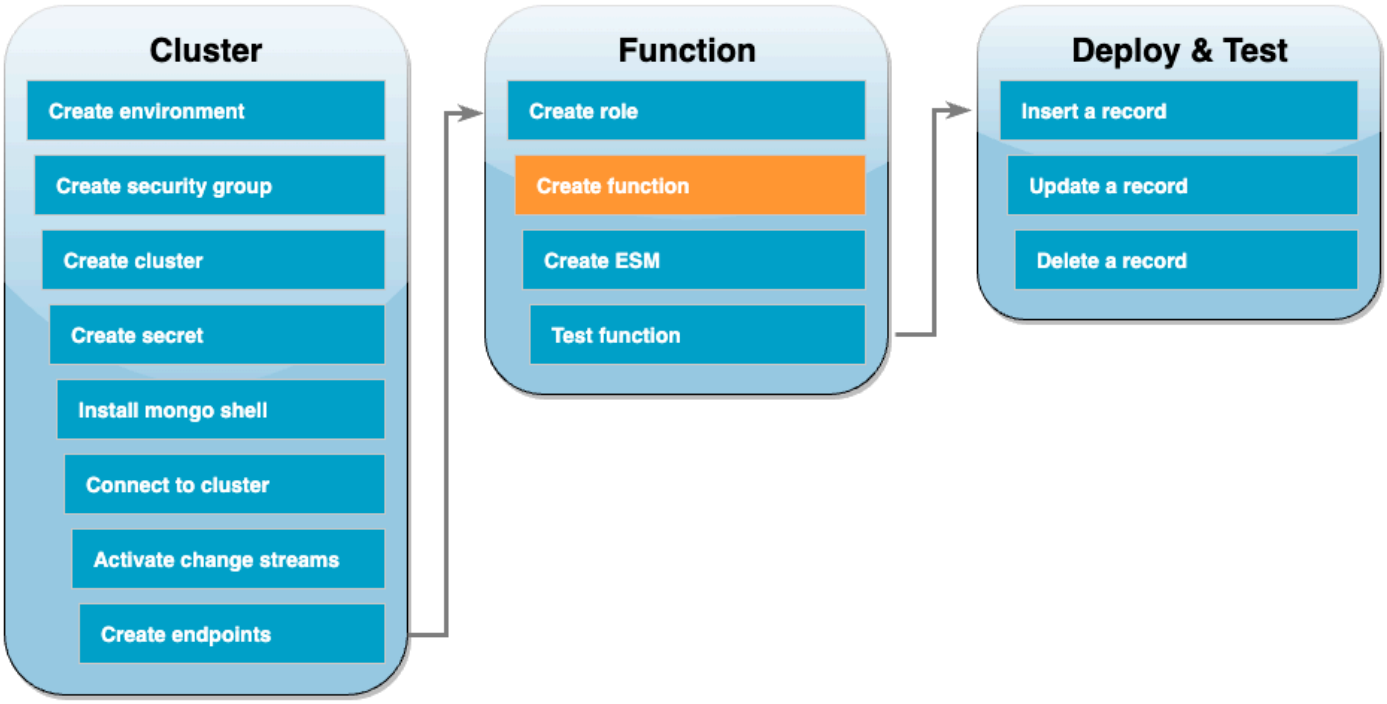
3. Wählen Sie Weiter: Tags und dann Weiter: Prüfen aus.
4. Geben Sie unter Name `AWSDocumentDBLambdaPolicy` ein.
5. Wählen Sie Richtlinie erstellen aus.

So erstellen Sie die IAM-Rolle

1. Öffnen Sie die Seite Rollen in der IAM-Konsole und wählen Sie Rolle erstellen.
2. Wählen Sie für Vertrauenswürdige Entität auswählen die folgenden Optionen:
   - Typ der vertrauenswürdigen Entität — AWS Dienst
   - Anwendungsfall – Lambda
   - Wählen Sie Weiter aus.

3. Wählen Sie für Berechtigungen hinzufügen die `AWSDocumentDBLambdaPolicy` Richtlinie aus, die Sie gerade erstellt haben, sowie die, `AWSLambdaBasicExecutionRole` um Ihrer Funktion Berechtigungen zum Schreiben in Amazon CloudWatch Logs zu erteilen.
4. Wählen Sie Weiter aus.
5. Geben Sie für Role name (Rollenname) den Namen `AWSDocumentDBLambdaExecutionRole` ein.
6. Wählen Sie Create role (Rolle erstellen) aus.

So erstellen Sie die Lambda-Funktion:



Der folgende Beispiel-Code empfängt eine DocumentDB-Ereigniseingabe und verarbeitet die darin enthaltene Nachricht.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package main

import (
 "context"
 "encoding/json"
 "fmt"

 "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
 Events []Record `json:"events"`
}

type Record struct {
 Event struct {
  OperationType string `json:"operationType"`
  NS            struct {
   DB   string `json:"db"`
   Coll string `json:"coll"`
  } `json:"ns"`
  FullDocument interface{} `json:"fullDocument"`
 } `json:"event"`
}

func main() {
```

```
 lambda.Start(handler)
}

func handler(ctx context.Context, event Event) (string, error) {
 fmt.Println("Loading function")
 for _, record := range event.Events {
  logDocumentDBEvent(record)
 }

 return "OK", nil
}

func logDocumentDBEvent(record Record) {
 fmt.Printf("Operation type: %s\n", record.Event.OperationType)
 fmt.Printf("db: %s\n", record.Event.NS.DB)
 fmt.Printf("collection: %s\n", record.Event.NS.Coll)
 docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", "  ")
 fmt.Printf("Full document: %s\n", string(docBytes))
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Amazon DocumentDB DocumentDB-Ereignis mit Lambda verwenden. JavaScript

```
console.log('Loading function');
exports.handler = async (event, context) => {
    event.events.forEach(record => {
        logDocumentDBEvent(record);
    });
    return 'OK';
};

const logDocumentDBEvent = (record) => {
```

```
    console.log('Operation type: ' + record.event.operationType);
    console.log('db: ' + record.event.ns.db);
    console.log('collection: ' + record.event.ns.coll);
    console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
 2));
};
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda mithilfe von Python.

```
import json

def lambda_handler(event, context):
    for record in event.get('events', []):
        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})

    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
    print("Full document:", json.dumps(full_document, indent=2))
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda mithilfe von Ruby.

```
require 'json'

def lambda_handler(event:, context:)
  event['events'].each do |record|
    log_document_db_event(record)
  end
  'OK'
end

def log_document_db_event(record)
  event_data = record['event'] || {}
  operation_type = event_data['operationType'] || 'Unknown'
  db = event_data.dig('ns', 'db') || 'Unknown'
  collection = event_data.dig('ns', 'coll') || 'Unknown'
  full_document = event_data['fullDocument'] || {}

  puts "Operation type: #{operation_type}"
  puts "db: #{db}"
  puts "collection: #{collection}"
  puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

So erstellen Sie die Lambda-Funktion:

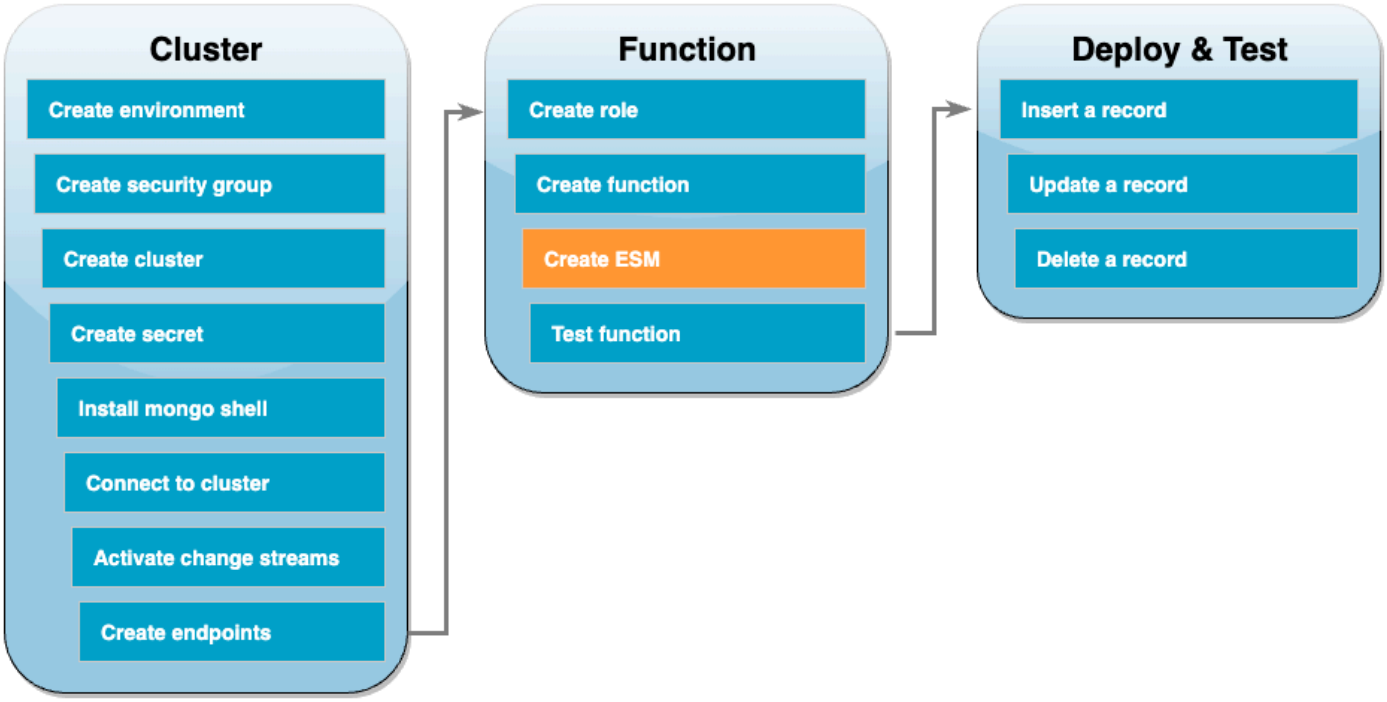
1. Kopieren Sie den Beispiel-Code in eine Datei mit dem Namen `index.js`.
2. Erstellen Sie ein Bereitstellungspaket mit dem folgenden -Befehl.

```
zip function.zip index.js
```

3. Verwenden Sie den folgenden CLI-Befehl, um die Funktion zu erstellen. Ersetzen Sie `us-east-1` durch Ihre Region und `123456789012` durch Ihre Konto-ID.

```
aws lambda create-function --function-name ProcessDocumentDBRecords \
    --zip-file fileb://function.zip --handler index.handler --runtime nodejs20.x \
    --region us-east-1 \
    --role arn:aws:iam::123456789012:role/AWSDocumentDBLambdaExecutionRole
```

Erstellen Sie die Zuordnung von Ereignisquellen in Lambda



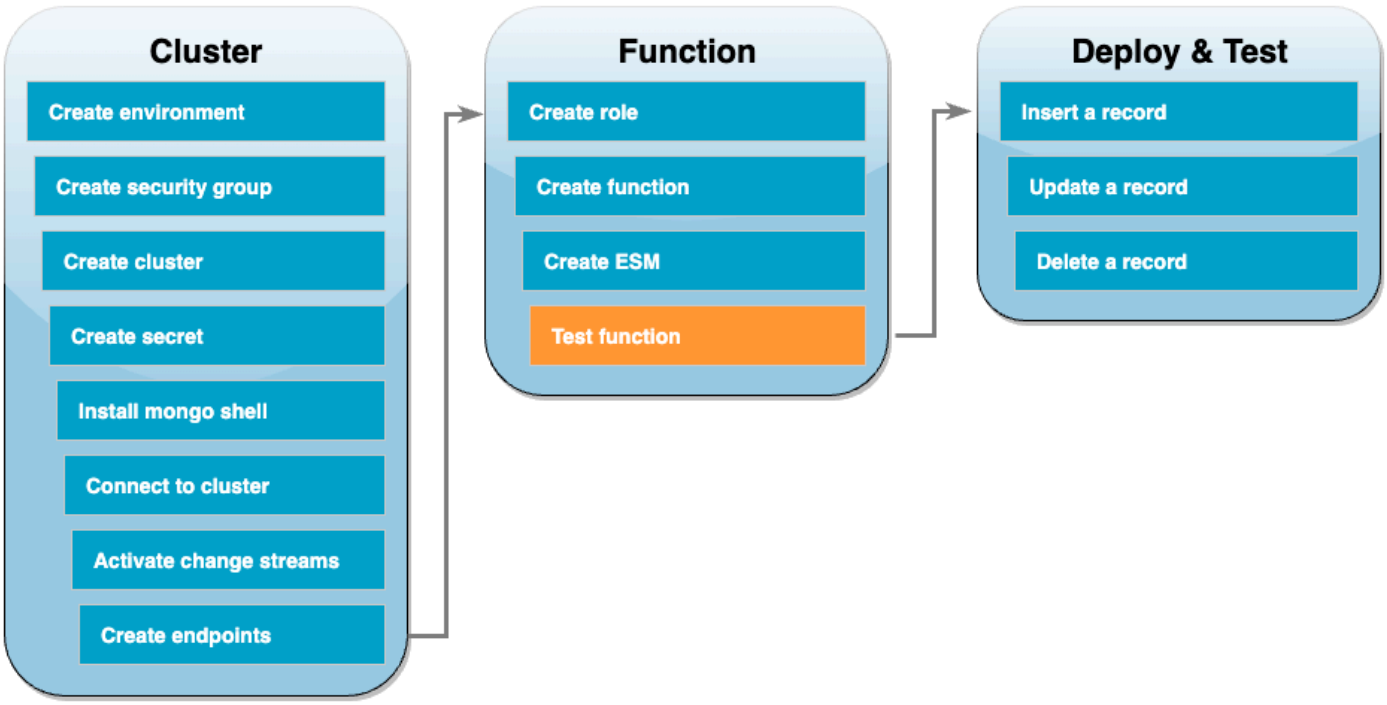
Erstellen Sie die Zuordnung von Ereignisquellen, die Ihren DocumentDB-Change-Stream mit Ihrer Lambda-Funktion verknüpft. Nachdem Sie diese Ereignisquellenzuordnung erstellt haben, beginnt AWS Lambda sofort die Abfrage des Streams.

Die Zuordnung von Ereignisquellen erstellen

1. Öffnen Sie die Seite Funktionen in der Lambda-Konsole.
2. Wählen Sie die `ProcessDocumentDBRecords`-Funktion aus, die Sie zuvor erstellt haben.

3. Wählen Sie die Registerkarte Konfiguration und dann im linken Menü Auslöser.
4. Wählen Sie Add trigger.
5. Wählen Sie unter Trigger-Konfiguration als Quelle die Option DocumentDB aus.
6. Erstellen Sie die Zuordnung von Ereignisquellen mit der folgenden Konfiguration:
   - DocumentDB-Cluster – Wählen Sie den Cluster aus, den Sie zuvor erstellt haben.
   - Name der Datenbank – `docdbdemo`
   - Name der Kollektion – Produkte
   - Batch size – 1
   - Startposition – Neueste
   - Authentifizierung – BASIC_AUTH
   - Secrets-Manager-Schlüssel – Wählen Sie den `DocumentDBSecret` aus, den Sie gerade erstellt haben.
   - Batchfenster – 1
   - Vollständige Konfiguration des Dokuments — UpdateLookup
7. Wählen Sie Hinzufügen aus. Die Erstellung Ihrer Zuordnung von Ereignisquellen kann einige Minuten dauern.

Testen Sie Ihre -Funktion – manueller Aufruf



Um zu testen, ob Sie Ihre Funktion und die Zuordnung von Ereignisquellen korrekt erstellt haben, rufen Sie Ihre Funktion mit dem Befehl `invoke` auf. Kopieren Sie dazu zunächst die folgende Ereignis-JSON in eine Datei mit dem Namen `input.txt`:

```
{
  "eventSourceArn": "arn:aws:rds:us-east-1:123456789012:cluster:canaryclusterb2a659a2-
qo5tcmqkcl03",
  "events": [
    {
      "event": {
        "_id": {
          "_data": "0163eeb6e7000000090100000009000041e1"
        },
        "clusterTime": {
          "$timestamp": {
            "t": 1676588775,
            "i": 9
          }
        },
        "documentKey": {
          "_id": {
            "$oid": "63eeb6e7d418cd98afb1c1d7"
```

```
          }
        },
        "fullDocument": {
          "_id": {
            "$oid": "63eeb6e7d418cd98afb1c1d7"
          },
          "anyField": "sampleValue"
        },
        "ns": {
          "db": "docdbdemo",
          "coll": "products"
        },
        "operationType": "insert"
      }
    }
  ],
  "eventSource": "aws:docdb"
}
```

Verwenden Sie dann den folgenden Befehl, um Ihre Funktion mit diesem Ereignis aufzurufen:

```
aws lambda invoke --function-name ProcessDocumentDBRecords \
    --cli-binary-format raw-in-base64-out \
    --region us-east-1 \
    --payload file://input.txt out.txt
```

Sie sollten eine Antwort erhalten, die wie die folgende aussieht:

```
{
   "StatusCode": 200,
   "ExecutedVersion": "$LATEST"
}
```

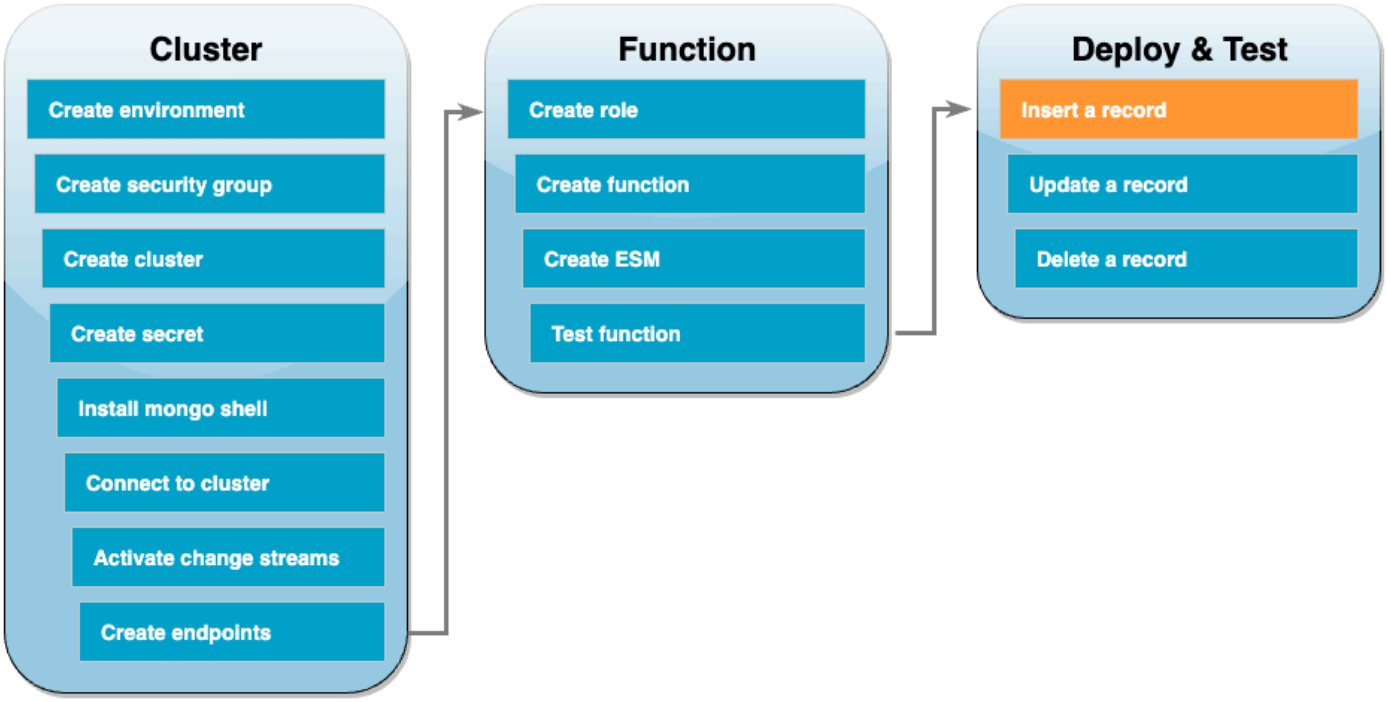
Sie können überprüfen, ob Ihre Funktion das Ereignis erfolgreich verarbeitet hat, indem Sie die Option CloudWatch Logs überprüfen.

Um den manuellen Aufruf über CloudWatch Logs zu überprüfen

1. Öffnen Sie die Seite Funktionen in der Lambda-Konsole.

2. Wählen Sie die Registerkarte „Überwachen“ und anschließend „ CloudWatch Protokolle anzeigen“. Dadurch gelangen Sie zu der spezifischen Protokollgruppe, die Ihrer Funktion in der CloudWatch Konsole zugeordnet ist.
3. Wählen Sie den neuesten Protokollstreams aus. In den Protokollnachrichten sollten Sie die Ereignis-JSON sehen.

Testen Sie Ihre Funktion – fügen Sie einen Datensatz ein



Testen Sie Ihr end-to-end Setup, indem Sie direkt mit Ihrer DocumentDB-Datenbank interagieren. In den nächsten Schritten fügen Sie einen Datensatz ein, aktualisieren ihn und löschen ihn dann.

Um einen Datensatz einzufügen

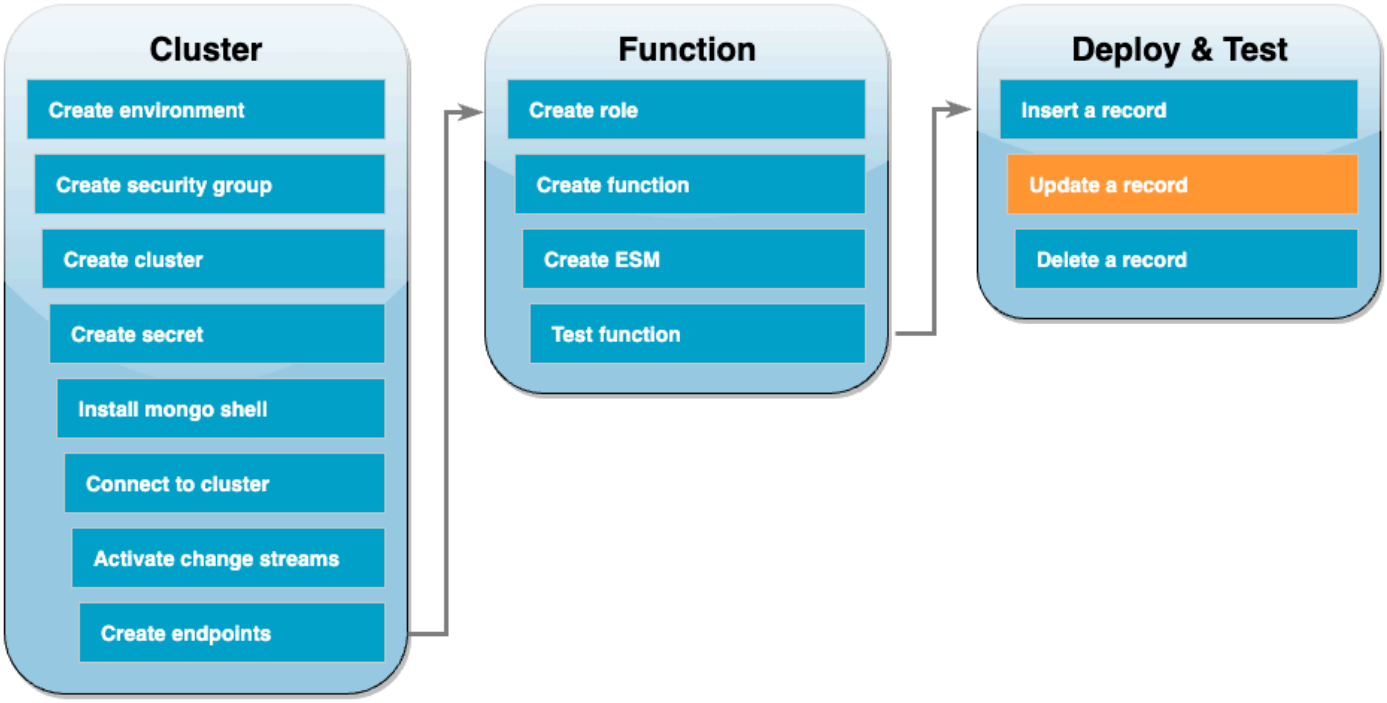
1. Stellen Sie erneut eine Verbindung zu Ihrem DocumentDB-Cluster in Ihrer Cloud9-Umgebung her.
2. Verwenden Sie diesen Befehl, um sicherzustellen, dass Sie gerade die `docdbdemo`-Datenbank verwenden:

```
use docdbdemo
```

3. Fügen Sie einen Datensatz in die `products`-Sammlung der `docdbdemo`-Datenbank ein:

```
db.products.insert({"name":"Pencil", "price": 1.00})
```

Testen Sie Ihre Funktion – aktualisieren Sie einen Datensatz

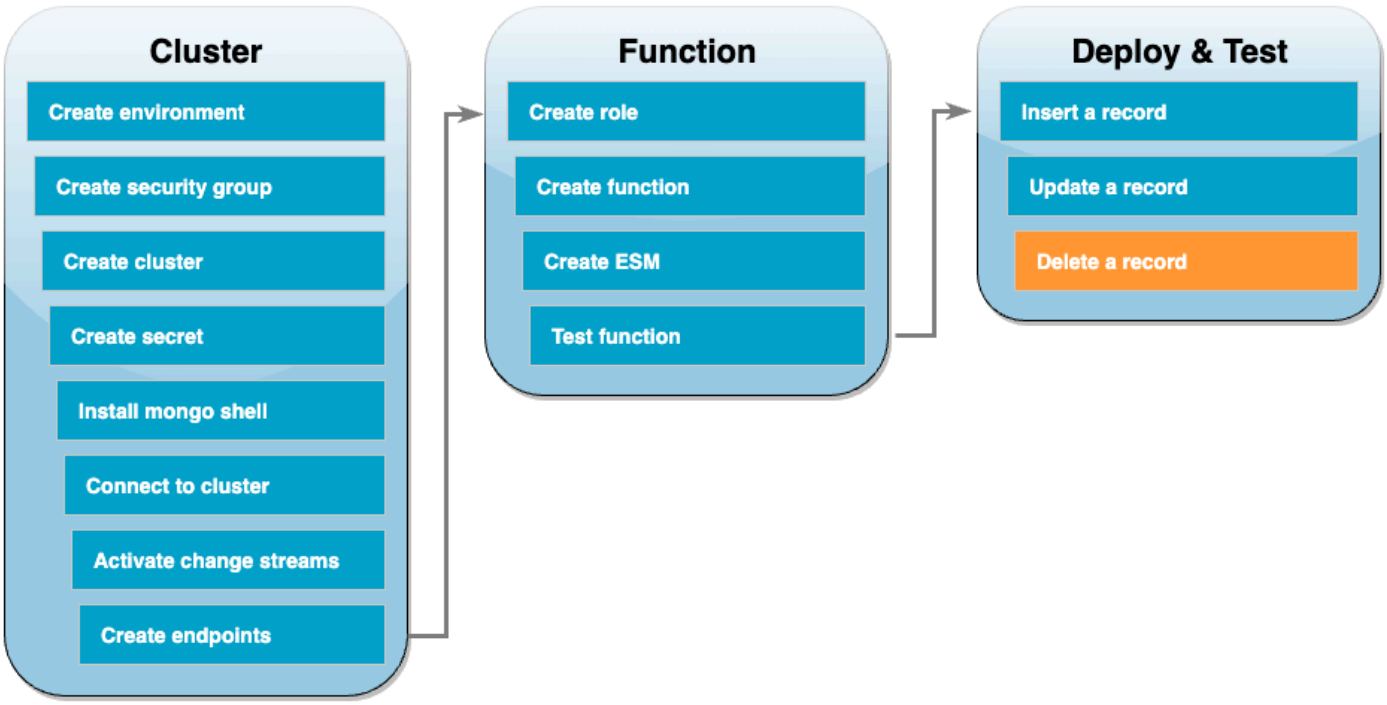


Aktualisieren Sie als Nächstes den gerade eingefügten Datensatz mit dem folgenden Befehl:

```
db.products.update(
    { "name": "Pencil" },
    { $set: { "price": 0.50 }}
)
```

Überprüfen Sie anhand von CloudWatch Logs, ob Ihre Funktion dieses Ereignis erfolgreich verarbeitet hat.

Testen Sie Ihre Funktion – löschen Sie einen Datensatz



Löschen Sie schließlich den Datensatz, den Sie gerade aktualisiert haben, mit dem folgenden Befehl:

```
db.products.remove( { "name": "Pencil" } )
```

Überprüfen Sie anhand von CloudWatch Logs, ob Ihre Funktion dieses Ereignis erfolgreich verarbeitet hat.

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS -Ressourcen, die Sie nicht mehr verwenden, können Sie verhindern, dass unnötige Gebühren in Ihrem AWS-Konto-Konto anfallen.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

Löschen von VPC-Endpunkten

1. Öffnen Sie die VPC;-Konsole. Wählen Sie im linken Menü unter Virtual Private Cloud die Option Endpunkte aus.
2. Wählen Sie die Endpunkte aus, die Sie erstellt haben.
3. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
4. Geben Sie **`delete`** in das Texteingabefeld ein.
5. Wählen Sie Löschen aus.

So löschen Sie den Amazon DocumentDB-Cluster

1. Öffnen Sie die DocumentDB-Konsole.
2. Wählen Sie den DocumentDB-Cluster aus, den Sie für dieses Tutorial erstellt haben, und deaktivieren Sie den Löschschutz.
3. Wählen Sie auf der Cluster-Hauptseite erneut Ihren DocumentDB-Cluster aus.
4. Wählen Sie Aktionen, Löschen aus.
5. Wählen Sie für Finalen Cluster-Snapshot erstellen die Option Nein aus.
6. Geben Sie **`delete`** in das Texteingabefeld ein.
7. Wählen Sie Löschen aus.

So löschen Sie das Secret im Secrets Manager

1. Öffnen Sie die Secrets Manager-Konsole.
2. Wählen Sie das Secret aus, das Sie für dieses Tutorial erstellt haben.
3. Wählen Sie Aktionen, Secret löschen.
4. Wählen Sie Schedule deletion.

Löschen einer Amazon-EC2-Sicherheitsgruppe

1. Öffnen Sie die EC2-Konsole. Wählen Sie unter Netzwerk und Sicherheit die Option Sicherheitsgruppen aus.
2. Wählen Sie die Sicherheitsgruppe, die Sie für dieses Tutorial erstellt haben.
3. Wählen Sie Aktionen, Sicherheitsgruppen löschen.
4. Wählen Sie Löschen aus.

Um die Cloud9-Umgebung zu löschen

1. Öffnen Sie die Cloud9-Konsole.
2. Wählen Sie die Umgebung aus, die Sie für dieses Tutorial erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein.
5. Wählen Sie Löschen.

Lambda-Ereignisfilterung

Sie können die Ereignisfilterung verwenden, um zu steuern, welche Datensätze aus einem Stream oder einer Warteschlange Lambda an Ihre Funktion sendet. Sie können zum Beispiel einen Filter hinzufügen, damit Ihre Funktion nur Amazon-SQS-Nachrichten verarbeitet, die bestimmte Datenparameter enthalten. Die Ereignisfilterung funktioniert mit der Zuordnung von Ereignisquellen. Sie können Filter zu Ereignisquellenzuordnungen für die folgenden AWS Dienste hinzufügen:

- Amazon-DynamoDB
- Amazon-Kinesis-Data-Streams
- Amazon MQ
- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- Selbstverwaltetes Apache Kafka
- Amazon-Simple-Queue-Service (Amazon SQS)

Lambda unterstützt keine Ereignisfilterung für Amazon DocumentDB.

Standardmäßig können Sie bis zu fünf verschiedene Filter für eine einzelne Zuordnung von Ereignisquellen definieren. Ihre Filter sind logisch via OR verknüpft. Wenn ein Datensatz aus Ihrer

Ereignisquelle einen oder mehrere Ihrer Filter erfüllt, nimmt Lambda den Datensatz in das nächste Ereignis auf, das es an Ihre Funktion sendet. Wenn keiner Ihrer Filter erfüllt ist, verwirft Lambda den Datensatz.

> **Note**
>
> Wenn Sie mehr als fünf Filter für eine Ereignisquelle definieren müssen, können Sie eine Kontingenterhöhung auf bis zu 10 Filter für jede Ereignisquelle beantragen. Wenn Sie versuchen, mehr Filter hinzuzufügen, als Ihr aktuelles Kontingent erlaubt, wird Lambda einen Fehler zurückgeben, wenn Sie versuchen, die Ereignisquelle zu erstellen.

Themen

Grundlagen der Ereignisfilterung

Ein Filterkriterienobjekt (`FilterCriteria`) ist eine Struktur, die aus einer Liste von Filtern (`Filters`) besteht. Jeder Filter ist eine Struktur, die ein Ereignisfiltermuster (`Pattern`) definiert. Ein Muster ist eine Zeichenkette, die eine JSON-Filterregel darstellt. Die Struktur eines `FilterCriteria`-Objekts ist wie folgt.

```
{
   "Filters": [
```

```
        {
            "Pattern": "{ \"Metadata1\": [ rule1 ], \"data\": { \"Data1\":
 [ rule2 ] }}"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "Metadata1": [ rule1 ],
    "data": {
        "Data1": [ rule2 ]
    }
}
```

Ihr Filtermuster kann Metadateneigenschaften, Dateneigenschaften oder beides enthalten. Die verfügbaren Metadatenparameter und das Format der Datenparameter variieren je nachdem, AWS-Service welche Person als Ereignisquelle fungiert. Nehmen wir zum Beispiel an, dass Ihre Zuordnung von Ereignisquellen den folgenden Datensatz von einer Amazon-SQS-Warteschlange empfängt:

```
{
    "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
    "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
    "body": "{\n "City": "Seattle",\n "State": "WA",\n "Temperature": "46"\n}",
    "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOLO23YVJ4VO",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
    },
    "messageAttributes": {},
    "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-east-2:123456789012:my-queue",
    "awsRegion": "us-east-2"
}
```

- Metadateneigenschaften sind die Felder, die Informationen über das Ereignis enthalten, das den Datensatz erstellt hat. Im Beispiel für den Amazon-SQS-Datensatz umfassen die Metadateneigenschaften Felder wie `messageID`, `eventSourceArn` und `awsRegion`.

- Dateneigenschaften sind die Felder des Datensatzes, die die Daten aus Ihrem Stream oder Ihrer Warteschlange enthalten. Im Amazon-SQS-Ereignisbeispiel ist der Schlüssel für das Datenfeld `body`, und die Dateneigenschaften sind die Felder `City`, `State` und `Temperature`.

Verschiedene Arten von Ereignisquellen verwenden unterschiedliche Schlüsselwerte für ihre Datenfelder. Um nach Dateneigenschaften zu filtern, müssen sie den richtigen Schlüssel in Ihrem Filtermuster verwenden. Eine Liste der Datenfilterschlüssel und Beispiele für Filtermuster für die einzelnen unterstützten AWS-Service Schlüssel finden Sie unterVerwenden von Filtern mit unterschiedlichen AWS-Services.

Die Ereignisfilterung kann mehrstufige JSON-Filterung verarbeiten. Betrachten Sie zum Beispiel das folgende Fragment eines Datensatzes aus einem DynamoDB-Stream:

```
"dynamodb": {
    "Keys": {
        "ID": {
            "S": "ABCD"
        }
        "Number": {
            "N": "1234"
    },
    ...
}
```

Angenommen, Sie möchten nur die Datensätze verarbeiten, bei denen die `Number` des Sortierschlüssels 4567 ist. In diesem Fall würde Ihr `FilterCriteria`-Objekt wie folgt aussehen:

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\": { \"Keys\": { \"Number\": { \"N\":
 [ "4567" ] } } } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "dynamodb": {
```

```
        "Keys": {
            "Number": {
                "N": [ "4567" ]
                }
            }
        }
}
```

Umgang mit Datensätzen, die die Filterkriterien nicht erfüllen

Die Art und Weise, wie Datensätze behandelt werden, die Ihrem Filter nicht entsprechen, hängt von der Ereignisquelle ab.

- Bei Amazon SQS entfernt Lambda die Nachricht automatisch aus der Warteschlange, wenn die Nachricht Ihren Filterkriterien nicht entspricht. Sie müssen diese Nachrichten in Amazon SQS nicht manuell löschen.
- Bei Kinesis und DynamoDB geht der Stream-Iterator über einen Datensatz hinaus, sobald Ihre Filterkriterien einen Datensatz verarbeiten. Wenn der Datensatz Ihre Filterkriterien nicht erfüllt, müssen Sie den Datensatz nicht manuell aus Ihrer Ereignisquelle löschen. Nach Ablauf der Aufbewahrungsfrist löschen Kinesis und DynamoDB diese alten Datensätze automatisch. Wenn Sie möchten, dass Datensätze früher gelöscht werden, lesen Sie Ändern des Zeitraums der Datenaufbewahrung.
- Bei Amazon MSK-, selbstverwalteten Apache-Kafka- und Amazon MQ-Nachrichten verwirft Lambda Nachrichten, die nicht allen im Filter enthaltenen Feldern entsprechen. Bei selbstverwaltetem Apache Kafka schreibt Lambda Offsets für übereinstimmende und nicht übereinstimmende Nachrichten fest, nachdem die Funktion erfolgreich aufgerufen wurde. Bei Amazon MQ bestätigt Lambda übereinstimmende Nachrichten nach erfolgreichem Aufruf der Funktion und bestätigt nicht übereinstimmende Nachrichten beim Filtern.

Filterregelsyntax

Für Filterregeln unterstützt Lambda die EventBridge Amazon-Regeln und verwendet dieselbe Syntax wie EventBridge. Weitere Informationen finden Sie unter Amazon EventBridge Event Patterns im EventBridge Amazon-Benutzerhandbuch.

Im Folgenden finden Sie eine Zusammenfassung aller Vergleichsoperatoren, die für die Lambda-Ereignisfilterung verfügbar sind.

Vergleichsoperator	Beispiel	Regelsyntax
Null	UserID is null	"UserID": [null]
Leer	LastName ist leer	"LastName": [""]
Gleichheitszeichen	Name is "Alice"	"Name": ["Alice"]
Gleich (Groß-/Kleinschreibung ignorieren)	Name is "Alice"	„Name“: [{"equals-ignore-case„: „Alice“}]
And	Location is "New York" and Day is "Monday"	"Location": ["New York"], "Day": ["Monday"]
Oder	PaymentType ist „Kredit“ oder „Lastschrift“	"PaymentType„: [„Kredit“, „Lastschrift"]
Oder (mehrere Felder)	Location is "New York", or Day is "Monday".	"$or": [{ "Location": ["New York"] }, { "Day": ["Monday"] }]
Nicht	Weather is anything but "Raining"	"Weather": [{ "anything-but": ["Raining"] }]
Numeric (equals)	Price is 100	"Price": [{ "numeric": ["=", 100] }]
Numeric (range)	Price is more than 10, and less than or equal to 20	"Price": [{ "numeric": [">", 10, "<=", 20] }]
Vorhanden	ProductName existiert	"ProductName„: [{„existiert“: wahr}]
Nicht vorhanden	ProductName existiert nicht	"ProductName„: [{„existiert“: falsch}]
Beginnt mit	Region is in the US	"Region": [{"prefix": "us-" }]
Endet mit	FileName endet mit der Erweiterung.png.	"FileName„: [{„Suffix“: „.png“}]

> **Note**
>
> Wie bei EventBridge Zeichenketten verwendet Lambda den exakten character-by-character Abgleich ohne Umschaltung der Groß- und Kleinschreibung oder eine andere Normalisierung von Zeichenketten. Bei Zahlen verwendet Lambda auch eine Zeichenfolgendarstellung. 300, 300,0 und 3,0e2 werden z. B. nicht gleich behandelt.

Beachten Sie, dass der Exists-Operator nur für Blattknoten in Ihrer JSON-Ereignisquelle funktioniert. Er entspricht nicht den Zwischenknoten. Bei der folgenden JSON-Datei `{ "person": { "address": [ { "exists": true } ] } }` würde das Filtermuster beispielsweise keine Übereinstimmung finden, da es sich um einen Zwischenknoten `"address"` handelt.

```
{
  "person": {
    "name": "John Doe",
    "age": 30,
    "address": {
      "street": "123 Main St",
      "city": "Anytown",
      "country": "USA"
    }
  }
}
```

Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole)

Führen Sie diese Schritte aus, um eine neue Ereignisquellenzuordnung mit Filterkriterien über die Lambda-Konsole zu erstellen.

Eine neue Ereignisquellenzuordnung mit Filterkriterien erstellen (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus, für die eine Ereignisquellenzuordnung erstellt werden soll.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).

4. Wählen Sie bei Trigger configuration (Auslöserkonfiguration) einen Auslösertyp aus, der Ereignisfilterung unterstützt. Eine Liste der unterstützten Services finden Sie in der Liste am Anfang dieser Seite.
5. Erweitern Sie Additional settings (Zusätzliche Einstellungen).
6. Wählen Sie unter Filter criteria (Filterkriterien) die Option Add (Hinzufügen) aus und definieren Sie anschließend Ihre Filter. Sie können z. B. Folgendes eingeben.

   ```
   { "Metadata" : [ 1, 2 ] }
   ```

   Damit wird Lambda angewiesen, nur Datensätze zu verarbeiten, in denen das Feld `Metadata` gleich 1 oder 2 ist. Sie können weiterhin Hinzufügen auswählen, um weitere Filter bis zur maximal zulässigen Anzahl hinzuzufügen.
7. Wenn Sie fertig mit dem Hinzufügen Ihrer Filter sind, klicken Sie auf Speichern.

Wenn Sie Filterkriterien über die Konsole eingeben, geben Sie nur das Filtermuster ein und müssen weder den `Pattern`-Schlüssel noch Escape-Anführungszeichen angeben. In Schritt 6 der Anweisungen oben entspricht `{ "Metadata" : [ 1, 2 ] }` den folgenden `FilterCriteria`.

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
      }
   ]
}
```

Nachdem Sie Ihre Ereignisquellenzuordnung in der Konsole erstellt haben, sehen Sie die formatierten `FilterCriteria` in den Auslöserdetails. Weitere Beispiele zum Erstellen von Ereignisfiltern mithilfe der -Konsole finden Sie unter Verwenden von Filtern mit unterschiedlichen AWS-Services.

Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (AWS CLI)

Angenommen, Sie möchten, dass eine Ereignisquellenzuordnung folgende hat `FilterCriteria`:

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
```

```
      }
   ]
}
```

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ]}"}]}'
```

Dieser create-event-source-mappingBefehl erstellt eine neue Amazon SQS SQS-Ereignisquellenzuordnung für eine Funktion `my-function` mit dem angegebenen `FilterCriteria` Wert.

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"Metadata\" : [ 1, 2 ]}"}]}'
```

Beachten Sie, dass Sie zum Aktualisieren einer Ereignisquellenzuordnung ihre UUID benötigen. Sie können die UUID aus einem Anruf abrufen. list-event-source-mappings Lambda gibt auch die UUID in der CLI-Antwort zurück. create-event-source-mapping

Um Filterkriterien aus einer Ereignisquelle zu entfernen, können Sie den folgenden update-event-source-mappingBefehl mit einem leeren Objekt ausführen. `FilterCriteria`

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria "{}"
```

Weitere Beispiele für das Erstellen von Ereignisfiltern mithilfe von finden Sie unterVerwenden von Filtern mit unterschiedlichen AWS-Services. AWS CLI

Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (AWS SAM)

Angenommen, Sie möchten eine Ereignisquelle so konfigurieren AWS SAM , dass sie die folgenden Filterkriterien verwendet:

```
{
   "Filters": [
      {
          "Pattern": "{ \"Metadata\" : [ 1, 2 ] }"
      }
   ]
}
```

Um diese Filterkriterien zu Ihrer Zuordnung von Ereignisquellen hinzuzufügen, fügen Sie das folgende Snippet in die YAML-Vorlage für Ihre Ereignisquelle ein.

```
FilterCriteria:
  Filters:
    - Pattern: '{"Metadata": [1, 2]}'
```

Weitere Informationen zum Erstellen und Konfigurieren einer AWS SAM Vorlage für eine Ereignisquellenzuordnung finden Sie im EventSourceAbschnitt des AWS SAM Entwicklerhandbuchs. Weitere Beispiele für die Erstellung von Ereignisfiltern mithilfe von AWS SAM Vorlagen finden Sie unterVerwenden von Filtern mit unterschiedlichen AWS-Services.

Verwenden von Filtern mit unterschiedlichen AWS-Services

Verschiedene Arten von Ereignisquellen verwenden unterschiedliche Schlüsselwerte für ihre Datenfelder. Um nach Dateneigenschaften zu filtern, müssen sie den richtigen Schlüssel in Ihrem Filtermuster verwenden. In der folgenden Tabelle sind die Filterschlüssel für jeden unterstützten Schlüssel aufgeführt AWS-Service.

AWS-Service	Filterschlüssel
DynamoDB	`dynamodb`
Kinesis	`data`
Amazon MQ	`data`
Amazon MSK	`value`
Selbstverwaltetes Apache Kafka	`value`
Amazon SQS	`body`

In den folgenden Abschnitten finden Sie Beispiele für Filtermuster für verschiedene Arten von Ereignisquellen. Sie enthalten auch Definitionen der unterstützten Formate für eingehende Daten und Filtermuster für jeden unterstützten Service.

Filtern mit DynamoDB

Angenommen, Sie haben eine DynamoDB-Tabelle mit dem Primärschlüssel `CustomerName` und den Attributen `AccountManager` und `PaymentTerms`. Im Folgenden sehen Sie einen Beispieldatensatz aus dem Stream Ihrer DynamoDB-Tabelle.

```
{
      "eventID": "1",
      "eventVersion": "1.0",
      "dynamodb": {
          "ApproximateCreationDateTime": "1678831218.0",
          "Keys": {
              "CustomerName": {
                  "S": "AnyCompany Industries"
              },
              "NewImage": {
                  "AccountManager": {
                      "S": "Pat Candella"
                  },
                  "PaymentTerms": {
                      "S": "60 days"
                  },
                  "CustomerName": {
                      "S": "AnyCompany Industries"
                  }
              },
              "SequenceNumber": "111",
              "SizeBytes": 26,
              "StreamViewType": "NEW_IMAGE"
          }
      }
  }
```

Um anhand der Schlüssel- und Attributwerte in Ihrer DynamoDB-Tabelle zu filtern, verwenden Sie den `dynamodb`-Schlüssel im Datensatz. Die folgenden Abschnitte enthalten Beispiele für verschiedene Filtertypen.

Filtern mit Tabellenschlüsseln

Angenommen, Sie möchten, dass Ihre Funktion nur die Datensätze verarbeitet, bei denen der Primärschlüssel „AnyCompany Branchen“ `CustomerName` lautet. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
     "Filters": [
          {
              "Pattern": "{ \"dynamodb\" : { \"Keys\" : { \"CustomerName\" : { \"S\" :
 [ \"AnyCompany Industries\" ] } } } }"
          }
      ]
 }
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
     "dynamodb": {
          "Keys": {
              "CustomerName": {
                  "S": [ "AnyCompany Industries" ]
                  }
              }
          }
 }
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer AWS SAM Vorlage hinzufügen.

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany
 Industries" ] } } } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" :
 { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"Keys\" :
 { \"CustomerName\" : { \"S\" : [ \"AnyCompany Industries\" ] } } } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
   Filters:
     - Pattern: '{ "dynamodb" : { "Keys" : { "CustomerName" : { "S" : [ "AnyCompany
 Industries" ] } } } }'
```

Filtern mit Tabellenattributen

Mit DynamoDB können Sie auch die Schlüssel `NewImage` und `OldImage` verwenden, um nach Attributwerten zu filtern. Angenommen, Sie möchten Datensätze filtern, bei denen das `AccountManager`-Attribut im letzten Tabellenbild "Pat Candella" oder "Shirley Rodriguez" lautet. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S
\" : [ \"Pat Candella\", \"Shirley Rodriguez\" ] } } } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "dynamodb": {
        "NewImage": {
            "AccountManager": {
                "S": [ "Pat Candella", "Shirley Rodriguez" ]
            }
        }
    }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer AWS SAM Vorlage hinzufügen.

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat Candella",
 "Shirley Rodriguez" ] } } } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez
\" ] } } } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
```

```
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\", \"Shirley Rodriguez
\" ] } } } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella", "Shirley Rodriguez" ] } } } }'
```

Filtern mit booleschen Ausdrücken

Sie können Filter auch mithilfe von booleschen UND-Ausdrücken erstellen. Diese Ausdrücke können sowohl die Schlüssel- als auch die Attributparameter Ihrer Tabelle enthalten. Angenommen, Sie möchten Datensätze filtern, bei denen der `NewImage`-Wert von `AccountManager` „Pat Candella“ und der `OldImage`-Wert „Terry Whitlock“ ist. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"dynamodb\" : { \"NewImage\" : { \"AccountManager\" : { \"S
\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" : { \"OldImage\" : { \"AccountManager
\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "dynamodb" : {
        "NewImage" : {
            "AccountManager" : {
                "S" : [
                    "Pat Candella"
```

```
                ]
            }
        }
    },
    "dynamodb": {
        "OldImage": {
            "AccountManager": {
                "S": [
                    "Terry Whitlock"
                ]
            }
        }
    }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer AWS SAM Vorlage hinzufügen.

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" :
 [ "Terry Whitlock" ] } } } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:dynamodb:us-east-2:123456789012:table/my-table \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" :
 { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }
 "}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"dynamodb\" : { \"NewImage
\" : { \"AccountManager\" : { \"S\" : [ \"Pat Candella\" ] } } } , \"dynamodb\" :
 { \"OldImage\" : { \"AccountManager\" : { \"S\" : [ \"Terry Whitlock\" ] } } } }
 "}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "dynamodb" : { "NewImage" : { "AccountManager" : { "S" : [ "Pat
 Candella" ] } } } , "dynamodb" : { "OldImage" : { "AccountManager" : { "S" :
 [ "Terry Whitlock" ] } } } }'
```

> **Note**
>
> Die DynamoDB-Ereignisfilterung unterstützt nicht die Verwendung von numerischen Operatoren (numerisch gleich und numerisch Bereich). Auch wenn Elemente in Ihrer Tabelle als Zahlen gespeichert sind, werden diese Parameter im JSON-Datensatzobjekt in Strings umgewandelt.

Verwenden des Exists-Operators mit DynamoDB

Aufgrund der Art und Weise, wie JSON-Ereignisobjekte von DynamoDB strukturiert sind, erfordert die Verwendung des Exists-Operators besondere Vorsicht. Der Exists-Operator funktioniert nur für Blattknoten im Event-JSON. Wenn Ihr Filtermuster also Exists verwendet, um nach einem Zwischenknoten zu testen, funktioniert er nicht. Betrachten Sie das folgende DynamoDB-Tabellenelement:

```
{
  "UserID": {"S": "12345"},
  "Name": {"S": "John Doe"},
  "Organizations": {"L": [
      {"S":"Sales"},
```

```
      {"S":"Marketing"},
      {"S":"Support"}
    ]
  }
}
```

Möglicherweise möchten Sie ein Filtermuster wie das folgende erstellen, das auf Ereignisse prüft, die Folgendes enthalten: `"Organizations"`

```
{ "dynamodb" : { "NewImage" : { "Organizations" : [ { "exists": true } ] } } }
```

Dieses Filtermuster würde jedoch niemals eine Übereinstimmung zurückgeben, da `"Organizations"` es sich nicht um einen Blattknoten handelt. Das folgende Beispiel zeigt, wie der Exists-Operator richtig verwendet wird, um das gewünschte Filtermuster zu erstellen:

```
{ "dynamodb" : { "NewImage" : {"Organizations": {"L": {"S": [ {"exists":
 true } ] } } } } }
```

JSON-Format für DynamoDB-Filterung

Um Ereignisse aus DynamoDB-Quellen richtig zu filtern, müssen sowohl das Datenfeld als auch Ihre Filterkriterien für das Datenfeld (`dynamodb`) im gültigen JSON-Format vorliegen. Wenn eines der Felder kein gültiges JSON-Format hat, verwirft Lambda die Nachricht oder gibt eine Ausnahme aus. In der folgenden Tabelle ist das Verhalten zusammengefasst:

Format der eingehenden Daten	Filtermusterformat für Dateneigenschaften	Resultierende Aktion
Gültiges JSON	Gültiges JSON	Lambda filtert basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein JSON	Lambda gibt zum Zeitpunkt der Erstellung oder Aktualisi

Format der eingehenden Daten	Filtermusterformat für Dateneigenschaften	Resultierende Aktion
		erung der Ereignisquellenzuordnung eine Ausnahme aus. Das Filtermuster für Dateneigenschaften muss ein gültiges JSON-Format haben.
Kein JSON	Gültiges JSON	Lambda verwirft den Datensatz.
Kein JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Kein JSON	Kein JSON	Lambda gibt zum Zeitpunkt der Erstellung oder Aktualisierung der Ereignisquellenzuordnung eine Ausnahme aus. Das Filtermuster für Dateneigenschaften muss ein gültiges JSON-Format haben.

Filtern mit Kinesis

Angenommen, ein Producer gibt JSON-formatierte Daten in Ihren Kinesis-Datenstrom ein. Ein Beispieldatensatz würde wie folgt aussehen, wobei die JSON-Daten im `data`-Feld in eine Base64-kodierte Zeichenfolge umgewandelt wurden.

```
{
    "kinesis": {
        "kinesisSchemaVersion": "1.0",
        "partitionKey": "1",
        "sequenceNumber": "49590338271490256608559692538361571095921575989136588898",
        "data":
 "eyJSZWNvcmROdW1iZXIiOiAiMDAwMSIsICJUaW1lU3RhbXAiOiAieXl5eS1tbS1kZFRoaDptbTpzcyIsICJSZXF1ZXN0Q
        "approximateArrivalTimestamp": 1545084650.987
```

```
        },
    "eventSource": "aws:kinesis",
    "eventVersion": "1.0",
    "eventID":
 "shardId-000000000006:49590338271490256608559692538361571095921575989136588898",
    "eventName": "aws:kinesis:record",
    "invokeIdentityArn": "arn:aws:iam::123456789012:role/lambda-role",
    "awsRegion": "us-east-2",
    "eventSourceARN": "arn:aws:kinesis:us-east-2:123456789012:stream/lambda-stream"
}
```

Solange die Daten, die der Producer in den Stream einspeist, als JSON gültig sind, können Sie die Ereignisfilterung verwenden, um Datensätze anhand des `data`-Schlüssels zu filtern. Nehmen wir an, ein Produzent gibt Datensätze im folgenden JSON-Format in Ihren Kinesis-Stream ein.

```
{
    "record": 12345,
    "order": {
        "type": "buy",
        "stock": "ANYCO",
        "quantity": 1000
        }
}
```

Um nur die Datensätze zu filtern, bei denen der Auftragstyp "Kaufen" ist, würde das `FilterCriteria`-Objekt wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : { \"order\" : { \"type\" : [ \"buy\" ] } } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "data": {
        "order": {
            "type": [ "buy" ]
```

```
            }
        }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer AWS SAM Vorlage hinzufügen.

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "data" : { "order" : { "type" : [ "buy" ] } } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kinesis:us-east-2:123456789012:stream/my-stream \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type
\" : [ \"buy\" ] } } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"order\" : { \"type
\" : [ \"buy\" ] } } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
```

```
Filters:
  - Pattern: '{ "data" : { "order" : { "type" : [ "buy" ] } } }'
```

Um Ereignisse aus Kinesis-Quellen ordnungsgemäß zu filtern, müssen sowohl das Datenfeld als auch die Filterkriterien für das Datenfeld ein gültiges JSON-Format aufweisen. Wenn eines der Felder kein gültiges JSON-Format hat, verwirft Lambda die Nachricht oder gibt eine Ausnahme aus. In der folgenden Tabelle ist das Verhalten zusammengefasst:

Format der eingehenden Daten	Filtermusterformat für Dateneigenschaften	Resultierende Aktion
Gültiges JSON	Gültiges JSON	Lambda filtert basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein JSON	Lambda gibt zum Zeitpunkt der Erstellung oder Aktualisierung der Ereignisquellenzuordnung eine Ausnahme aus. Das Filtermuster für Dateneigenschaften muss ein gültiges JSON-Format haben.
Kein JSON	Gültiges JSON	Lambda verwirft den Datensatz.
Kein JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Kein JSON	Kein JSON	Lambda gibt zum Zeitpunkt der Erstellung oder Aktualisierung der Ereignisquellenzuo

Format der eingehenden Daten	Filtermusterformat für Dateneigenschaften	Resultierende Aktion
		rdnung eine Ausnahme aus. Das Filtermuster für Dateneige nschaften muss ein gültiges JSON-Format haben.

Filtern von aggregierten Kinesis-Datensätzen

Mit Kinesis können Sie mehrere Datensätze in einem einzigen Kinesis-Datenstrom-Datensatz zusammenfassen, um Ihren Datendurchsatz zu erhöhen. Lambda kann Filterkriterien nur auf aggregierte Datensätze anwenden, wenn Sie Kinesis Enhanced Fanout verwenden. Das Filtern aggregierter Datensätze mit Standard-Kinesis wird nicht unterstützt. Bei der Verwendung von Enhanced Fan-Out konfigurieren Sie einen dedizierten Kinesis-Durchsatzverbraucher, der als Auslöser für Ihre Lambda-Funktion dient. Lambda filtert dann die aggregierten Datensätze und übergibt nur die Datensätze, die Ihren Filterkriterien entsprechen.

Weitere Informationen zur Aggregation von Kinesis-Datensätzen finden Sie im Abschnitt Aggregation auf der Seite mit den wichtigsten Konzepten der Kinesis Producer Library (KPL). Weitere Informationen zur Verwendung von Lambda mit Kinesis Enhanced Fan-Out finden Sie im Compute-Blog unter Steigerung der Echtzeit-Stream-Verarbeitungsleistung mit Amazon Kinesis Data Streams Enhanced Fan-Out und AWS Lambda. AWS

Filtern mit Amazon MQ

Angenommen, Ihre Amazon-MQ-Nachrichtenwarteschlange enthält Nachrichten entweder im gültigen JSON-Format oder als einfache Zeichenfolgen. Ein Beispieldatensatz würde wie folgt aussehen, wobei die Daten im `data`-Feld in eine Base64-kodierte Zeichenfolge umgewandelt wurden.

ActiveMQ

```
{
    "messageID": "ID:b-9bcfa592-423a-4942-879d-eb284b418fc8-1.mq.us-
west-2.amazonaws.com-37557-1234520418293-4:1:1:1:1",
    "messageType": "jms/text-message",
    "deliveryMode": 1,
    "replyTo": null,
    "type": null,
```

```
    "expiration": "60000",
    "priority": 1,
    "correlationId": "myJMSCoID",
    "redelivered": false,
    "destination": {
      "physicalName": "testQueue"
    },
    "data":"QUJDOkFBQUE=",
    "timestamp": 1598827811958,
    "brokerInTime": 1598827811958,
    "brokerOutTime": 1598827811959,
    "properties": {
      "index": "1",
      "doAlarm": "false",
      "myCustomProperty": "value"
    }
}
```

RabbitMQ

```
{
    "basicProperties": {
        "contentType": "text/plain",
        "contentEncoding": null,
        "headers": {
            "header1": {
                "bytes": [
                  118,
                  97,
                  108,
                  117,
                  101,
                  49
                ]
            },
            "header2": {
                "bytes": [
                  118,
                  97,
                  108,
                  117,
                  101,
```

```
                    50
                ]
            },
            "numberInHeader": 10
        },
        "deliveryMode": 1,
        "priority": 34,
        "correlationId": null,
        "replyTo": null,
        "expiration": "60000",
        "messageId": null,
        "timestamp": "Jan 1, 1970, 12:33:41 AM",
        "type": null,
        "userId": "AIDACKCEVSQ6C2EXAMPLE",
        "appId": null,
        "clusterId": null,
        "bodySize": 80
        },
    "redelivered": false,
    "data": "eyJ0aW1lb3V0IjowLCJkYXRhIjoiQ1pybWYwR3c4T3Y0YnFMUXhENEUifQ=="
}
```

Sowohl für Active MQ- als auch für Rabbit MQ-Broker können Sie die Ereignisfilterung verwenden, um Datensätze anhand des `data`-Schlüssels zu filtern. Angenommen, Ihre Amazon-MQ-Warteschlange enthält Nachrichten im folgenden JSON-Format.

```
{
    "timeout": 0,
    "IPAddress": "203.0.113.254"
}
```

Um nur die Datensätze zu filtern, bei denen das `timeout`-Feld größer als 0 ist, würde das `FilterCriteria`-Objekt wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : { \"timeout\" : [ { \"numeric\": [ \">\",
 0] } } ] } }"
        }
```

```
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "data": {
        "timeout": [ { "numeric": [ ">", 0 ] } ]
        }
}
```

Sie können Ihren Filter mithilfe der Konsole oder einer Vorlage hinzufügen. AWS CLI AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :
 [ { \"numeric\": [ \">\", 0 ] } ] } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : { \"timeout\" :
 [ { \"numeric\": [ \">\", 0 ] } ] } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "data" : { "timeout" : [ { "numeric": [ ">", 0 ] } ] } }'
```

Mit Amazon MQ können Sie auch Datensätze filtern, bei denen die Nachricht eine einfache Zeichenfolge ist. Angenommen, Sie möchten nur Datensätze verarbeiten, bei denen die Meldung mit „Ergebnis:“ beginnt. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"data\" : [ { \"prefix\": \"Result: \" } ] }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "data": [
        {
        "prefix": "Result: "
        }
    ]
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer Vorlage hinzufügen. AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "data" : [ { "prefix": "Result: " } ] }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:mq:us-east-2:123456789012:broker:my-
broker:b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":
 \"Result: \" } ] }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"data\" : [ { \"prefix\":
 \"Result: \" } ] }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "data" : [ { "prefix": "Result " } ] }'
```

Amazon-MQ-Nachrichten müssen UTF-8-kodierte Zeichenfolgen sein (entweder einfache Zeichenfolgen oder im JSON-Format). Das liegt daran, dass Lambda Byte-Arrays von Amazon MQ vor Anwendung der Filterkriterien in UTF-8 dekodiert. Wenn Ihre Nachrichten eine andere Kodierung nutzen, z. B. UTF-16 oder ASCII, oder das Nachrichtenformat nicht dem `FilterCriteria`-Format entspricht, verarbeitet Lambda nur Metadatenfilter. In der folgenden Tabelle ist das Verhalten zusammengefasst:

-Format der eingehenden Nachricht	Filtermusterformat für Nachrichteneigenschaften	Resultierende Aktion
Einfache Zeichenfolge	Einfache Zeichenfolge	Lambda filtert basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Gültiges JSON	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Einfache Zeichenfolge	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Gültiges JSON	Lambda filtert basierend auf Ihren Filterkriterien.
Nicht UTF-8-kodierte Zeichenfolge	JSON, einfache Zeichenfolge oder kein Muster	Lambda filtert (nur für die anderen Metadateneigenschaften) basierend auf Ihren Filterkriterien.

Filtern mit Amazon MSK und selbstverwaltetem Apache Kafka

Angenommen, ein Producer schreibt Nachrichten zu einem Thema in Ihrem Amazon MSK- oder selbstverwalteten Apache-Kafka-Cluster, entweder im gültigen JSON-Format oder als einfache

Zeichenketten. Ein Beispieldatensatz würde wie folgt aussehen, wobei die Nachricht im `value`-Feld in eine Base64-kodierte Zeichenfolge umgewandelt wurde.

```
{
    "mytopic-0":[
        {
            "topic":"mytopic",
            "partition":0,
            "offset":15,
            "timestamp":1545084650987,
            "timestampType":"CREATE_TIME",
            "value":"SGVsbG8sIHRoaXMgaXMgYSB0ZXN0Lg==",
            "headers":[]
        }
    ]
}
```

Angenommen, Ihr Apache-Kafka-Producer schreibt Nachrichten zu Ihrem Thema im folgenden JSON-Format.

```
{
    "device_ID": "AB1234",
    "session":{
        "start_time": "yyyy-mm-ddThh:mm:ss",
        "duration": 162
    }
}
```

Sie können den `value`-Schlüssel verwenden, um Datensätze zu filtern. Angenommen, Sie möchten nur die Datensätze filtern, bei denen `device_ID` mit den Buchstaben AB beginnen. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"value\" : { \"device_ID\" : [ { \"prefix\": \"AB\" } ] } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "value": {
        "device_ID": [ { "prefix": "AB" } ]
      }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer Vorlage hinzufügen. AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "value" : { "device_ID" : [ { "prefix":  "AB" } ] } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :
 [ { \"prefix\":  \"AB\" } ] } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : { \"device_ID\" :
 [ { \"prefix\":  \"AB\" } ] } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : { "device_ID" : [ { "prefix":  "AB" } ] } }'
```

Mit Amazon MQ und selbstverwaltetem Apache Kafka können Sie auch Datensätze filtern, bei denen die Nachricht eine einfache Zeichenfolge ist. Angenommen, Sie möchten die Meldungen ignorieren, in denen die Zeichenfolge „error“ ist. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"value\" : [ { \"anything-but\": [ \"error\" ] } ] }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "value": [
        {
        "anything-but": [ "error" ]
        }
    ]
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer Vorlage hinzufügen. AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "value" : [ { "anything-but": [ "error" ] } ] }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:kafka:us-east-2:123456789012:cluster/my-cluster/
b-8ac7cc01-5898-482d-be2f-a6b596050ea8 \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":
 [ \"error\" ] } ] }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"value\" : [ { \"anything-but\":
 [ \"error\" ] } ] }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "value" : [ { "anything-but": [ "error" ] } ] }'
```

Amazon MSK- und selbstverwaltete Apache-Kafka-Nachrichten müssen UTF-8-kodierte Strings sein, entweder einfache Strings oder im JSON-Format. Das liegt daran, dass Lambda Byte-Arrays von Amazon MSK vor Anwendung der Filterkriterien in UTF-8 dekodiert. Wenn Ihre Nachrichten eine andere Kodierung nutzen, z. B. UTF-16 oder ASCII, oder das Nachrichtenformat nicht dem `FilterCriteria`-Format entspricht, verarbeitet Lambda nur Metadatenfilter. In der folgenden Tabelle ist das Verhalten zusammengefasst:

-Format der eingehenden Nachricht	Filtermusterformat für Nachrichteneigenschaften	Resultierende Aktion
Einfache Zeichenfolge	Einfache Zeichenfolge	Lambda filtert basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenscha

-Format der eingehenden Nachricht	Filtermusterformat für Nachrichteneigenschaften	Resultierende Aktion
		ften) basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Gültiges JSON	Lambda filtert (nur für die anderen Metadateneigenscha ften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Einfache Zeichenfolge	Lambda filtert (nur für die anderen Metadateneigenscha ften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenscha ften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Gültiges JSON	Lambda filtert basierend auf Ihren Filterkriterien.
Nicht UTF-8-kodierte Zeichenfolge	JSON, einfache Zeichenfolge oder kein Muster	Lambda filtert (nur für die anderen Metadateneigenscha ften) basierend auf Ihren Filterkriterien.

Filtern mit Amazon SQS

Angenommen, Ihre Amazon-SQS-Warteschlange enthält Nachrichten im folgenden JSON-Format.

```
{
    "RecordNumber": 0000,
    "TimeStamp": "yyyy-mm-ddThh:mm:ss",
    "RequestCode": "AAAA"
}
```

Ein Beispieldatensatz für diese Warteschlange würde wie folgt aussehen.

```
{
    "messageId": "059f36b4-87a3-44ab-83d2-661975830a7d",
    "receiptHandle": "AQEBwJnKyrHigUMZj6rYigCgxlaS3SLy0a...",
    "body": "{\n "RecordNumber": 0000,\n "TimeStamp": "yyyy-mm-ddThh:mm:ss",\n
 "RequestCode": "AAAA"\n}",
    "attributes": {
        "ApproximateReceiveCount": "1",
        "SentTimestamp": "1545082649183",
        "SenderId": "AIDAIENQZJOLO23YVJ4VO",
        "ApproximateFirstReceiveTimestamp": "1545082649185"
        },
    "messageAttributes": {},
    "md5OfBody": "e4e68fb7bd0e697a0ae8f1bb342846b3",
    "eventSource": "aws:sqs",
    "eventSourceARN": "arn:aws:sqs:us-west-2:123456789012:my-queue",
    "awsRegion": "us-west-2"
}
```

Um anhand des Inhalts Ihrer Amazon-SQS-Nachrichten zu filtern, verwenden Sie den `body`-Schlüssel im Amazon-SQS-Nachrichtendatensatz. Angenommen, Sie möchten nur die Datensätze verarbeiten, bei denen `RequestCode` in Ihrer Amazon-SQS-Nachricht „BBBB“ ist. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
    "Filters": [
        {
            "Pattern": "{ \"body\" : { \"RequestCode\" : [ \"BBBB\" ] } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "body": {
        "RequestCode": [ "BBBB" ]
        }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer Vorlage hinzufügen. AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "body" : { "RequestCode" : [ "BBBB" ] } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" :
 [ \"BBBB\" ] } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RequestCode\" :
 [ \"BBBB\" ] } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RequestCode" : [ "BBBB" ] } }'
```

Angenommen, Sie möchten, dass Ihre Funktion nur die Datensätze verarbeitet, bei denen `RecordNumber` größer als 9999 ist. Das `FilterCriteria`-Objekt würde wie folgt aussehen.

```
{
```

```
    "Filters": [
        {
            "Pattern": "{ \"body\" : { \"RecordNumber\" : [ { \"numeric\": [ \">\",
 9999 ] } ] } }"
        }
    ]
}
```

Zur Verdeutlichung sehen Sie hier den Wert des Filter-`Pattern` in reinem JSON.

```
{
    "body": {
        "RecordNumber": [
            {
                "numeric": [ ">", 9999 ]
            }
        ]
    }
}
```

Sie können Ihren Filter mithilfe der Konsole AWS CLI oder einer Vorlage hinzufügen. AWS SAM

Console

Um diesen Filter mithilfe der Konsole hinzuzufügen, folgen Sie den Anweisungen unter Anhängen von Filterkriterien an eine Ereignisquellenzuordnung (Konsole) und geben Sie die folgende Zeichenfolge für die Filterkriterien ein.

```
{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }
```

AWS CLI

Führen Sie den folgenden Befehl aus, um mithilfe von AWS Command Line Interface (AWS CLI) eine neue Ereignisquellenzuordnung mit diesen Filterkriterien zu erstellen.

```
aws lambda create-event-source-mapping \
    --function-name my-function \
    --event-source-arn arn:aws:sqs:us-east-2:123456789012:my-queue \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" :
 [ { \"numeric\": [ \">\", 9999 ] } ] } }"}]}'
```

Führen Sie den folgenden Befehl aus, um diese Filterkriterien zu einer vorhandenen Zuordnung von Ereignisquellen hinzuzufügen.

```
aws lambda update-event-source-mapping \
    --uuid "a1b2c3d4-5678-90ab-cdef-11111EXAMPLE" \
    --filter-criteria '{"Filters": [{"Pattern": "{ \"body\" : { \"RecordNumber\" :
 [ { \"numeric\": [ \">\", 9999 ] } ] } }"}]}'
```

AWS SAM

Um diesen Filter mithilfe hinzuzufügen AWS SAM, fügen Sie der YAML-Vorlage für Ihre Ereignisquelle den folgenden Ausschnitt hinzu.

```
FilterCriteria:
  Filters:
    - Pattern: '{ "body" : { "RecordNumber" : [ { "numeric": [ ">", 9999 ] } ] } }'
```

Für Amazon SQS kann der Nachrichtenkörper eine beliebige Zeichenfolge sein. Dies kann jedoch problematisch sein, wenn die `FilterCriteria` erwarten, dass `body` ein gültiges JSON-Format hat. Umgekehrt gilt dasselbe – wenn der Textkörper der eingehenden Nachricht ein JSON-Format aufweist, die Filterkriterien jedoch erwarten, dass `body` eine einfache Zeichenfolge ist, kann dies zu unbeabsichtigtem Verhalten führen.

Um dieses Problem zu vermeiden, stellen Sie sicher, dass das Körperformat in Ihren `FilterCriteria` mit dem erwarteten Format von `body` in den Nachrichten übereinstimmt, die Sie von Ihrer Warteschlange erhalten. Bevor Sie Ihre Nachrichten filtern, wertet Lambda automatisch das Format des Körpers der eingehenden Nachricht und Ihres Filtermusters für `body` aus. Wenn es keine Übereinstimmung gibt, verwirft Lambda die Nachricht. In der folgenden Tabelle ist diese Auswertung zusammengefasst:

body-Format der eingehenden Nachricht	**body**-Format des Filtermus ters	Resultierende Aktion
Einfache Zeichenfolge	Einfache Zeichenfolge	Lambda filtert basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenscha

body-Format der eingehenden Nachricht	**body**-Format des Filtermus ters	Resultierende Aktion
		ften) basierend auf Ihren Filterkriterien.
Einfache Zeichenfolge	Gültiges JSON	Lambda verwirft die Nachricht.
Gültiges JSON	Einfache Zeichenfolge	Lambda verwirft die Nachricht.
Gültiges JSON	Kein Filtermuster für Dateneigenschaften	Lambda filtert (nur für die anderen Metadateneigenscha ften) basierend auf Ihren Filterkriterien.
Gültiges JSON	Gültiges JSON	Lambda filtert basierend auf Ihren Filterkriterien.

Testen von Lambda-Funktionen mit Hilfe der Konsole

Sie können Ihre Lambda-Funktion in der Konsole testen, indem Sie Ihre Funktion mit einem Testereignis aufrufen. Ein Testereignis ist eine JSON-Eingabe für Ihre Funktion. Wenn Ihre Funktion keine Eingabe erfordert, kann das Ereignis ein leeres Dokument (`{}`) sein.

Wenn Sie einen Test in der Konsole ausführen, ruft Lambda Ihre Funktion synchron mit dem Testereignis auf. Die Funktionslaufzeit konvertiert das Ereignis-JSON in ein Objekt und übergibt es zur Verarbeitung an die Handler-Methode Ihres Codes.

> **Erstellen Sie ein Testereignis**
>
> Bevor Sie in der Konsole testen können, müssen Sie ein privates oder gemeinsam nutzbares Testereignis erstellen.

Aufrufen von Funktionen mit Testereignissen

So testen Sie eine Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Klicken Sie auf den Namen der Funktion, die Sie testen möchten.
3. Wählen Sie die Registerkarte Test.
4. Wählen Sie unter Test event (Testereignis) die Option Create new event (Neues Ereignis erstellen) oder Edit saved event (Gespeichertes Ereignis bearbeiten) und dann das gespeicherte Ereignis aus, das Sie verwenden möchten.
5. Optional — wählen Sie ein Template (Vorlage) für den Event-JSON.
6. Wählen Sie Test aus.
7. Erweitern Sie unter Execution result (Ausführungsergebnis) die Option Details, um die Testergebnisse anzuzeigen.

Um Ihre Funktion aufzurufen, ohne Ihr Testereignis zu speichern, wählen Sie Test (Testen) vor dem Speichern aus. Dadurch wird ein nicht gespeichertes Testereignis erstellt, das Lambda nur für die Dauer der Sitzung beibehält.

Über die Registerkarte Code können Sie auch auf Ihre gespeicherten und ungespeicherten Testereignisse zugreifen. Wählen Sie von dort Test (Testen) und anschließend Ihr Testereignis aus.

Private Testereignisse erstellen

Private Testereignisse stehen nur dem Ereignisersteller zur Verfügung und benötigen keine zusätzlichen Berechtigungen zur Verwendung. Sie können bis zu 10 Testereignisse pro Funktion erstellen und speichern.

So erstellen Sie ein privates Testereignis

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Klicken Sie auf den Namen der Funktion, die Sie testen möchten.
3. Wählen Sie die Registerkarte Test.
4. Erledigen Sie unter Testereignis Folgendes:
    a. Wählen Sie eine Vorlage.
    b. Geben Sie einen Namen für den Test an.
    c. Geben Sie im Texteingabefeld das JSON-Testereignis ein.
    d. Unter Ereignisfreigabeeinstellungen wählen Sie Privat aus.
5. Wählen Sie Änderungen speichern aus.

Sie können auch neue Testereignisse auf der Registerkarte Code erstellen. Wählen Sie von dort Test aus, dann Testereignis konfigurieren.

Freigabefähige Testereignisse erstellen

Freigabefähige Ereignisse sind Testereignisse, die Sie für andere Benutzer desselben AWS-Kontos freigeben können. Sie können die freigabefähigen Testereignisse anderer Benutzer bearbeiten und Ihre Funktion damit aufrufen.

Lambda speichert gemeinsam nutzbare Testereignisse als Schemata in einer Amazon EventBridge (CloudWatch Events)-Schemaregistrierung mit dem Namen `lambda-testevent-schemas`. Da Lambda diese Registry verwendet, um gemeinsam genutzte Testereignisse zu speichern und aufzurufen, empfehlen wir Ihnen nicht, diese Registry zu bearbeiten oder eine Registry mit dem Namen `lambda-testevent-schemas` zu erstellen.

Um freigabefähige Testereignisse anzuzeigen, freizugeben und zu bearbeiten, müssen Sie über Berechtigungen für alle folgenden EventBridge (CloudWatch Ereignisse) Schemaregistrierungs-API-Operationen verfügen:

- schemas.CreateRegistry
- schemas.CreateSchema
- schemas.DeleteSchema
- schemas.DeleteSchemaVersion
- schemas.DescribeRegistry
- schemas.DescribeSchema
- schemas.GetDiscoveredSchema
- schemas.ListSchemaVersions
- schemas.UpdateSchema

Beachten Sie, dass das Speichern von Änderungen an einem freigabefähigen Testereignis dieses Ereignis überschreibt.

Wenn Sie keine freigabefähigen Testereignisse erstellen, bearbeiten oder anzeigen können, überprüfen Sie, ob Ihr Konto über die erforderlichen Berechtigungen für diese Operationen verfügt. Wenn Sie über die erforderlichen Berechtigungen verfügen, aber immer noch nicht auf freigabefähige Testereignisse zugreifen können, suchen Sie nach ressourcenbasierten Richtlinien, die den Zugriff auf die EventBridge (CloudWatch Events)-Registrierung einschränken könnten.

So erstellen Sie ein freigabefähiges Testereignis

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Klicken Sie auf den Namen der Funktion, die Sie testen möchten.
3. Wählen Sie die Registerkarte Test.
4. Erledigen Sie unter Testereignis Folgendes:
    a. Wählen Sie eine Vorlage.
    b. Geben Sie einen Namen für den Test an.
    c. Geben Sie im Texteingabefeld das JSON-Testereignis ein.
    d. Wählen Sie unter Event sharing settings (Ereignisfreigabeeinstellungen) Shareable (Freigabefähig) aus.
5. Wählen Sie Änderungen speichern aus.

Verwenden Sie gemeinsam nutzbare Testereignisse mit AWS Serverless Application Model.

Sie können AWS SAM verwenden, um gemeinsam nutzbare Testereignisse aufzurufen. Siehe `sam remote test-event` im Entwicklerhandbuch für AWS Serverless Application Model

Löschen von freigabefähigen Test-Ereignisschemas

Wenn Sie freigabefähige Testereignisse löschen, entfernt Lambda sie aus der `lambda-testevent-schemas`-Registry. Wenn Sie das letzte freigabefähige Testereignis aus der Registry entfernen, löscht Lambda die Registry.

Wenn Sie die Funktion löschen, löscht Lambda keine verknüpften freigabefähigen Testereignisschemas. Sie müssen diese Ressourcen manuell über die EventBridge (CloudWatch Events)-Konsole bereinigen.

Lambda-Funktionszustände

Lambda enthält in der Funktionskonfiguration für alle Funktionen ein Statusfeld, das anzeigt, wann Ihre Funktion zum Aufruf bereit ist. `State` gibt Auskunft über den aktuellen Status der Funktion, einschließlich der Frage, ob Sie die Funktion erfolgreich aufrufen können. Funktionszustände ändern nicht das Verhalten von Funktionsaufrufen oder wie Ihre Funktion den Code ausführt. Zu den Funktionszustände gehören:

- `Pending` – Nachdem Lambda die Funktion erstellt hat, setzt es den Status auf „Ausstehend“. Im Status „Ausstehend“ versucht Lambda, Ressourcen für die Funktion zu erstellen oder zu konfigurieren, beispielsweise VPC- oder EFS-Ressourcen. Lambda ruft während des ausstehenden Status keine Funktion auf. Alle Aufrufe oder andere API-Aktionen, die mit der Funktion arbeiten, schlagen fehl.
- `Active` – Ihre Funktion wechselt in den aktiven Status, nachdem Lambda die Ressourcenkonfiguration und -Bereitstellung abgeschlossen hat. Funktionen können nur erfolgreich aufgerufen werden, wenn sie aktiv sind.
- `Failed` – Gibt an, dass bei der Ressourcenkonfiguration oder bei der Bereitstellung ein Fehler aufgetreten ist.
- `Inactive` – Eine Funktion wird inaktiv, wenn sie lange genug im Leerlauf war, damit Lambda die externen Ressourcen zurückfordern kann, die für sie konfiguriert wurden. Wenn Sie versuchen, eine Funktion aufzurufen, die inaktiv ist, schlägt der Aufruf fehl und Lambda setzt die Funktion auf den Status „Ausstehend“, bis die Funktionsressourcen neu erstellt werden. Wenn Lambda die Ressourcen nicht neu erstellen kann, kehrt die Funktion in den inaktiven Zustand zurück. Wenn Ihre Funktion im inaktiven Zustand hängen bleibt, finden Sie weitere Informationen zur Fehlerbehebung in den `StatusCodeReason` Attributen `StatusCode` und der Funktion. Möglicherweise müssen Sie alle Fehler beheben und Ihre Funktion erneut bereitstellen, um sie im aktiven Zustand wiederherzustellen.

Wenn Sie SDK-basierte Automatisierungs-Workflows verwenden oder die Service-APIs von Lambda direkt aufrufen, überprüfen Sie vor dem Aufruf einer Funktion, ob sie aktiv ist. Sie können dies mit der Lambda-API-Aktion tun GetFunctionoder einen Waiter mit dem AWS SDK for Java 2.0 konfigurieren.

```
aws lambda get-function --function-name my-function --query 'Configuration.[State,
 LastUpdateStatus]'
```

Die Ausgabe sollte folgendermaßen aussehen:

```
[
 "Active",
 "Successful"
]
```

Die folgenden Operationen schlagen fehl, während die Funktionserstellung aussteht:

- Aufrufen
- UpdateFunctionCode
- UpdateFunctionConfiguration
- PublishVersion

Funktionszustände während der Aktualisierung

Lambda bietet zusätzlichen Kontext für Funktionen, die mit dem `LastUpdateStatus`-Attribut aktualisiert werden und die folgenden Status haben können:

- `InProgress` – Bei einer vorhandenen Funktion wird eine Aktualisierung durchgeführt. Während ein Funktionsupdate ausgeführt wird, gehen Aufrufe zum vorherigen Code und Konfiguration der Funktion.
- `Successful` – Das Update ist abgeschlossen. Sobald Lambda das Update beendet hat, bleibt dies bis zu einem weiteren Update festgelegt.
- `Failed` – Die Aktualisierung der Funktion ist fehlgeschlagen. Lambda bricht das Update ab und der vorherige Code und die Konfiguration der Funktion bleiben verfügbar.

Example

Das Folgende ist das Ergebnis von `get-function-configuration` für eine Funktion, die einem Update unterzogen wird.

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
    "Runtime": "nodejs20.x",
    "VpcConfig": {
        "SubnetIds": [
            "subnet-071f712345678e7c8",
```

```
            "subnet-07fd123456788a036",
            "subnet-0804f77612345cacf"
        ],
        "SecurityGroupIds": [
            "sg-085912345678492fb"
        ],
        "VpcId": "vpc-08e1234569e011e83"
    },
    "State": "Active",
    "LastUpdateStatus": "InProgress",
    ...
}
```

FunctionConfiguration verfügt über zwei weitere Attribute, `LastUpdateStatusReason` und `LastUpdateStatusReasonCode`, um Probleme bei der Aktualisierung zu beheben.

Die folgenden Operationen schlagen fehl, während eine asynchrone Aktualisierung ausgeführt wird:

- UpdateFunctionCode
- UpdateFunctionConfiguration
- PublishVersion
- TagResource

Grundlegendes zum Wiederholungsverhalten in Lambda

Wenn Sie eine Funktion direkt aufrufen, bestimmen Sie die Strategie für den Umgang mit Fehlern im Zusammenhang mit dem Funktionscode. Lambda wiederholt diese Art von Fehlern nicht automatisch in Ihrem Namen. Um den Vorgang zu wiederholen, können Sie die Funktion manuell erneut aufrufen, das fehlgeschlagene Ereignis zum Debuggen an eine Warteschlange senden oder den Fehler ignorieren. Der Code Ihrer Funktion wurde möglicherweise vollständig, teilweise oder überhaupt nicht ausgeführt. Wenn Sie es erneut versuchen, stellen Sie sicher, dass der Code Ihrer Funktion das gleiche Ereignis mehrmals verarbeiten kann, ohne doppelte Transaktionen oder andere unerwünschte Nebenwirkungen zu verursachen.

Wenn Sie eine Funktion indirekt aufrufen, müssen Sie sich über das Wiederholungsverhalten des Aufrufers und alle Services im Klaren sein, mit denen die Anforderung während des Vorgangs konfrontiert wird. Dies umfasst die folgenden Szenarien.

- Asynchroner Aufruf – Lambda startet bei Funktionsfehlern zwei Wiederholungsversuche. Wenn die Kapazität der Funktion nicht für die Verarbeitung aller eingehenden Anforderungen ausreicht, verbleiben die an die Funktion zu sendenden Ereignisse möglicherweise stunden- oder tagelang in der Warteschlange. Sie können für die Funktion eine Warteschlange für unzustellbare Nachrichten konfigurieren, um nicht erfolgreich verarbeitete Ereignisse aufzufangen. Weitere Informationen finden Sie unter Asynchroner Aufruf.
- Ereignisquellen-Mappings – Ereignisquellen-Mappings, die aus Streams lesen, führen für den gesamten Batch von Elementen einen Wiederholungsversuch durch. Wiederholte Fehlermeldungen blockieren die Verarbeitung des betroffenen Shards, bis der Fehler behoben ist oder die Elemente ablaufen. Zum Erkennen blockierter Shards können Sie die Metrik Iterator Age überwachen.

  Für Ereignisquellen-Zuweisungen, die aus einer Warteschlange lesen, bestimmen Sie die Zeitdauer zwischen Wiederholversuchen und dem Ziel für fehlgeschlagene Ereignisse, indem Sie für die Quellwarteschlange die Zeitbeschränkung für die Sichtbarkeit und die Redrive-Richtlinie konfigurieren. Weitere Informationen finden Sie unter Wie Lambda Datensätze aus Stream- und warteschlangenbasierten Ereignisquellen verarbeitet und in der servicespezifischen Dokumentation unter Lambda mit Ereignissen aus anderen Diensten aufrufen AWS.
- AWS Dienste — AWS Dienste können Ihre Funktion synchron oder asynchron aufrufen. Beim synchronen Aufruf entscheidet der Dienst, ob er es erneut versucht. Zum Beispiel wiederholen Amazon-S3-Batch-Operationen den Vorgang, wenn die Lambda-Funktion einen `TemporaryFailure`-Antwortcode zurückgibt. Dienste, die Anfragen von einem Upstream-

Benutzer oder -Client weiterleiten, haben möglicherweise eine Wiederholungsstrategie oder leiten die Fehlerantwort an den Anforderer zurück. Beispielsweise leitet API Gateway die Fehlerantwort immer an den Anforderer zurück.

Bei asynchronen Aufrufen ist das Verhalten identisch mit dem Verhalten, wenn Sie die Funktion synchron aufrufen. Weitere Informationen finden Sie in den servicespezifischen Hilfethemen Lambda mit Ereignissen aus anderen Diensten aufrufen AWS und in der Dokumentation des aufrufenden Services.

- Andere Konten und Clients – Wenn Sie Zugriff auf andere Konten gewähren, können Sie mithilfe von ressourcenbasierten Richtlinien einschränken, welche Services und Ressourcen von ihnen zum Aufruf Ihrer Funktion konfiguriert werden können. Zum Schutz Ihrer Funktion vor einer Überlastung sollten Sie Ihrer Funktion mit Amazon API Gateway eine API-Ebene vorlagern.

Um Ihnen bei der Behebung von Fehlern in Lambda-Anwendungen zu helfen, ist Lambda in Dienste wie Amazon CloudWatch und integriert. AWS X-Ray Sie können mithilfe einer Kombination aus Protokollen, Metriken, Alarmen und Ablaufverfolgung Probleme in Funktionscode, API und anderen Ressourcen, die für Ihre Anwendung erforderlich sind, schnell erkennen und aufdecken. Weitere Informationen finden Sie unter Überwachung und Fehlerbehebung bei Lambda-Funktionen.

Verwenden Sie die rekursive Lambda-Schleifenerkennung, um Endlosschleifen zu verhindern

Wenn Sie als Ziel für die Ausgabe einer Lambda-Funktion den gleichen Service oder die gleiche Ressource konfigurieren, durch den bzw. durch die die Funktion aufgerufen wird, kann eine unendliche rekursive Schleife entstehen. Ein Beispiel wäre etwa eine Lambda-Funktion, die eine Nachricht in eine Amazon Simple Queue Service (Amazon SQS)-Warteschlange schreibt, die wiederum die gleiche Funktion aufruft. Dieser Aufruf veranlasst die Funktion, eine weitere Nachricht in die Warteschlange zu schreiben, die wiederum erneut die Funktion aufruft.

Unbeabsichtigte rekursive Schleifen können dazu führen, dass Ihnen unerwartete Gebühren in Rechnung gestellt werden. AWS-Konto Außerdem können Schleifen dazu führen, dass Lambda skaliert wird und die gesamte verfügbare Parallelität Ihres Kontos nutzt. Um die Auswirkungen unbeabsichtigter Schleifen zu verringern, kann Lambda bestimmte Arten von rekursiven Schleifen kurz nach ihrem Auftreten erkennen. Wenn Lambda eine rekursive Schleife erkennt, wird der Aufruf Ihrer Funktion beendet und Sie erhalten eine entsprechende Benachrichtigung.

Wenn Ihr Entwurf bewusst rekursive Muster verwendet, können Sie die Deaktivierung der Erkennung rekursiver Lambda-Schleifen anfordern. Wenden Sie sich an AWS Support, um diese Änderung anzufordern.

> **Important**
>
> Wenn Ihr Design bewusst eine Lambda-Funktion verwendet, um Daten in dieselbe AWS Ressource zurückzuschreiben, die die Funktion aufruft, gehen Sie vorsichtig vor und implementieren Sie geeignete Schutzplanken, um zu verhindern, dass Ihnen unerwartete Gebühren in Rechnung gestellt werden. AWS-Konto Weitere Informationen zu bewährten Methoden für die Verwendung rekursiver Aufrufmuster finden Sie bei Serverless Land unter Recursive patterns that cause run-away Lambda functions.

Sections

Grundlegendes zur Erkennung rekursiver Schleifen

Zur Erkennung rekursiver Schleifen in Lambda werden Ereignisse nachverfolgt. Lambda ist ein ereignisgesteuerter Compute-Service, der Ihren Funktionscode ausführt, wenn bestimmte Ereignisse auftreten. Ein Beispiel wäre etwa das Hinzufügen eines Elements zu einer Amazon-SQS-Warteschlange oder zu einem Amazon Simple Notification Service (Amazon SNS)-Thema. Ereignisse werden von Lambda als JSON-Objekte mit Informationen zur Änderung des Systemstatus an Ihre Funktion übergeben. Die Ausführung Ihrer Funktion infolge eines Ereignisses wird als Aufruf bezeichnet.

Zur Erkennung rekursiver Schleifen verwendet Lambda AWS X-Ray-Ablaufverfolgungs-Header. Wenn AWS-Services , die die Erkennung rekursiver Schleifen unterstützen, Ereignisse an Lambda senden, werden diese Ereignisse automatisch mit Metadaten versehen. Wenn Ihre Lambda-Funktion eines dieser Ereignisse AWS-Service mithilfe einer unterstützten Version eines AWS SDK in ein anderes Ereignis schreibt, aktualisiert sie diese Metadaten. In den aktualisierten Metadaten ist angegeben, wie oft das Ereignis die Funktion aufgerufen hat.

> **Note**
>
> Dieses Feature funktioniert ohne Aktivierung der aktiven X-Ray-Ablaufverfolgung. Die Erkennung rekursiver Schleifen ist standardmäßig für alle AWS -Kunden aktiviert. Die Nutzung des Features ist kostenlos.

Bei einer Kette von Anforderungen handelt es sich um eine Sequenz von Lambda-Aufrufen, die durch das gleiche auslösende Ereignis verursacht werden. Ein Beispiel: Angenommen, eine Amazon-SQS-Warteschlange ruft Ihre Lambda-Funktion auf. Anschließend sendet Ihre Lambda-Funktion das verarbeitete Ereignis an die gleiche Amazon-SQS-Warteschlange zurück und diese ruft wiederum erneut Ihre Funktion auf. In diesem Beispiel gehört jeder Aufruf Ihrer Funktion zur gleichen Kette von Anforderungen.

Wenn Ihre Funktion mehr als 16-mal in der gleichen Kette von Anforderungen aufgerufen wird, beendet Lambda automatisch den nächsten Funktionsaufruf in dieser Anforderungskette und benachrichtigt Sie. Wenn Ihre Funktion mit mehreren Auslösern konfiguriert ist, sind Aufrufe von anderen Auslösern nicht betroffen.

> **Note**
>
> Wenn die `maxReceiveCount`-Einstellung in der Redrive-Richtlinie der Quellwarteschlange höher als 16 ist, verhindert der Lambda-Rekursionsschutz nicht, dass Amazon SQS die Nachricht erneut versucht, nachdem eine rekursive Schleife erkannt und beendet wurde. Wenn Lambda eine rekursive Schleife erkennt und nachfolgende Aufrufe abbricht, gibt es ein `RecursiveInvocationException` an die Zuordnung von Ereignisquellen zurück. Dadurch wird der `receiveCount` Wert in der Nachricht erhöht. Lambda versucht die Nachricht erneut und blockiert weiterhin Funktionsaufrufe, bis Amazon SQS feststellt, dass der Wert überschritten `maxReceiveCount` ist, und die Nachricht an die konfigurierte Warteschlange für unzustellbare Briefe sendet.

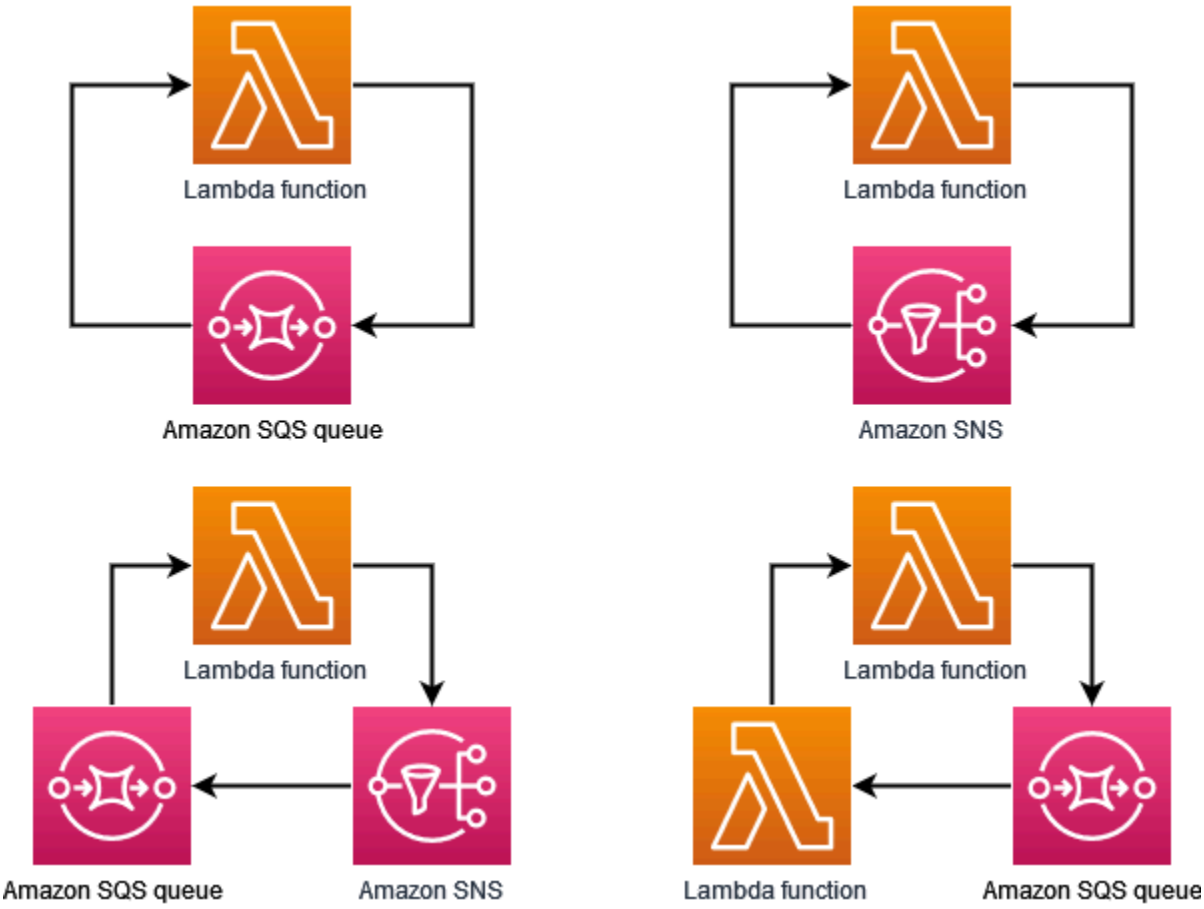
Wenn Sie für Ihre Funktion ein Ziel bei Ausfall oder eine Warteschlange für unzustellbare Nachrichten konfiguriert haben, sendet Lambda das Ereignis aus dem beendeten Aufruf auch an Ihr Ziel oder an die Warteschlange für unzustellbare Nachrichten. Wenn Sie für Ihre Funktion ein Ziel oder eine Warteschlange für unzustellbare Nachrichten konfigurieren, achten Sie darauf, kein Amazon-SNS-Thema und keine Amazon-SQS-Warteschlange zu verwenden, die Ihre Funktion auch als Ereignisauslöser oder für die Zuordnung von Ereignisquellen verwendet. Wenn Sie Ereignisse an die Ressource senden, die auch Ihre Funktion aufruft, können Sie eine weitere rekursive Schleife erstellen.

Unterstützte SDKs und SDKs AWS-Services

Lambda kann nur rekursive Schleifen erkennen, die bestimmte unterstützte enthalten. AWS-Services Damit rekursive Schleifen erkannt werden können, muss Ihre Funktion auch eines der unterstützten SDKs verwenden. AWS

Unterstützt AWS-Services

Lambda erkennt derzeit rekursive Schleifen zwischen Funktionen, Amazon SQS und Amazon SNS. Außerdem erkennt Lambda Schleifen, die nur aus Lambda-Funktionen bestehen, die sich synchron oder asynchron gegenseitig aufrufen. Die folgenden Diagramme zeigen einige Beispiele für Schleifen, die von Lambda erkannt werden:



Wenn ein anderes AWS-Service System wie Amazon DynamoDB oder Amazon Simple Storage Service (Amazon S3) Teil der Schleife ist, kann Lambda es derzeit nicht erkennen und stoppen.

Da Lambda derzeit nur rekursive Schleifen erkennt, an denen Amazon SQS und Amazon SNS beteiligt sind, ist es immer noch möglich, dass Schleifen, an denen andere beteiligt sind, zu einer unbeabsichtigten Nutzung Ihrer Lambda-Funktionen führen AWS-Services können.

Um zu verhindern, dass Ihnen unerwartete Gebühren in Rechnung gestellt werden AWS-Konto, empfehlen wir Ihnen, CloudWatchAmazon-Alarme so zu konfigurieren, dass Sie auf ungewöhnliche Nutzungsmuster aufmerksam gemacht werden. Sie können beispielsweise so konfigurieren, dass Sie über CloudWatch Spitzenwerte bei der Parallelität oder bei Aufrufen von Lambda-Funktionen benachrichtigt werden. Des Weiteren können Sie einen Abrechnungsalarm konfigurieren, um benachrichtigt zu werden, wenn die Ausgaben für Ihr Konto einen von Ihnen angegebenen Schwellenwert übersteigen. Eine weitere Möglichkeit ist die Verwendung der AWS Cost Anomaly Detection, um über ungewöhnliche Abrechnungsmuster informiert zu werden.

Unterstützte SDKs AWS

Damit Lambda rekursive Schleifen erkennt, muss Ihre Funktion eine der folgenden SDK-Mindestversionen verwenden:

Laufzeit	Minimale erforderliche AWS SDK-Version
Node.js	2.1147.0 (SDK-Version 2) 3.105.0 (SDK-Version 3)
Python	1.24.46 (boto3) 1.27.46 (botocore)
Java 8 und Java 11	1.12.200 (SDK-Version 1) 2.17.135 (SDK-Version 2)
Java 17	2.20.81
Java 21	2,21,24
.NET	3,7,293,0
Ruby	3,134,0
PHP	3,232,0

Einige Lambda-Laufzeiten wie Python und Node.js enthalten eine Version des AWS SDK. Wenn die in der Laufzeit Ihrer Funktion enthaltene SDK-Version kleiner ist als die erforderliche Mindestversion, können Sie dem Bereitstellungspaket Ihrer Funktion eine unterstützte Version des SDK hinzufügen. Sie können auch eine Lambda-Ebene verwenden, um Ihrer Funktion eine unterstützte SDK-Version hinzuzufügen. Eine Liste der SDKs, die in der jeweiligen Lambda-Laufzeitumgebung enthalten sind, finden Sie unter Lambda-Laufzeiten.

Die Lambda-Rekursionserkennung wird für die Lambda-Go-Laufzeit nicht unterstützt.

Benachrichtigungen zu rekursiven Schleifen

Wenn Lambda eine rekursive Schleife beendet, erhalten Sie Benachrichtigungen über das AWS Health Dashboard und per E-Mail. Sie können auch CloudWatch Metriken verwenden, um die Anzahl der rekursiven Aufrufe zu überwachen, die Lambda gestoppt hat.

AWS Health Dashboard Benachrichtigungen

Wenn Lambda einen rekursiven Aufruf stoppt, wird auf der Seite Ihr Kontostatus unter Offene und aktuelle Probleme eine Benachrichtigung AWS Health Dashboard angezeigt. Beachten Sie, dass es nach der Beendigung eines rekursiven Aufrufs durch Lambda bis zu drei Stunden dauern kann, bis diese Benachrichtigung angezeigt wird. Weitere Informationen zum Anzeigen von Kontoereignissen in der AWS Health Dashboard finden Sie unter Erste Schritte mit Ihrem AWS Health Dashboard — Ihr Kontostatus im AWS Health-Benutzerhandbuch.

E-Mail-Benachrichtigungen

Wenn Lambda zum ersten Mal einen rekursiven Aufruf Ihrer Funktion beendet, erhalten Sie eine E-Mail-Benachrichtigung. Für jede Funktion in Ihrem AWS-Konto wird alle 24 Stunden maximal eine E-Mail gesendet. Nachdem Lambda eine E-Mail-Benachrichtigung gesendet hat, erhalten Sie für einen Zeitraum von 24 Stunden keine E-Mails mehr zu dieser Funktion. Das gilt auch, wenn Lambda weitere rekursive Aufrufe der Funktion beendet. Beachten Sie, dass es nach der Beendigung eines rekursiven Aufrufs durch Lambda bis zu drei Stunden dauern kann, bis Sie diese E-Mail-Benachrichtigung erhalten.

Lambda sendet rekursive Loop-E-Mail-Benachrichtigungen an Ihren primären AWS-Konto Kundenkontakt und an den alternativen Betriebskontakt. Informationen zum Anzeigen oder Aktualisieren der E-Mail-Adressen in Ihrem Konto finden Sie in der allgemeinen AWS -Referenz unter Updating contact information.

CloudWatch Amazon-Metriken

Die CloudWatch Metrik `RecursiveInvocationsDropped` zeichnet die Anzahl der Funktionsaufrufen auf, die Lambda gestoppt hat, weil Ihre Funktion in einer einzigen Anforderungskette mehr als 16 Mal aufgerufen wurde. Lambda gibt diese Metrik aus, sobald ein rekursiver Aufruf beendet wurde. Um diese Metrik anzuzeigen, folgen Sie den Anweisungen unter Metriken anzeigen auf der CloudWatch Konsole und wählen Sie die Metrik aus. `RecursiveInvocationsDropped`

Reagieren auf Benachrichtigungen im Zusammenhang mit der Erkennung rekursiver Schleifen

Wenn Ihre Funktion mehr als 16-mal durch das gleiche auslösende Ereignis aufgerufen wird, beendet Lambda den nächsten Funktionsaufruf für dieses Ereignis, um die rekursive Schleife zu unterbrechen. Gehen Sie wie folgt vor, um zu verhindern, dass eine rekursive Schleife, die von Lambda unterbrochen wurde, erneut auftritt:

- Reduzieren Sie die verfügbare Parallelität Ihrer Funktion auf Null. Dadurch werden alle zukünftigen Aufrufe gedrosselt.
- Entfernen oder deaktivieren Sie den Auslöser oder die Zuordnung von Ereignisquellen, der bzw. die Ihre Funktion aufruft.
- Identifizieren und beheben Sie Codefehler, die Ereignisse in die AWS Ressource zurückschreiben, die Ihre Funktion aufruft. Eine Fehlerquelle entsteht häufig, wenn die Ereignisquelle und das Ziel einer Funktion mithilfe von Variablen definiert werden. Achten Sie darauf, nicht für beide Variablen den gleichen Wert zu verwenden.

Wenn die Ereignisquelle für Ihre Lambda-Funktion eine Amazon-SQS-Warteschlange ist, empfiehlt es sich außerdem gegebenenfalls, für die Quellwarteschlange eine Warteschlange für unzustellbare Nachrichten zu konfigurieren.

> **Note**
>
> Achten Sie darauf, die Warteschlange für unzustellbare Nachrichten für die Quellwarteschlange und nicht für die Lambda-Funktion zu konfigurieren. Die Warteschlange für unzustellbare Nachrichten, die Sie für eine Funktion konfigurieren, wird für die Warteschlange asynchroner Aufrufe der Funktion und nicht für Ereignisquellen-Warteschlangen verwendet.

Wenn es sich bei der Ereignisquelle um ein Amazon-SNS-Thema handelt, empfiehlt es sich gegebenenfalls, für Ihre Funktion ein Ziel bei Ausfall hinzuzufügen.

So reduzieren Sie die verfügbare Parallelität Ihrer Funktion auf Null (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen Ihrer Funktion aus.

3. Wählen Sie Drosseln aus.
4. Wählen Sie im Dialogfeld Funktion drosseln die Option Bestätigen aus.

So entfernen Sie einen Auslöser oder eine Zuordnung von Ereignisquellen für Ihre Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen Ihrer Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und anschließend Auslöser aus.
4. Wählen Sie unter Auslöser den Auslöser oder die Zuordnung von Ereignisquellen aus, den bzw. die Sie löschen möchten, und wählen Sie anschließend Löschen aus.
5. Wählen Sie im Dialogfeld Auslöser löschen die Option Löschen aus.

So deaktivieren Sie eine Zuordnung von Ereignisquellen für Ihre Funktion (AWS CLI)

1. Führen Sie den Befehl AWS Command Line Interface (AWS CLI) list-event-source-mappings aus, um die UUID für die Ereignisquellenzuordnung zu finden, die Sie deaktivieren möchten.

   ```
   aws lambda list-event-source-mappings
   ```

2. Um die Zuordnung der Ereignisquellen zu deaktivieren, führen Sie den folgenden Befehl update-event-source-mapping aus. AWS CLI

   ```
   aws lambda update-event-source-mapping --function-name MyFunction \
   --uuid a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 --no-enabled
   ```

Lambda-Funktions-URLs

Eine Funktions-URL ist ein dedizierter HTTPS-Endpunkt für Ihre Lambda-Funktion. Sie können eine Funktions-URL über die Lambda-Konsole oder die Lambda-API erstellen und konfigurieren. Wenn Sie eine Funktions-URL erstellen, generiert Lambda automatisch einen eindeutigen URL-Endpunkt für Sie. Sobald Sie eine Funktions-URL erstellt haben, ändert sich ihr URL-Endpunkt nie mehr. Funktions-URL-Endpunkte haben das folgende Format:

```
https://<url-id>.lambda-url.<region>.on.aws
```

> **Note**
>
> Funktions-URLs werden in den folgenden Regionen nicht unterstützt: Asien-Pazifik (Hyderabad) (`ap-south-2`), Asien-Pazifik (Melbourne) (`ap-southeast-4`), Kanada West (Calgary) (`ca-west-1`), Europa (Spanien) (`eu-south-2`), Europa (Zürich) (`eu-central-2`), Israel (Tel Aviv) (`il-central-1`) und Naher Osten (VAE) (`me-central-1`).

Funktions-URLs sind Dual-Stack-fähig und unterstützen IPv4 und IPv6. Nachdem Sie eine Funktions-URL für Ihre Funktion konfiguriert haben, können Sie Ihre Funktion über ihren HTTP(S)-Endpunkt über einen Webbrowser, curl, Postman oder einen beliebigen HTTP-Client aufrufen.

> **Note**
>
> Auf Ihre Funktions-URL können Sie nur über das öffentliche Internet zugreifen. Lambda-Funktionen unterstützen AWS PrivateLink, Funktions-URLs hingegen nicht.

URLs der Lambda-Funktion verwenden ressourcenbasierte Richtlinien für Sicherheit und Zugriffskontrolle. Funktions-URLs unterstützen auch CORS-Konfigurationsoptionen (Cross-Origin Resource Sharing).

Sie können Funktions-URLs auf jeden Funktionsalias oder auf die `$LATEST` unveröffentlichte Funktionsversion anwenden. Sie können keiner anderen Funktionsversion eine Funktions-URL hinzufügen.

Themen

- Erstellen und Verwalten von Lambda-Funktions-URLs

- Steuern Sie den Zugriff auf Lambda-Funktions-URLs
- Aufrufen von Lambda-Funktions-URLs
- Überwachen der Lambda-Funktions-URLs
- Tutorial: Erstellen einer Lambda-Funktion mit einer Funktions-URL

Erstellen und Verwalten von Lambda-Funktions-URLs

Eine Funktions-URL ist ein dedizierter HTTPS-Endpunkt für Ihre Lambda-Funktion. Sie können eine Funktions-URL über die Lambda-Konsole oder die Lambda-API erstellen und konfigurieren. Wenn Sie eine Funktions-URL erstellen, generiert Lambda automatisch einen eindeutigen URL-Endpunkt für Sie. Sobald Sie eine Funktions-URL erstellt haben, ändert sich ihr URL-Endpunkt nie mehr. Funktions-URL-Endpunkte haben das folgende Format:

```
https://<url-id>.lambda-url.<region>.on.aws
```

> **Note**
>
> Funktions-URLs werden in den folgenden Regionen nicht unterstützt: Asien-Pazifik (Hyderabad) (`ap-south-2`), Asien-Pazifik (Melbourne) (`ap-southeast-4`), Kanada West (Calgary) (`ca-west-1`), Europa (Spanien) (`eu-south-2`), Europa (Zürich) (), Israel (Tel Aviv`eu-central-2`) () und Naher Osten (VA`il-central-1`) (). `me-central-1`

Der folgende Abschnitt zeigt, wie Sie eine Funktions-URL mithilfe der Lambda-Konsole AWS CLI, und -Vorlage erstellen und AWS CloudFormation verwalten.

Themen

- Erstellen einer Funktions-URL (Konsole)
- Erstellen einer Funktions-URL (AWS CLI)
- Hinzufügen einer Funktions-URL zu einer CloudFormation Vorlage
- Cross-Origin Resource Sharing (CORS)
- Drosseln von Funktions-URLs
- Deaktivieren von Funktions-URLs
- Löschen von Funktions-URLs

Erstellen einer Funktions-URL (Konsole)

Gehen Sie wie folgt vor, um eine Funktions-URL mit der Konsole zu erstellen.

So erstellen Sie eine Funktions-URL für eine vorhandene Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie den Namen der Funktion, für die Sie die Funktions-URL erstellen möchten.
3. Wählen Sie die Registerkarte Konfiguration und dann Funktions-URL.
4. Wählen Sie Funktions-URL erstellen.
5. Für Auth-Typ wählen Sie AWS_IAM oder KEINE aus. Weitere Informationen zur Authentifizierung der Funktions-URL finden Sie unter Zugriffskontrolle.
6. (Optional) Wählen Sie Configure cross-origin resource sharing (CORS) (Cross-Origin Resource Sharing (CORS) konfigurieren) aus und konfigurieren Sie dann die CORS-Einstellungen für Ihre Funktions-URL. Weitere Informationen über CORS finden Sie unter Cross-Origin Resource Sharing (CORS).
7. Wählen Sie Speichern.

Dies erstellt eine Funktions-URL für die `$LATEST` unveröffentlichte Version Ihrer Funktion. Die Funktions-URL wird im Abschnitt Function overview (Funktionsübersicht) der Konsole angezeigt.

So erstellen Sie eine Funktions-URL für einen vorhandenen Alias (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen der Funktion mit dem Alias, für die Sie die Funktions-URL erstellen möchten.
3. Wählen Sie die Registerkarte Aliase und wählen Sie dann den Namen der Funktion mit dem Alias, für die Sie die Funktions-URL erstellen möchten.
4. Wählen Sie die Registerkarte Konfiguration und dann Funktions-URL.
5. Wählen Sie Funktions-URL erstellen.
6. Für Auth-Typ wählen Sie AWS_IAM oder KEINE aus. Weitere Informationen zur Authentifizierung der Funktions-URL finden Sie unter Zugriffskontrolle.
7. (Optional) Wählen Sie Configure cross-origin resource sharing (CORS) (Cross-Origin Resource Sharing (CORS) konfigurieren) aus und konfigurieren Sie dann die CORS-Einstellungen für Ihre Funktions-URL. Weitere Informationen über CORS finden Sie unter Cross-Origin Resource Sharing (CORS).
8. Wählen Sie Speichern.

Dies erstellt eine Funktions-URL für Ihren Funktionsalias. Die Funktions-URL wird im Abschnitt Funktionsübersicht der Konsole für Ihren Alias angezeigt.

So erstellen Sie eine neue Funktion mit einem Funktions-URL (Konsole)

So erstellen Sie eine neue Funktion mit einer Funktions-URL (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie unter Funktionsname einen Namen für Ihre Funktion ein, z. B. **`my-function`**.
   b. Wählen Sie für Runtime (Laufzeit) die bevorzugte Sprachlaufzeit aus, z. B. Node.js 18.x.
   c. Wählen Sie für Architecture (Architektur) entweder x86_64 oder arm64 aus.
   d. Erweitern Sie Permissions (Berechtigungen) und wählen Sie dann aus, ob eine neue Ausführungsrolle erstellt oder eine vorhandene Rolle verwendet werden soll.
4. Erweitern Sie Advanced settings (Erweiterte Einstellungen) und wählen Sie dann Funktions-URL aus.
5. Wählen Sie als Auth type (Authentifizierungstyp) die Option AWS_IAM (AWS_IAM) oder NONE (KEINE) aus. Weitere Informationen zur Authentifizierung der Funktions-URL finden Sie unter Zugriffskontrolle.
6. (Optional) Wählen Sie Cross-Origin Resource Sharing (CORS) konfigurieren aus. Wenn Sie diese Option während der Funktionserstellung auswählen, lässt Ihre Funktions-URL standardmäßig sämtliche Anfragen zu. Sie können die CORS-Einstellungen für Ihre Funktions-URL bearbeiten, nachdem Sie die Funktion erstellt haben. Weitere Informationen über CORS finden Sie unter Cross-Origin Resource Sharing (CORS).
7. Wählen Sie Funktion erstellen.

Dies erstellt eine neue Funktions mit einer Funktions-URL für die `$LATEST` unveröffentlichte Version Ihrer Funktion. Die Funktions-URL wird im Abschnitt Function overview (Funktionsübersicht) der Konsole angezeigt.

Erstellen einer Funktions-URL (AWS CLI)

Führen Sie den folgenden Befehl aus, um mit der AWS Command Line Interface (AWS CLI) eine Funktions-URL für eine bestehende Lambda-Funktion zu erstellen:

```
aws lambda create-function-url-config \
    --function-name my-function \
```

```
    --qualifier prod \ // optional
    --auth-type AWS_IAM
    --cors-config {AllowOrigins="https://example.com"} // optional
```

Dies fügt eine Funktions-URL zum **`prod`**-Qualifizierer für die Funktion**`my-function`** hinzu. Weitere Informationen zu diesen Konfigurationsparametern finden Sie CreateFunctionUrlConfigin der API-Referenz.

> **Note**
>
> Um eine Funktions-URL über die zu erstellen AWS CLI, muss die Funktion bereits vorhanden sein.

Hinzufügen einer Funktions-URL zu einer CloudFormation Vorlage

Verwenden Sie die folgende Syntax, um Ihrer AWS CloudFormation Vorlage eine `AWS::Lambda::Url` Ressource hinzuzufügen:

JSON

```
{
  "Type" : "AWS::Lambda::Url",
  "Properties" : {
      "AuthType" : String,
      "Cors" : Cors,
      "Qualifier" : String,
      "TargetFunctionArn" : String
    }
}
```

YAML

```
Type: AWS::Lambda::Url
Properties:
  AuthType: String
  Cors:
    Cors
  Qualifier: String
  TargetFunctionArn: String
```

Parameter

- (Erforderlich) `AuthType` – Definiert den Typ der Authentifizierung für Ihre Funktions-URL. Die möglichen Werte sind `AWS_IAM` oder `NONE`. Um den Zugriff nur auf authentifizierte Benutzer zu beschränken, setzen Sie den Wert auf `AWS_IAM`. Um die IAM-Authentifizierung zu umgehen und jedem Benutzer zu erlauben, Anfragen an Ihre Funktion zu stellen, setzten Sie dies auf `NONE`.
- (Optional)`Cors` – Definiert die CORS-Einstellungen für Ihre Funktions-URL. Verwenden Sie `Cors` die folgende Syntax CloudFormation, um Ihrer `AWS::Lambda::Url` Ressource in etwas hinzuzufügen.

  Example AWS::Lambda::Url.Cors (JSON)

  ```
  {
    "AllowCredentials" : Boolean,
    "AllowHeaders" : [ String, ... ],
    "AllowMethods" : [ String, ... ],
    "AllowOrigins" : [ String, ... ],
    "ExposeHeaders" : [ String, ... ],
    "MaxAge" : Integer
  }
  ```

  Example AWS::Lambda::Url.Cors (YAML)

  ```
    AllowCredentials: Boolean
    AllowHeaders:
      - String
    AllowMethods:
      - String
    AllowOrigins:
      - String
    ExposeHeaders:
      - String
    MaxAge: Integer
  ```

- (Optional) `Qualifier` – Der Aliasname.
- (Erforderlich) `TargetFunctionArn` – Der Name oder der Amazon-Ressourcenname (ARN) der Lambda-Funktion. Gültige Namensformate sind unter anderem:
  - Funktionsname – `my-function`.
  - Funktions-ARN – `arn:aws:lambda:us-west-2:123456789012:function:my-function`.

- Partiellet ARN – `123456789012:function:my-function`.

Cross-Origin Resource Sharing (CORS)

Um zu definieren, wie verschiedene Ursprünge auf Ihre Funktions-URL zugreifen können, verwenden Sie Cross-Origin Resource Sharing (CORS). Wir empfehlen, CORS zu konfigurieren, wenn Sie beabsichtigen, Ihre Funktions-URL von einer anderen Domain aus aufzurufen. Lambda unterstützt die folgenden CORS-Header für Funktions-URLs.

CORS-Header	CORS-Konfigurationseigenschaft	Beispielwerte

Access-Control-Allow-Origin	`AllowOrigins`	`*` (alle Ursprünge zulassen)
		`https://www.example.com`
		`http://localhost:60905`

Access-Control-Allow-Methods	`AllowMethods`	`GET`, `POST`, `DELETE`, `*`
Access-Control-Allow-Headers	`AllowHeaders`	`Date`, `Keep-Alive` , `X-Custom-Header`
Access-Control-Expose-Headers	`ExposeHeaders`	`Date`, `Keep-Alive` , `X-Custom-Header`
Access-Control-Allow-Credentials	`AllowCredentials`	`TRUE`
Access-Control-Max-Age	`MaxAge`	`5` (Standard), `300`

Wenn Sie CORS für eine Funktions-URL mithilfe der Lambda-Konsole oder der konfigurieren AWS CLI, fügt Lambda über die Funktions-URL automatisch die CORS-Header zu allen Antworten hinzu. Alternativ können Sie Ihrer Funktionsantwort manuell CORS-Header hinzufügen. Wenn es widersprüchliche Header gibt, haben die konfigurierten CORS-Header auf der Funktions-URL Vorrang.

Drosseln von Funktions-URLs

Die Drosselungsrate begrenzt die Geschwindigkeit, mit der Ihre Funktion Anfragen verarbeitet. Dies ist in vielen Situationen nützlich, z. B. um zu verhindern, dass Ihre Funktion nachgelagerte Ressourcen überlastet, oder beim Verarbeiten eines plötzlichen Anstiegs der Anfragen.

Sie können die Rate der Anfragen, die Ihre Lambda-Funktion über eine Funktions-URL verarbeitet, drosseln, indem Sie die reservierte Gleichzeitigkeit konfigurieren. Reservierte Gleichzeitigkeit begrenzt die Anzahl der maximalen gleichzeitigen Aufrufe für Ihre Funktion. Die maximale Anforderungsrate Ihrer Funktion pro Sekunde (RPS) entspricht dem Zehnfachen der konfigurierten reservierten Gleichzeitigkeit. Wenn Sie Ihre Funktion beispielsweise mit einer reservierten Gleichzeitigkeit von 100 konfigurieren, beträgt der maximale RPS 1 000.

Immer wenn Ihre Funktionsparallelität die reservierte Gleichzeitigkeit überschreitet, gibt Ihre Funktions-URL einen HTTP-429-Statuscode zurück. Wenn Ihre Funktion eine Anforderung erhält, die das 10-fache RPS-Maximum basierend auf Ihrer konfigurierten reservierten Gleichzeitigkeit überschreitet, erhalten Sie auch einen HTTP-429-Fehler. Weitere Hinweise zur reservierten Gleichzeitigkeit finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.

Deaktivieren von Funktions-URLs

Im Notfall sollten Sie den gesamten Datenverkehr zu Ihrer Funktions-URL ablehnen. Um eine Funktion zu deaktivieren, setzen Sie die reservierte Gleichzeitigkeit auf Null. Dies drosselt alle Anfragen an Ihre Funktions-URL, was zu HTTP-429-Statusantworten führt. Um Ihre Funktions-URL zu reaktivieren, löschen Sie die Konfiguration für die reservierte Gleichzeitigkeit oder legen Sie die Konfiguration auf einen Betrag größer als null fest.

Löschen von Funktions-URLs

Wenn Sie eine Funktions-URL löschen, können Sie sie nicht wiederherstellen. Das Erstellen einer neuen Funktions-URL führt zu einer anderen URL-Adresse.

> **Note**
>
> Wenn Sie Ihre Funktions-URL mit Authentifizierungstyp `NONE` löschen, löscht Lambda nicht automatisch die zugehörige ressourcenbasierte Richtlinie. Wenn Sie diese Richtlinie löschen möchten, müssen Sie dies manuell tun.

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie die Registerkarte Konfiguration und dann Funktions-URL.
4. Wählen Sie Löschen aus.
5. Geben Sie den Ausdruck delete (löschen) in das Feld ein, um den Löschvorgang zu bestätigen.
6. Wählen Sie Löschen aus.

> **Note**
>
> Wenn Sie eine Funktion löschen, die eine Funktions-URL hat, löscht Lambda die Funktions-URL asynchron. Wenn Sie sofort eine neue Funktion mit demselben Namen in demselben Konto erstellen, ist es möglich, dass die ursprüngliche Funktions-URL der neuen Funktion zugeordnet und nicht gelöscht wird.

Steuern Sie den Zugriff auf Lambda-Funktions-URLs

Sie können den Zugriff auf Ihre Lambda-Funktions-URLs mit dem `AuthType`-Parameter kombiniert mit ressourcenbasierten Richtlinien kontrollieren, die an Ihre spezifische Funktion angehängt sind. Die Konfiguration dieser beiden Komponenten bestimmt, wer andere administrative Aktionen für Ihre Funktions-URL aufrufen oder ausführen kann.

Der `AuthType`-Parameter bestimmt, wie Lambda Anfragen an Ihre Funktions-URL authentifiziert oder autorisiert. Wenn Sie Ihre Funktions-URL konfigurieren, müssen Sie eine der folgenden `AuthType`-Optionen angeben:

- `AWS_IAM`— Lambda verwendet AWS Identity and Access Management (IAM), um Anfragen auf der Grundlage der Identitätsrichtlinie des IAM-Prinzipals und der ressourcenbasierten Richtlinie der Funktion zu authentifizieren und zu autorisieren. Wählen Sie diese Option, wenn Sie möchten, dass nur authentifizierte -Benutzer und -Rollen Ihre Funktion über die Funktions-URL aufrufen können.

- `NONE` – Lambda führt keine Authentifizierung durch, bevor Sie Ihre Funktion aufrufen. Die ressourcenbasierte Richtlinie Ihrer Funktion ist jedoch immer in Kraft und muss öffentlichen Zugriff gewähren, bevor Ihre Funktions-URL Anfragen erhalten kann. Wählen Sie diese Option, um öffentlichen, nicht authentifizierten Zugriff auf Ihre Funktions-URL zu ermöglichen.

Zusätzlich zu `AuthType` können Sie auch ressourcenbasierte Richtlinien verwenden, um anderen AWS-Konten Berechtigungen zu gewähren, Ihre Funktion aufzurufen. Weitere Informationen finden Sie unter Arbeiten mit ressourcenbasierten Richtlinien in Lambda.

Für zusätzliche Einblicke in die Sicherheit können Sie eine umfassende Analyse des externen AWS Identity and Access Management Access Analyzer Zugriffs auf Ihre Funktions-URL nutzen. IAM Access Analyzer überwacht auch auf neue oder aktualisierte Berechtigungen für Ihre Lambda-Funktionen, um Berechtigungen zu identifizieren, die öffentlichen und kontoübergreifenden Zugriff gewähren. Die Nutzung von IAM Access Analyzer ist für jeden AWS Kunden kostenlos. Informationen zu den ersten Schritten mit IAM Access Analyzer finden Sie unter Verwenden von AWS IAM Access Analyzer.

Diese Seite enthält Beispiele für ressourcenbasierte Richtlinien für beide Authentifizierungstypen sowie die Erstellung dieser Richtlinien mithilfe des AddPermissionAPI-Vorgangs oder der Lambda-Konsole. Informationen darüber, wie Sie Ihre Funktions-URL aufrufen können, nachdem Sie Berechtigungen eingerichtet haben, finden Sie unter Aufrufen von Lambda-Funktions-URLs.

Themen

Verwenden des Auth-Typs **AWS_IAM**

Wenn Sie den Authentifizierungstyp `AWS_IAM` auswählen, müssen Benutzer, die Ihre Lambda-Funktions-URL aufrufen, die `lambda:InvokeFunctionUrl`-Berechtigung haben. Je nachdem, wer die Aufrufanforderung stellt, müssen Sie diese Berechtigung möglicherweise mithilfe einer ressourcenbasierten Richtlinie erteilen.

Wenn sich der Principal, der die Anfrage stellt, in derselben URL befindet AWS-Konto wie die Funktions-URL, muss der Principal entweder über `lambda:InvokeFunctionUrl` Berechtigungen in seiner identitätsbasierten Richtlinie verfügen oder ihm in der ressourcenbasierten Richtlinie der Funktion Berechtigungen erteilt worden sein. Mit anderen Worten, eine ressourcenbasierte Richtlinie ist optional, wenn der Benutzer bereits `lambda:InvokeFunctionUrl`-Berechtigungen in seiner identitätsbasierten Richtlinie hat. Die Bewertung der Richtlinien folgt den im Abschnitt Ermitteln, ob eine Anforderung innerhalb eines Kontos zugelassen oder verweigert wird erläuterten Regeln.

Wenn der Prinzipal, der die Anfrage stellt, in einem anderen Konto ist, muss der Prinzipal sowohl eine identitätsbasierte Richtlinie haben, die ihm `lambda:InvokeFunctionUrl`-Berechtigungen gewährt, als auchBerechtigungen, die ihm in einer ressourcenbasierten Richtlinie für die Funktion gewährt werden, die er aufrufen möchte. In diesen kontoübergreifenden Fällen folgt die Richtlinienbewertung den im Abschnitt Festlegen, ob eine kontoübergreifende Anforderung zulässig ist erläuterten Regeln.

Bei einem Beispiel für eine kontenübergreifende Interaktion ermöglicht die folgende ressourcenbasierte Richtlinie der `example` Rolle in, die der Funktion zugeordnete Funktions-URL AWS-Konto `444455556666` aufzurufen: `my-function`

Example Kontoübergreifende Aufrufrichtlinie für Funktions-URL

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

```
                "AWS": "arn:aws:iam::444455556666:role/example"
            },
            "Action": "lambda:InvokeFunctionUrl",
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "AWS_IAM"
                }
            }
        }
    ]
}
```

Sie können diese Richtlinienanweisung über die Konsole erstellen, indem Sie die folgenden Schritte ausführen:

So erteilen Sie einem anderen Konto (Konsole) URL-Aufrufberechtigungen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen der Funktion aus, für die Sie URL-Aufrufberechtigungen gewähren möchten.
3. Wählen Sie die Registerkarte Konfiguration und dann Berechtigungen aus.
4. Wählen Sie unter Resource-based policy (Ressourcenbasierte Richtlinie) die Option Add permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Funktions-URL aus.
6. Wählen Sie für Auth type (Authentifizierungstyp) die Option AWS_IAM aus.
7. (Optional) Geben Sie für Statement ID (Statement-ID) eine ID für Ihre Richtlinienanweisung ein.
8. Geben Sie unter Prinzipal den Amazon-Ressourcennamen (ARN) des Benutzers oder der Rolle ein, dem bzw. der Sie Berechtigungen gewähren möchten. Zum Beispiel: **444455556666**.
9. Wählen Sie Speichern.

Alternativ können Sie diese Richtlinienanweisung mit dem folgenden Befehl AWS Command Line Interface add-permission () erstellen:AWS CLI

```
aws lambda add-permission --function-name my-function \
    --statement-id example0-cross-account-statement \
    --action lambda:InvokeFunctionUrl \
    --principal 444455556666 \
```

```
    --function-url-auth-type AWS_IAM
```

Im vorangegangenen Beispiel ist der `lambda:FunctionUrlAuthType`-Bedingungsschlüsselwert `AWS_IAM`. Diese Richtlinie erlaubt den Zugriff nur, wenn der Authentifizierungstyp Ihrer Funktions-URL ebenfalls `AWS_IAM` ist.

Verwenden des Authentifizierungstyps **NONE**

> **Important**
>
> Wenn Ihre Funktions-URL-Auth-Typ `NONE` ist und Sie eine ressourcenbasierte Richtlinie haben, die öffentlichen Zugriff gewährt, kann jeder nicht authentifizierte Benutzer mit Ihrer Funktions-URL Ihre Funktion aufrufen.

In einigen Fällen möchten Sie möglicherweise, dass Ihre Funktions-URL öffentlich ist. So können Sie beispielsweise Anfragen direkt von einem Webbrowser aus bereitstellen. Um den öffentlichen Zugriff auf Ihre Funktions-URL zu ermöglichen, wählen Sie den Auth-Typ `NONE` aus.

Wenn Sie den Auth-Typ `NONE` auswählen, verwendet Lambda IAM nicht, um Anfragen an Ihre Funktions-URL zu authentifizieren. Benutzer müssen jedoch immer noch `lambda:InvokeFunctionUrl`-Berechtigungen haben, um Ihre Funktions-URL erfolgreich aufzurufen. Sie können `lambda:InvokeFunctionUrl`-Berechtigungen erteilen, indem Sie die folgende ressourcenbasierte Richtlinie verwenden:

Example Funktions-URL-Aufrufrichtlinie für alle nicht authentifizierten Prinzipale

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "lambda:InvokeFunctionUrl",
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-function",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "NONE"
                }
            }
        }
```

```
    ]
}
```

> **Note**
>
> Wenn Sie eine Funktions-URL mit dem Authentifizierungstyp `NONE` über die Konsole oder AWS Serverless Application Model (AWS SAM) erstellen, erstellt Lambda automatisch die vorherige ressourcenbasierte Richtlinienanweisung für Sie. Wenn die Richtlinie bereits vorhanden ist oder der Benutzer oder die Rolle, die die Anwendung erstellt, nicht über die entsprechenden Berechtigungen verfügt, erstellt Lambda sie nicht für Sie. Wenn Sie die AWS CLI AWS CloudFormation, oder die Lambda-API direkt verwenden, müssen Sie selbst `lambda:InvokeFunctionUrl` Berechtigungen hinzufügen. Dies macht Ihre Funktion öffentlich.
>
> Wenn Sie Ihre Funktions-URL mit Authentifizierungstyp `NONE` löschen, löscht Lambda außerdem nicht automatisch die zugehörige ressourcenbasierte Richtlinie. Wenn Sie diese Richtlinie löschen möchten, müssen Sie dies manuell tun.

In dieser Anweisung ist der `lambda:FunctionUrlAuthType`-Bedingungsschlüsselwert `NONE`. Diese Richtlinienanweisung erlaubt den Zugriff nur, wenn der Auth-Typ Ihrer Funktions-URL ebenfalls `NONE` ist.

Wenn die ressourcenbasierte Richtlinie einer Funktion `lambda:invokeFunctionUrl`-Berechtigungen nicht gewährt, dann erhalten Benutzer einen 403-Forbidden-Fehlercode beim Versuch, Ihre Funktions-URL aufzurufen, auch wenn die Funktions-URL den Authentifizierungstyp `NONE` verwendet.

Governance und Zugriffskontrolle

Zusätzlich zu den Berechtigungen für den URL-Aufruf von Funktionen können Sie auch den Zugriff auf Aktionen kontrollieren, die zum Konfigurieren von Funktions-URLs verwendet werden. Lambda unterstützt die folgenden IAM-Richtlinienaktionen für Funktions-URLs:

- `lambda:InvokeFunctionUrl` – Ruft eine Lambda-Funktion mit der Funktions-URL auf.
- `lambda:CreateFunctionUrlConfig` – Erstellt eine Funktions-URL und legt ihren `AuthType` fest.
- `lambda:UpdateFunctionUrlConfig` – Aktualisiert eine Funktions-URL-Konfiguration und ihren `AuthType`.

- `lambda:GetFunctionUrlConfig` – Zeigt die Details einer Funktions-URL an.
- `lambda:ListFunctionUrlConfigs` – Listet die Funktions-URL-Konfigurationen auf.
- `lambda:DeleteFunctionUrlConfig` – Löscht eine Funktions-URL.

> **Note**
>
> Die Lambda-Konsole unterstützt das Hinzufügen von Berechtigungen nur für `lambda:InvokeFunctionUrl`. Für alle anderen Aktionen müssen Sie Berechtigungen mit der Lambda-API oder AWS CLI hinzufügen.

Um anderen AWS Entitäten den Zugriff auf Funktions-URLs zu gewähren oder zu verweigern, nehmen Sie diese Aktionen in die IAM-Richtlinien auf. Die folgende Richtlinie gewährt der `example` Rolle in beispielsweise AWS-Konto `444455556666` Berechtigungen zur Aktualisierung der Funktions-URL für die Funktion **`my-function`** im Konto`123456789012`.

Example Kontoübergreifende Funktions-URL-Richtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/example"
            },
            "Action": "lambda:UpdateFunctionUrlConfig",
            "Resource": "arn:aws:lambda:us-east-2:123456789012:function:my-function"
        }
    ]
}
```

Bedingungsschlüssel

Verwenden Sie einen Bedingungsschlüssel, um eine feinabgestimmte Zugriffskontrolle über Ihre Funktions-URLs zu erhalten. Lambda unterstützt einen zusätzlichen Bedingungsschlüssel für Funktions-URLs: `FunctionUrlAuthType`. Der Schlüssel `FunctionUrlAuthType` definiert einen Aufzählungswert, der den Authentifizierungstyp beschreibt, den Ihre Funktions-URL verwendet. Der Wert kann entweder `AWS_IAM` oder `NONE` sein.

Sie können diesen Bedingungsschlüssel in Richtlinien verwenden, die mit Ihrer Funktion verknüpft sind. Sie können beispielsweise einschränken, wer Konfigurationsänderungen an Ihren Funktions-URLs vornehmen kann. Um alle `UpdateFunctionUrlConfig`-Anfragen an jede Funktion mit dem URL-Auth-Typ `NONE` zu verweigern, können Sie die folgende Richtlinie definieren:

Example Funktions-URL-Richtlinie mit expliziter Zugriffsverweigerung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action":[
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "NONE"
                }
            }
        }
    ]
}
```

Um der `example` Rolle AWS-Konto `444455556666` Berechtigungen zum Stellen `CreateFunctionUrlConfig` und `UpdateFunctionUrlConfig` Anfragen für Funktionen mit dem URL-Authentifizierungstyp zu gewähren`AWS_IAM`, können Sie die folgende Richtlinie definieren:

Example Funktions-URL-Richtlinie mit expliziter Zulassung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:role/example"
            },
            "Action":[
                "lambda:CreateFunctionUrlConfig",
```

```
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:us-east-1:123456789012:function:*",
            "Condition": {
                "StringEquals": {
                    "lambda:FunctionUrlAuthType": "AWS_IAM"
                }
            }
        }
    ]
}
```

Sie können diesen Bedingungsschlüssel auch in einer Service-Kontrollrichtlinie (SCP) verwenden. Verwenden Sie SCPs, um Berechtigungen in einer gesamten Organisation in AWS Organizations zu verwalten. Zum Beispiel, um Benutzern das Erstellen oder Aktualisieren von Funktions-URLs zu verweigern, die etwas anderes als den Auth-Typ `AWS_IAM` verwenden, verwenden Sie die folgende Service-Kontrollrichtlinie:

Example Funktions-URL-SCP mit expliziter Zugriffsverweigerung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action":[
                "lambda:CreateFunctionUrlConfig",
                "lambda:UpdateFunctionUrlConfig"
            ],
            "Resource": "arn:aws:lambda:*:123456789012:function:*",
            "Condition": {
                "StringNotEquals": {
                    "lambda:FunctionUrlAuthType": "AWS_IAM"
                }
            }
        }
    ]
}
```

Aufrufen von Lambda-Funktions-URLs

Eine Funktions-URL ist ein dedizierter HTTPS-Endpunkt für Ihre Lambda-Funktion. Sie können eine Funktions-URL über die Lambda-Konsole oder die Lambda-API erstellen und konfigurieren. Wenn Sie eine Funktions-URL erstellen, generiert Lambda automatisch einen eindeutigen URL-Endpunkt für Sie. Sobald Sie eine Funktions-URL erstellt haben, ändert sich ihr URL-Endpunkt nie mehr. Funktions-URL-Endpunkte haben das folgende Format:

```
https://<url-id>.lambda-url.<region>.on.aws
```

> **Note**
>
> Funktions-URLs werden in den folgenden Regionen nicht unterstützt: Asien-Pazifik (Hyderabad) (`ap-south-2`), Asien-Pazifik (Melbourne) (`ap-southeast-4`), Kanada West (Calgary) (`ca-west-1`), Europa (Spanien) (`eu-south-2`), Europa (Zürich) (`eu-central-2`), Israel (Tel Aviv) (`il-central-1`) und Naher Osten (VAE) (`me-central-1`).

Funktions-URLs sind Dual-Stack-fähig und unterstützen IPv4 und IPv6. Nachdem Sie Ihre Funktions-URL konfiguriert haben, können Sie Ihre Funktion über ihren HTTP(S)-Endpunkt über einen Webbrowser, cURL, Postman oder einen beliebigen HTTP-Client aufrufen. Um eine Funktions-URL aufzurufen, müssen Sie `lambda:InvokeFunctionUrl`-Berechtigungen haben. Weitere Informationen finden Sie unter Zugriffskontrolle.

Themen

- Grundlagen des Aufrufs von Funktions-URLs
- Anfordern und Beantworten von Nutzlasten

Grundlagen des Aufrufs von Funktions-URLs

Wenn Ihre Funktions-URL den Auth-Typ `AWS_IAM` hat, müssen Sie jede HTTP-Anfrage mit der AWS Signature Version 4 (SigV4) signieren. Tools wie awscurl, Postman und AWSSigV4-Proxy bieten integrierte Möglichkeiten, Ihre Anfragen mit SigV4 zu signieren.

Wenn Sie kein Tool verwenden, um HTTP-Anfragen an Ihre Funktions-URL zu signieren, müssen Sie jede Anfrage manuell mit SigV4 signieren. Wenn Ihre Funktions-URL eine Anfrage erhält, berechnet Lambda auch die SigV4-Signatur. Nur wenn die Signaturen übereinstimmen, verarbeitet Lambda

die Anfrage. Anweisungen zum manuellen Signieren Ihrer Anforderungen mit SigV4 finden Sie unter Signieren von AWS-Anforderungen mit Signature Version 4 im Allgemeine Amazon Web Services-Referenz.

Wenn Ihre Funktions-URL den Authentifizierungstyp `NONE` verwendet, müssen Sie Ihre Anfragen nicht mit SigV4 signieren. Sie können Ihre Funktion per Webbrowser, cURL, Postman oder einem beliebigen HTTP-Client aufrufen.

Um einfache `GET`-Anfragen an Ihre Funktion zu testen, verwenden Sie einen Webbrowser. Wenn Ihre Funktions-URL zum Beispiel `https://abcdefg.lambda-url.us-east-1.on.aws` ist und sie einen Zeichenfolgeparameter `message` aufnimmt, könnte Ihre Anforderungs-URL folgendermaßen aussehen:

```
https://abcdefg.lambda-url.us-east-1.on.aws/?message=HelloWorld
```

Um andere HTTP-Anfragen zu testen, z. B. eine `POST`-Anfrage, können Sie ein Tool wie cURL verwenden. Wenn Sie z. B. einige JSON-Daten in eine `POST`-Anfrage an Ihre Funktions-URL aufnehmen möchten, können Sie den folgenden cURL-Befehl verwenden:

```
curl -v 'https://abcdefg.lambda-url.us-east-1.on.aws/?message=HelloWorld' \
-H 'content-type: application/json' \
-d '{ "example": "test" }'
```

Anfordern und Beantworten von Nutzlasten

Wenn ein Client Ihre Funktions-URL aufruft, ordnet Lambda die Anforderung einem Ereignisobjekt zu, bevor es sie an Ihre Funktion übergibt. Die Antwort Ihrer Funktion wird dann einer HTTP-Antwort zugeordnet, die Lambda über die Funktions-URL an den Client zurücksendet.

Die Formate für Anforderungs- und Antwortereignisse folgen dem gleichen Schema wie die Amazon-API-Gateway-Nutzlastformatversion 2.0.

Anforderungsnutzlastformat

Eine Anforderungsnutzlast hat die folgende Struktur:

```
{
  "version": "2.0",
  "routeKey": "$default",
  "rawPath": "/my/path",
  "rawQueryString": "parameter1=value1&parameter1=value2&parameter2=value",
```

```
  "cookies": [
    "cookie1",
    "cookie2"
  ],
  "headers": {
    "header1": "value1",
    "header2": "value1,value2"
  },
  "queryStringParameters": {
    "parameter1": "value1,value2",
    "parameter2": "value"
  },
  "requestContext": {
    "accountId": "123456789012",
    "apiId": "<urlid>",
    "authentication": null,
    "authorizer": {
        "iam": {
                "accessKey": "AKIA...",
                "accountId": "111122223333",
                "callerId": "AIDA...",
                "cognitoIdentity": null,
                "principalOrgId": null,
                "userArn": "arn:aws:iam::111122223333:user/example-user",
                "userId": "AIDA..."
        }
    },
    "domainName": "<url-id>.lambda-url.us-west-2.on.aws",
    "domainPrefix": "<url-id>",
    "http": {
      "method": "POST",
      "path": "/my/path",
      "protocol": "HTTP/1.1",
      "sourceIp": "123.123.123.123",
      "userAgent": "agent"
    },
    "requestId": "id",
    "routeKey": "$default",
    "stage": "$default",
    "time": "12/Mar/2020:19:03:58 +0000",
    "timeEpoch": 1583348638390
  },
  "body": "Hello from client!",
  "pathParameters": null,
```

```
  "isBase64Encoded": false,
  "stageVariables": null
}
```

Parameter	Beschreibung	Beispiel
`version`	Die Nutzlastformatversion für dieses Ereignis. Lambda-Funktions-URLs unterstützen derzeit die Nutzlastformatversion 2.0.	`2.0`
`routeKey`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `$default` als Platzhalter.	`$default`
`rawPath`	Der Anforderungspfad. Wenn die Anforderungs-URL beispielsweise `https://{url-id}.lambda-url.{region}.on.aws/example/test/demo` ist, dann ist der Rohpfadwert `/example/test/demo`.	`/example/test/demo`
`rawQueryString`	Die Rohzeichenfolge, die die Abfragezeichenfolge-Parameter der Anforderung enthält. Zu den unterstützten Zeichen gehören `a-z`, `A-Z`, `0-9`, `.`, `_`, `-`, `%`, `&`, `=`, und `+`.	`"?parameter1=value1&parameter2=value2"`
`cookies`	Ein Array, das alle Cookies enthält, die im Rahmen der Anforderung gesendet wurden.	`["Cookie_1=Value_1", "Cookie_2=Value_2"]`

Parameter	Beschreibung	Beispiel
`headers`	Die Liste der Anforderungs-Header, die als Schlüssel -Wert-Paare dargestellt werden.	`{"header1": "value1", "header2": "value2"}`
`queryStringParameters`	Die Abfrageparameter für die Anforderung. Wenn die Anforderungs-URL beispielsweise `https://{url-id}.lambda-url.{region}.on.aws/example?name=Jane` ist, dann ist der `queryStringParameters` -Wert ein JSON-Objekt mit einem Schlüssel von `name` und einem Wert von `Jane`.	`{"name": "Jane"}`
`requestContext`	Ein Objekt, das zusätzliche Informationen über die Anforderung enthält, z. B. `requestId` , den Zeitpunkt der Anfrage und die Identität des Anrufers, falls über AWS Identity and Access Management (IAM) autorisiert.	
`requestContext.accountId`	Die AWS-Konto-ID des Funktionsbesitzers.	`"123456789012"`
`requestContext.apiId`	Die ID der Funktions-URL.	`"33anwqw8fj"`
`requestContext.authentication`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `null`.	`null`

Parameter	Beschreibung	Beispiel
`requestContext.authorizer`	Ein Objekt, das Informationen über die Aufruferidentität enthält, wenn die Funktions-URL den Authentifizierungstyp `AWS_IAM` verwendet. Ansonsten setzt Lambda dies auf `null`.	
`requestContext.authorizer.iam.accessKey`	Der Zugriffsschlüssel der Anruferidentität.	`"AKIAIOSFODNN7EXAMPLE"`
`requestContext.authorizer.iam.accountId`	Die AWS-Konto-Identitäts-ID des Anrufers.	`"111122223333"`
`requestContext.authorizer.iam.callerId`	Die ID (Benutzer-ID) des Aufrufers.	`"AIDACKCEVSQ6C2EXAMPLE"`
`requestContext.authorizer.iam.cognitoIdentity`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `null` oder schließt dies aus der JSON aus.	`null`
`requestContext.authorizer.iam.principalOrgId`	Die Prinzipal-Organisations-ID, die mit der Anruferidentität verknüpft ist.	`"AIDACKCEVSQORGEXAMPLE"`
`requestContext.authorizer.iam.userArn`	Der Benutzer-ARN (Amazon-Ressourcenname) der Anruferidentität.	`"arn:aws:iam::111122223333:user/example-user"`
`requestContext.authorizer.iam.userId`	Die Benutzer-ID des Anrufers.	`"AIDACOSFODNN7EXAMPLE2"`

Parameter	Beschreibung	Beispiel
`requestContext.domainName`	Der Domain-Name der Funktions-URL.	`"<url-id>.lambda-url.us-west-2.on.aws"`
`requestContext.domainPrefix`	Das Domain-Präfix der Funktions-URL.	`"<url-id>"`
`requestContext.http`	Ein Objekt, das Details zur HTTP-Anforderung enthält.	
`requestContext.http.method`	Die in der Anforderung verwendete HTTP-Methode. Gültige Werte sind unter anderem `GET`, `POST`, `PUT`, `HEAD`, `OPTIONS`, `PATCH` und `DELETE`.	`GET`
`requestContext.http.path`	Der Anforderungspfad. Zum Beispiel, wenn die Anforderungs-URL `https://{url-id}.lambda-url.{region}.on.aws/example/test/demo` ist, dann ist der Pfadwert `/example/test/demo` .	`/example/test/demo`
`requestContext.http.protocol`	Das Protokoll der Anforderung.	`HTTP/1.1`
`requestContext.http.sourceIp`	Die Quell-IP-Adresse der TCP-Verbindung, von der die Anforderung stammt.	`123.123.123.123`

Parameter	Beschreibung	Beispiel
`requestContext.http.userAgent`	Der Headerwert der Benutzer-Agent-Anforderung.	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Gecko/20100101 Firefox/42.0`
`requestContext.requestId`	Die ID der aktuellen Aufrufanforderung. Sie können diese ID verwenden, um Aufrufprotokolle zu verfolgen, die sich auf Ihre Funktion beziehen.	`e1506fd5-9e7b-434f-bd42-4f8fa224b599`
`requestContext.routeKey`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `$default` als Platzhalter.	`$default`
`requestContext.stage`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `$default` als Platzhalter.	`$default`
`requestContext.time`	Der Zeitstempel der Anfrage.	`"07/Sep/2021:22:50:22 +0000"`
`requestContext.timeEpoch`	Die Uhrzeit der Anfrage in Unix-Epochen-Zeit.	`"1631055022677"`
`body`	Der Text der Anforderung. Wenn der Inhaltstyp der Anforderung binär ist, ist der Text base64-kodiert.	`{"key1": "value1", "key2": "value2"}`

Parameter	Beschreibung	Beispiel
`pathParameters`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `null` oder schließt dies aus der JSON aus.	`null`
`isBase64Encoded`	`TRUE`, wenn der Text eine binäre Nutzlast hat und base64-kodiert ist. Ansonsten `FALSE`.	`FALSE`
`stageVariables`	Funktions-URLs verwenden diesen Parameter nicht. Lambda setzt dies auf `null` oder schließt dies aus der JSON aus.	`null`

Antwortnutzlastformat

Wenn Ihre Funktion eine Antwort zurückgibt, analysiert Lambda die Antwort und konvertiert sie in eine HTTP-Antwort. Funktionsantwortnutzlasten haben das folgende Format:

```
{
   "statusCode": 201,
    "headers": {
        "Content-Type": "application/json",
        "My-Custom-Header": "Custom Value"
    },
    "body": "{ \"message\": \"Hello, world!\" }",
    "cookies": [
        "Cookie_1=Value1; Expires=21 Oct 2021 07:48 GMT",
        "Cookie_2=Value2; Max-Age=78000"
    ],
    "isBase64Encoded": false
}
```

Lambda leitet das Antwortformat für Sie ab. Wenn Ihre Funktion gültiges JSON zurückgibt und keinen `statusCode` zurückgibt, geht Lambda von Folgendem aus:

- `statusCode` ist `200`.
- `content-type` ist `application/json`.
- `body` ist die Antwort der Funktion.
- `isBase64Encoded` ist `false`.

Die folgenden Beispiele zeigen, wie die Ausgabe Ihrer Lambda-Funktion der Antwortnutzlast und die Antwortnutzlast der endgültigen HTTP-Antwort zugeordnet wird. Wenn der Client Ihre Funktions-URL aufruft, wird die HTTP-Antwort angezeigt.

Beispielausgabe für eine Zeichenfolgeantwort

Lambda-Funktionsausgabe	Interpretierte Antwortausgabe	HTTP-Antwort (was der Client sieht)

`"Hello, world!"`	`{ "statusCode": 200, "body": "Hello, world!", "headers": { "content-type": "application/json" }, "isBase64Encoded": false }`	`HTTP/2 200`
		`date: Wed, 08 Sep 2021 18:02:24 GMT`
		`content-type: application/json`
		`content-length: 15`
		
		`"Hello, world!"`

Beispielausgabe für eine JSON-Antwort

Lambda-Funktionsausgabe	Interpretierte Antwortausgabe	HTTP-Antwort (was der Client sieht)
`{ "message": "Hello, world!" }`	`{ "statusCode": 200, "body": {`	`HTTP/2 200` `date: Wed, 08 Sep 2021 18:02:24 GMT`

Lambda-Funktionsausgabe	Interpretierte Antwortausgabe	HTTP-Antwort (was der Client sieht)

	<pre>"message": "Hello, world!" }, "headers": { "content-type": "application/json" }, "isBase64Encoded": false }</pre>	<pre>content-type: application/json content-length: 34
		
		{ "message": "Hello, world!" }</pre>

Beispielausgabe für eine benutzerdefinierte Antwort

Lambda-Funktionsausgabe	Interpretierte Antwortausgabe	HTTP-Antwort (was der Client sieht)

<pre>{ "statusCode": 201, "headers": { "Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false }</pre>	<pre>{ "statusCode": 201, "headers": { "Content-Type": "application/json", "My-Custom-Header": "Custom Value" }, "body": JSON.stringify({ "message": "Hello, world!" }), "isBase64Encoded": false }</pre>	<pre>HTTP/2 201 date: Wed, 08 Sep 2021 18:02:24 GMT content-type: application/json content-length: 27 my-custom-header: Custom Value
		
		{ "message": "Hello, world!" }</pre>

Cookies

Um Cookies von Ihrer Funktion zurückzugeben, fügen Sie `set-cookie`-Header nicht manuell hinzu. Fügen Sie stattdessen die Cookies in Ihr Antwortnutzlastobjekt ein. Lambda interpretiert

dies automatisch und fügt sie als `set-cookie`-Header in Ihre HTTP-Antwort ein, wie im folgenden Beispiel gezeigt.

Beispielausgabe für eine Antwort, die Cookies zurückgibt

Lambda-Funktionsausgabe	HTTP-Antwort (was der Client sieht)

```
{
   "statusCode": 201,
    "headers": {
        "Content-Type": "application/
json",
        "My-Custom-Header": "Custom
 Value"
    },
    "body": JSON.stringify({
        "message": "Hello, world!"
    }),
    "cookies": [
        "Cookie_1=Value1; Expires=21
 Oct 2021 07:48 GMT",
        "Cookie_2=Value2; Max-Age=7
8000"
    ],
    "isBase64Encoded": false
}
```

```
HTTP/2 201
date: Wed, 08 Sep 2021 18:02:24 GMT
content-type: application/json
content-length: 27
my-custom-header: Custom Value
set-cookie: Cookie_1=Value2;
 Expires=21 Oct 2021 07:48 GMT
set-cookie: Cookie_2=Value2; Max-
Age=78000

{
  "message": "Hello, world!"
}
```

Überwachen der Lambda-Funktions-URLs

Sie können Amazon verwenden AWS CloudTrail CloudWatch , um Ihre Funktions-URLs zu überwachen.

Themen

- Funktions-URLs überwachen mit CloudTrail
- CloudWatch Metriken für Funktions-URLs

Funktions-URLs überwachen mit CloudTrail

Für Funktions-URLs unterstützt Lambda automatisch die Protokollierung der folgenden API-Operationen als Ereignisse in CloudTrail Protokolldateien:

- CreateFunctionUrlConfig
- UpdateFunctionUrlConfig
- DeleteFunctionUrlConfig
- GetFunctionUrlConfig
- ListFunctionUrlConfigs

Jeder Protokolleintrag enthält Informationen über die Anruferidentität, wann die Anfrage gestellt wurde, und andere Details. In Ihrem CloudTrail Eventverlauf können Sie sich alle Ereignisse der letzten 90 Tage ansehen. Um Datensätze nach 90 Tagen beizubehalten, können Sie einen Trail erstellen.

Standardmäßig protokolliert CloudTrail es keine `InvokeFunctionUrl` Anfragen, die als Datenereignisse betrachtet werden. Sie können jedoch die Protokollierung von Datenereignissen aktivieren CloudTrail. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen für Trails im AWS CloudTrail -Benutzerhandbuch.

CloudWatch Metriken für Funktions-URLs

Lambda sendet aggregierte Metriken über Funktions-URL-Anfragen an. CloudWatch Mit diesen Metriken können Sie Ihre Funktions-URLs überwachen, Dashboards erstellen und Alarme in der Konsole konfigurieren. CloudWatch

Funktions-URLs unterstützen die folgenden Aufrufmetriken. Wir empfehlen, diese Metriken mit der `Sum`-Statistik anzuzeigen.

- `UrlRequestCount` – Die Anzahl der Anforderungen an diese Funktions-URL.
- `Url4xxCount` – Die Anzahl der Anforderungen, bei denen ein 4XX-HTTP-Statuscode zurückgegeben wurde. Codes der 4XX-Serie weisen auf clientseitige Fehler hin, z. B. schlechte Anforderungen.
- `Url5xxCount` – Die Anzahl der Anforderungen, bei denen ein 5XX-HTTP-Statuscode zurückgegeben wurde. Codes der 5XX-Serie weisen auf serverseitige Fehler wie Funktionsfehler und Timeouts hin.

Funktions-URLs unterstützen auch die folgende Leistungsmetrik. Wir empfehlen, diese Metriken mit der `Average`- oder `Max`-Statistik anzuzeigen.

- `UrlRequestLatency` – Die Zeit zwischen dem Erhalt der Funktions-URL eine Anforderung und wann die Funktions-URL eine Antwort zurückgibt.

Jede dieser Aufrufs- und Leistungsmetriken unterstützt die folgenden Dimensionen:

- `FunctionName` – Zeigt Aggregatmetriken für Funktions-URLs an, die der `$LATEST` unveröffentlichten Version oder einem der Aliase der Funktion zugeordnet sind. z. B. `hello-world-function`.
- `Resource` – Zeigt Metriken für eine bestimmte Funktions-URL an. Dies wird durch einen Funktionsnamen zusammen mit der `$LATEST` unveröffentlichten Version oder einem der Aliase der Funktion definiert. z. B. `hello-world-function:$LATEST`.
- `ExecutedVersion` – Zeigt Metriken für eine bestimmte Funktions-URL basierend auf der ausgeführten Version an. Sie können diese Dimension hauptsächlich verwenden, um die Funktions-URL zu verfolgen, die der `$LATEST`unveröffentlichten Version zugeordnet ist.

Tutorial: Erstellen einer Lambda-Funktion mit einer Funktions-URL

In diesem Tutorial erstellen Sie eine Lambda-Funktion, die als ZIP-Archiv mit einem öffentlichen Funktions-URL-Endpunkt definiert ist und das Produkt aus zwei Zahlen zurückgibt. Weitere Hinweise zum Konfigurieren von Funktions-URLs finden Sie unter Erstellen und Verwalten von Funktions-URLs.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Sofern noch nicht geschehen, befolgen Sie die Anweisungen unter Erstellen einer Lambda-Funktion mit der Konsole, um Ihre erste Lambda-Funktion zu erstellen.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen einer Ausführungsrolle

Erstellen Sie die Ausführungsrolle die Ihrer Lambda-Funktion die Berechtigung für den Zugriff auf AWS -Ressourcen erteilt.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Rollen der AWS Identity and Access Management (IAM-) Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie für Vertrauenswürdigen Entitätstyp AWS Service und dann für Anwendungsfall Lambda aus.
4. Wählen Sie Weiter aus.
5. Geben Sie im Bereich „Berechtigungsrichtlinien“ **`AWSLambdaBasicExecutionRole`** in das Suchfeld ein.
6. Aktivieren Sie das Kontrollkästchen neben der `AWSLambdaBasicExecutionRole` AWS verwalteten Richtlinie und wählen Sie dann Weiter aus.
7. Geben Sie **`lambda-url-role`** den Rollennamen ein und wählen Sie dann Rolle erstellen aus.

Die `AWSLambdaBasicExecutionRole` Richtlinie verfügt über die Berechtigungen, die die Funktion benötigt, um Protokolle in Amazon CloudWatch Logs zu schreiben. Später im Tutorial benötigen Sie den Amazon-Ressourcennamen (ARN) der Rolle, um Ihre Lambda-Funktion zu erstellen.

So finden Sie den ARN Ihrer Ausführungsrolle

1. Öffnen Sie die Seite Rollen der AWS Identity and Access Management (IAM-) Konsole.
2. Wählen Sie die Rolle aus, die Sie gerade erstellt haben (`lambda-url-role`).
3. Kopieren Sie im Übersichtsbereich den ARN.

Erstellen einer Lambda-Funktion mit einer Funktions-URL (ZIP-Dateiarchiv)

Erstellen Sie eine Lambda-Funktion mit einem Funktions-URL-Endpunkt mit einem ZIP-Dateiarchiv.

So erstellen Sie die Funktion

1. Kopieren Sie das folgende Codebeispiel in eine Datei mit dem Namen `index.js`.

Example index.js

```
exports.handler = async (event) => {
    let body = JSON.parse(event.body);
    const product = body.num1 * body.num2;
    const response = {
        statusCode: 200,
        body: "The product of " + body.num1 + " and " + body.num2 + " is " +
 product,
    };
    return response;
};
```

2. Erstellen Sie ein Bereitstellungspaket.

```
zip function.zip index.js
```

3. Erstellen Sie eine Lambda-Funktion mit dem Befehl `create-function`. Achten Sie darauf, den Rollen-ARN durch den ARN Ihrer eigenen Ausführungsrolle zu ersetzen, den Sie zuvor im Tutorial kopiert haben.

```
aws lambda create-function \
    --function-name my-url-function \
    --runtime nodejs18.x \
    --zip-file fileb://function.zip \
    --handler index.handler \
    --role arn:aws:iam::123456789012:role/lambda-url-role
```

4. Fügen Sie Ihrer Funktion eine ressourcenbasierte Richtlinie hinzu, die Berechtigungen für den öffentlichen Zugriff auf Ihre Funktions-URL gewährt.

```
aws lambda add-permission \
    --function-name my-url-function \
    --action lambda:InvokeFunctionUrl \
    --principal "*" \
    --function-url-auth-type "NONE" \
    --statement-id url
```

5. Erstellen Sie einen URL-Endpunkt für die Funktion mit dem Befehl `create-function-url-config`.

```
aws lambda create-function-url-config \
    --function-name my-url-function \
    --auth-type NONE
```

Testen des Funktions-URL-Endpunkts

Rufen Sie Ihre Lambda-Funktion auf, indem Sie Ihren Funktions-URL-Endpunkt mit einem HTTP-Client wie curl oder Postman aufrufen.

```
curl 'https://abcdefg.lambda-url.us-east-1.on.aws/' \
-H 'Content-Type: application/json' \
-d '{"num1": "10", "num2": "10"}'
```

Die Ausgabe sollte folgendermaßen aussehen:

```
The product of 10 and 10 is 100
```

Erstellen Sie eine Lambda-Funktion mit einer Funktions-URL () CloudFormation

Sie können mithilfe des AWS CloudFormation Typs `AWS::Lambda::Url` auch eine Lambda-Funktion mit einem Funktions-URL-Endpunkt erstellen.

```
Resources:
  MyUrlFunction:
    Type: AWS::Lambda::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs18.x
      Role: arn:aws:iam::123456789012:role/lambda-url-role
      Code:
        ZipFile: |
          exports.handler = async (event) => {
              let body = JSON.parse(event.body);
              const product = body.num1 * body.num2;
              const response = {
                  statusCode: 200,
                  body: "The product of " + body.num1 + " and " + body.num2 + " is " +
 product,
              };
```

```
            return response;
        };
    Description: Create a function with a URL.
  MyUrlFunctionPermissions:
    Type: AWS::Lambda::Permission
    Properties:
      FunctionName: !Ref MyUrlFunction
      Action: lambda:InvokeFunctionUrl
      Principal: "*"
      FunctionUrlAuthType: NONE
  MyFunctionUrl:
    Type: AWS::Lambda::Url
    Properties:
      TargetFunctionArn: !Ref MyUrlFunction
      AuthType: NONE
```

Erstellen einer Lambda-Funktion mit einer Funktions-URL (AWS SAM)

Sie können mit AWS Serverless Application Model (AWS SAM) auch eine Lambda-Funktion erstellen, die mit einer Funktions-URL konfiguriert ist.

```
ProductFunction:
  Type: AWS::Serverless::Function
  Properties:
    CodeUri: function/.
    Handler: index.handler
    Runtime: nodejs18.x
    AutoPublishAlias: live
    FunctionUrlConfig:
      AuthType: NONE
```

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.

3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

AWS Lambda Funktionen verwalten

Erfahren Sie, wie Sie die mit Ihrer Lambda-Funktion verknüpften Ressourcen mithilfe der Lambda-API oder -Konsole anpassen und sichern.

[Verwenden von Lambda mit dem AWS CLI]

Sie können den verwenden AWS Command Line Interface , um Funktionen und andere AWS Lambda Ressourcen zu verwalten. Das AWS CLI verwendet die AWS SDK for Python (Boto) , um mit der Lambda-API zu interagieren. In diesem Tutorial werden Sie Lambda-Funktionen mit der AWS CLI verwalten und aufrufen.

[Funktionsskalierung]

Sie können zwei Steuerelemente für die Gleichzeitigkeit auf Funktionsebene konfigurieren: reservierte Gleichzeitigkeit und bereitgestellte Gleichzeitigkeit. Die Gleichzeitigkeit ist die Anzahl der aktiven Instances Ihrer Funktion und kann so konfiguriert werden, dass kritische Funktionen nicht gedrosselt werden.

[Codesignatur]

Code Signing for Lambda bietet Vertrauens- und Integritätskontrollen, mit denen Sie überprüfen können, ob nur von genehmigten Entwicklern veröffentlichter unveränderter Code in Ihren Lambda-Funktionen bereitgestellt wird.

[Mit Tags organisieren]

Sie können Lambda-Funktionen markieren, um die [attributbasierte Zugriffskontrolle (ABAC)] zu aktivieren und diese nach Eigentümer, Projekt oder Abteilung zu organisieren.

[Verwenden von Ebenen]

Sie können zuvor erstellte Ebenen anwenden, um die Größe des Bereitstellungspakets zu reduzieren und die gemeinsame Nutzung von Code und die Trennung von Verantwortlichkeiten zu unterstützen, damit Sie beim Schreiben der Geschäftslogik schneller iterieren können.

Verwenden von Lambda mit der AWS CLI

Sie können die AWS Command Line Interface verwenden, um Funktionen und andere AWS Lambda-Ressourcen zu verwalten. Die AWS CLI verwendet die AWS SDK for Python (Boto) für die Interaktion mit der Lambda-API. Sie können damit mehr über die API erfahren und dieses Wissen für die Entwicklung von Anwendungen, die Lambda mit dem AWS-SDK verwenden, nutzen.

In diesem Tutorial werden Sie Lambda-Funktionen mit der AWS CLI verwalten und aufrufen. Weitere Informationen finden Sie unter Was ist AWS CLI? im AWS Command Line Interface-Benutzerhandbuch.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über Kenntnisse zu den grundlegenden Lambda-Operationen und der Lambda-Konsole verfügen. Wenn Sie es noch nicht getan haben, folgen Sie den Anweisungen in the section called “Erstellen einer Lambda-Funktion mit der Konsole”.

Um die folgenden Schritte durchzuführen, benötigen Sie die AWS Command Line Interface (AWS CLI) Version 2. Befehle und die erwartete Ausgabe werden in separaten Blöcken aufgeführt:

```
aws --version
```

Die Ausgabe sollte folgendermaßen aussehen:

```
aws-cli/2.13.27 Python/3.11.6 Linux/4.14.328-248.540.amzn2.x86_64 exe/x86_64.amzn.2
```

Bei langen Befehlen wird ein Escape-Zeichen (\) wird verwendet, um einen Befehl über mehrere Zeilen zu teilen.

Verwenden Sie auf Linux und macOS Ihren bevorzugten Shell- und Paket-Manager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux. Die CLI-Beispielbefehle in diesem Handbuch verwenden die Linux-Formatierung. Befehle, die Inline-JSON-Dokumente enthalten, müssen neu formatiert werden, wenn Sie die Windows-CLI verwenden.

Erstellen der Ausführungsrolle

Erstellen Sie die Ausführungsrolle die Ihrer Funktion die Berechtigung für den Zugriff auf AWS-Ressourcen erteilt. Verwenden Sie den Befehl AWS CLI, um eine Ausführungsrolle mit der `create-role` zu erstellen.

Im folgenden Beispiel geben Sie die Vertrauensrichtlinie inline an. Die Anforderungen für Escape-Anführungszeichen in der JSON-Zeichenfolge variieren je nach Shell.

```
aws iam create-role --role-name lambda-ex --assume-role-policy-document '{"Version":
 "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service":
 "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}'
```

Sie können die Vertrauensrichtlinie für die Rolle auch mithilfe einer JSON-Datei definieren. Im folgenden Beispiel ist `trust-policy.json` eine Datei im aktuellen Verzeichnis. Diese Vertrauensrichtlinie ermöglicht es Lambda, die Berechtigungen der Rolle zu verwenden, indem es dem Service-Prinzipal `lambda.amazonaws.com` die Erlaubnis erteilt, die Aktion AWS Security Token Service (AWS STS) `AssumeRole` aufzurufen.

Example trust-policy.json

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

```
aws iam create-role --role-name lambda-ex --assume-role-policy-document file://trust-
policy.json
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "lambda-ex",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/lambda-ex",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "lambda.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Um der Rolle Berechtigungen hinzuzufügen, verwenden Sie den attach-policy-to-role-Befehl. Beginnen Sie mit dem Hinzufügen der `AWSLambdaBasicExecutionRole` verwalteten Richtlinie.

```
aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole
```

Die AWSLambdaBasicExecutionRole Richtlinie verfügt über die Berechtigungen, die die Funktion zum Schreiben von Protokollen in CloudWatch -Protokolle benötigt.

Erstellen der Funktion

Das folgende Beispiel protokolliert die Werte der Umgebungsvariablen und des Ereignisobjekts.

Example index.js

```
exports.handler = async function(event, context) {
  console.log("ENVIRONMENT VARIABLES\n" + JSON.stringify(process.env, null, 2))
  console.log("EVENT\n" + JSON.stringify(event, null, 2))
  return context.logStreamName
}
```

So erstellen Sie die Funktion

1. Kopieren Sie den Beispiel-Code in eine Datei mit dem Namen `index.js`.
2. Erstellen Sie ein Bereitstellungspaket.

```
zip function.zip index.js
```

3. Erstellen Sie eine Lambda-Funktion mit dem Befehl `create-function`. Ersetzen Sie den markierten Text im Rollen-ARN durch Ihre Konto-ID.

```
aws lambda create-function --function-name my-function \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs20.x \
--role arn:aws:iam::123456789012:role/lambda-ex
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "FunctionName": "my-function",
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
    "Runtime": "nodejs20.x",
    "Role": "arn:aws:iam::123456789012:role/lambda-ex",
    "Handler": "index.handler",
    "CodeSha256": "FpFMvUhayLkOoVBpNuNiIVML/tuGv2iJQ7t0yWVTU8c=",
    "Version": "$LATEST",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "88ebe1e1-bfdf-4dc3-84de-3017268fa1ff",
    ...
}
```

Um Protokolle für einen Aufruf über die Befehlszeile abzurufen, verwenden Sie die Option `--log-type`. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Mit dem Dienstprogramm `base64` können Sie die Protokolle dekodieren.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text |  base64 -d
```

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
  "AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Serviceprogramm ist nur in Linux, macOS und Ubuntu auf Windows verfügbar. Im Fall von macOS lautet der Befehl `base64 -D`.

Um vollständige Protokollereignisse über die Befehlszeile zu erhalten, können Sie den Namen des Protokoll-Streams in die Ausgabe Ihrer Funktion einschließen, wie im voranstehenden Beispiel veranschaulicht. Das folgende Beispielskript ruft eine Funktion mit dem Namen `my-function` auf und lädt die letzten fünf Protokollereignisse herunter.

Example get-logs.sh-Skript

Dieses Beispiel erfordert, dass `my-function` eine Protokoll-Stream-ID zurückgibt.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-name
 $(cat out) --limit 5
```

Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
```

```
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Aktualisieren der Funktion

Nachdem Sie eine Funktion erstellt haben, können Sie zusätzliche Funktionen für die Funktion konfigurieren, z. B. Auslöser, Netzwerkzugriff und Dateisystemzugriff. Sie können auch Ressourcen anpassen, die mit der Funktion verknüpft sind, wie Arbeitsspeicher und Gleichzeitigkeit. Diese Konfigurationen gelten für Funktionen, die als ZIP-Dateiarchive definiert sind und für Funktionen, die als Container-Images definiert sind.

Verwenden Sie den update-function-configuration Befehl , um Funktionen zu konfigurieren. Im folgenden Beispiel wird der Funktionsspeicher auf 256 MB gesetzt.

Example update-function-configuration -Befehl

```
aws lambda update-function-configuration \
--function-name my-function \
--memory-size 256
```

Auflisten der Lambda-Funktionen in Ihrem Konto

Führen Sie den folgenden AWS CLI-Befehl `list-functions` aus, um eine Liste von Funktionen abzurufen, die Sie erstellt haben.

```
aws lambda list-functions --max-items 10
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Functions": [
        {
            "FunctionName": "cli",
```

```
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function",
            "Runtime": "nodejs20.x",
            "Role": "arn:aws:iam::123456789012:role/lambda-ex",
            "Handler": "index.handler",
            ...
        },
        {
            "FunctionName": "random-error",
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:random-
error",
            "Runtime": "nodejs20.x",
            "Role": "arn:aws:iam::123456789012:role/lambda-role",
            "Handler": "index.handler",
            ...
        },
        ...
      ],
      "NextToken": "eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMH0="
}
```

Als Reaktion gibt Lambda eine Liste von bis zu 10 Funktionen zurück. Wenn weitere Funktionen vorhanden sind, die Sie abrufen können, stellt `NextToken` eine Markierung bereit, die Sie in der nächsten `list-functions`-Anforderung verwenden können. Der folgende `list-functions` AWS CLI-Befehl zeigt den Parameter `--starting-token`.

```
aws lambda list-functions --max-items 10 --starting-
token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxMH0=
```

Abrufen einer Lambda-Funktion

Der Lambda-CLI-Befehl `get-function` gibt Lambda-Funktionsmetadaten sowie eine vorsignierte URL zurück, die Sie zum Herunterladen des Bereitstellungspakets der Funktion nutzen können.

```
aws lambda get-function --function-name my-function
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Configuration": {
        "FunctionName": "my-function",
```

```
        "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
        "Runtime": "nodejs20.x",
        "Role": "arn:aws:iam::123456789012:role/lambda-ex",
        "CodeSha256": "FpFMvUhayLkOoVBpNuNiIVML/tuGv2iJQ7t0yWVTU8c=",
        "Version": "$LATEST",
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "RevisionId": "88ebe1e1-bfdf-4dc3-84de-3017268fa1ff",
        ...
    },
    "Code": {
        "RepositoryType": "S3",
        "Location": "https://awslambda-us-east-2-tasks.s3.us-east-2.amazonaws.com/
snapshots/123456789012/my-function-4203078a-b7c9-4f35-..."
    }
}
```

Weitere Informationen finden Sie unter GetFunction.

Bereinigen

Führen Sie den folgenden `delete-function`-Befehl aus, um die `my-function`-Funktion zu löschen.

```
aws lambda delete-function --function-name my-function
```

Löschen Sie die IAM-Rolle, die Sie in der IAM-Konsole erstellt haben. Weitere Informationen zum Löschen von Rollen finden Sie unter Löschen von Rollen oder Instance-Profilen im IAM-Benutzerhandbuch.

Die Lambda-Funktionsskalierung verstehen

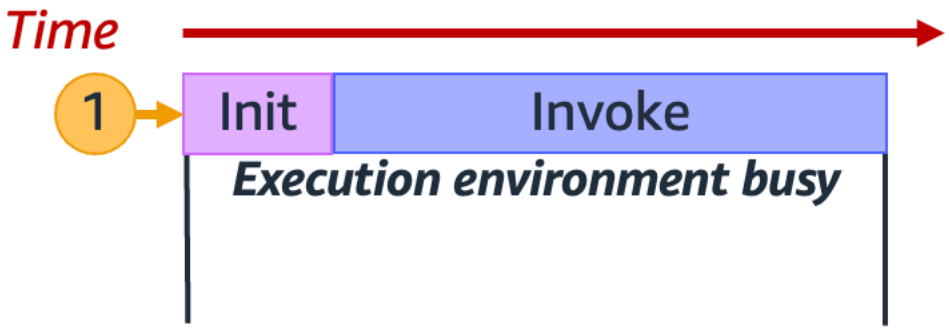
Parallelität ist die Anzahl der laufenden Anfragen, die Ihre AWS Lambda Funktion gleichzeitig bearbeitet. Für jede gleichzeitige Anfrage stellt Lambda eine separate Instance Ihrer Ausführungsumgebung bereit. Wenn Ihre Funktionen mehr Anfragen erhalten, sorgt Lambda automatisch für die Skalierung der Anzahl der Ausführungsumgebungen, bis Sie das Gleichzeitigkeitslimit für Ihr Konto erreichen. Standardmäßig stellt Lambda Ihrem Konto eine Gesamtnebenläufigkeitsgrenze von 1 000 gleichzeitigen Ausführungen für alle Funktionen in einer AWS-Region bereit. Um Ihre speziellen Kontoanforderungen zu unterstützen, können Sie eine Kontingenterhöhung anfordern und Gleichzeitigkeitskontrollen auf Funktionsebene konfigurieren, damit Ihre kritischen Funktionen nicht gedrosselt werden.

In diesem Thema werden Parallelitätskonzepte und Funktionsskalierung in Lambda erklärt. Am Ende dieses Themas werden Sie in der Lage sein, die Gleichzeitigkeit zu berechnen, die beiden Hauptoptionen für die Gleichzeitigkeitskontrolle (reserviert und bereitgestellt) zu visualisieren, geeignete Einstellungen für die Gleichzeitigkeitskontrolle zu schätzen und Metriken zur weiteren Optimierung anzuzeigen.

Sections

Verstehen und Visualisieren der Gleichzeitigkeit

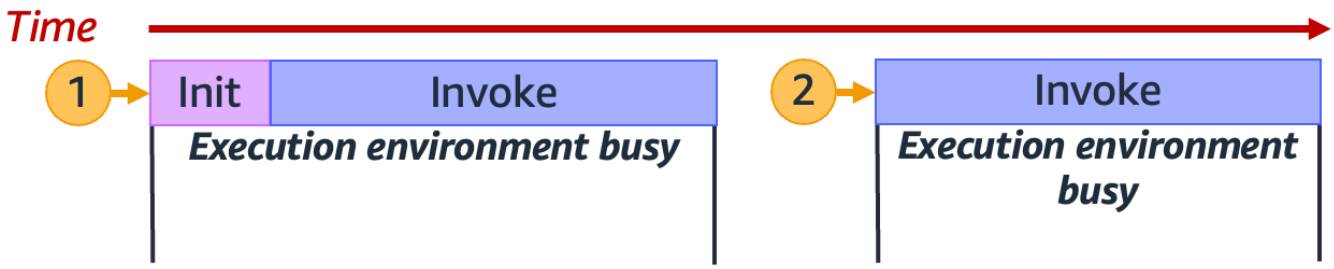
Lambda ruft Ihre Funktion in einer sicheren und isolierten Ausführungsumgebung auf. Um eine Anfrage zu bearbeiten, muss Lambda zuerst eine Ausführungsumgebung initialisieren (die Initialisierungsphase), bevor es zum Aufrufen Ihrer Funktion verwendet wird (die Aufrufphase):



> **Note**
>
> Die tatsächliche Initialisierungs- und Aufrufdauer kann von vielen Faktoren abhängen, z. B. von der von Ihnen ausgewählten Laufzeit und dem Lambda-Funktionscode. Das vorherige Diagramm soll nicht die genauen Proportionen der Initiierungs- und Aufrufphasendauer darstellen.

Im vorherigen Diagramm wird ein Rechteck verwendet, um eine einzelne Ausführungsumgebung darzustellen. Wenn Ihre Funktion ihre allererste Anfrage erhält (dargestellt durch den gelben Kreis mit der Bezeichnung 1), erstellt Lambda eine neue Ausführungsumgebung und führt den Code während der Initialisierungsphase außerhalb Ihres Haupthandlers aus. Anschließend führt Lambda den Haupthandlercode Ihrer Funktion während der Aufrufphase aus. Während des gesamten Prozesses ist diese Ausführungsumgebung ausgelastet und kann keine anderen Anfragen verarbeiten.

Wenn Lambda die Verarbeitung der ersten Anfrage abgeschlossen hat, kann diese Ausführungsumgebung weitere Anfragen für dieselbe Funktion verarbeiten. Für nachfolgende Anfragen muss Lambda die Umgebung nicht neu initialisieren.

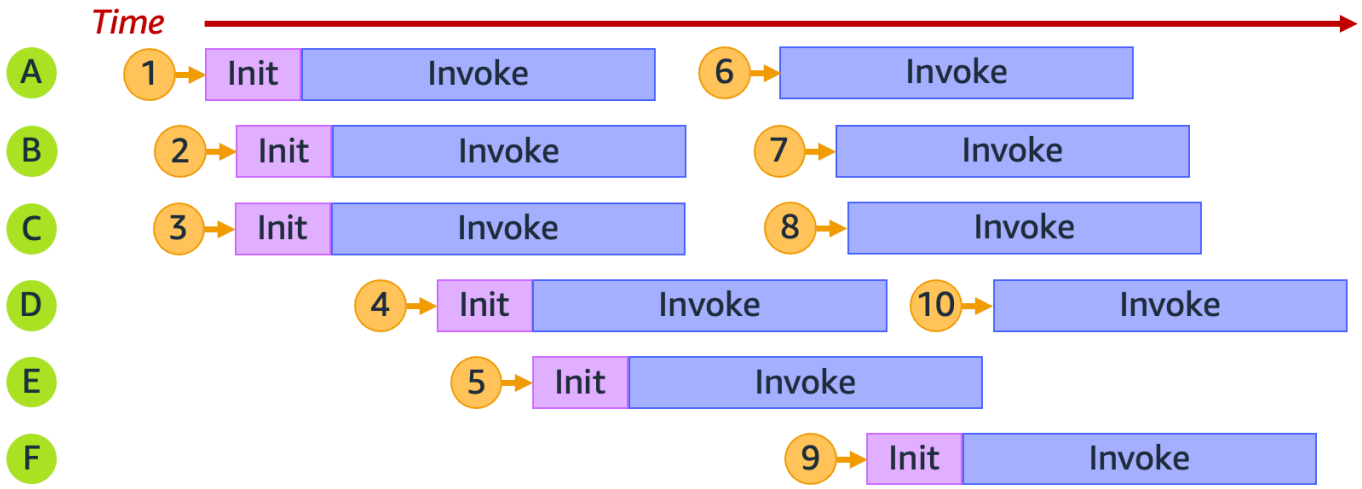


Im vorherigen Diagramm verwendet Lambda die Ausführungsumgebung erneut, um die zweite Anfrage zu verarbeiten (dargestellt durch den gelben Kreis mit der Bezeichnung 2).

Bisher haben wir uns nur auf eine einzige Instance Ihrer Ausführungsumgebung konzentriert (d. h. eine Gleichzeitigkeit von 1). In der Praxis muss Lambda möglicherweise mehrere Instances der Ausführungsumgebung parallel bereitstellen, um alle eingehenden Anfragen zu verarbeiten. Wenn Ihre Funktion eine neue Anfrage erhält, können zwei Dinge passieren:

- Wenn eine vorinitialisierte Instance der Ausführungsumgebung verfügbar ist, verwendet Lambda diese, um die Anfrage zu verarbeiten.
- Andernfalls erstellt Lambda eine neue Instance der Ausführungsumgebung, um die Anfrage zu verarbeiten.

Lassen Sie uns beispielsweise untersuchen, was passiert, wenn Ihre Funktion 10 Anfragen erhält:



Im vorherigen Diagramm stellt jede horizontale Ebene eine einzelne Instance der Ausführungsumgebung dar (von A bis F). So behandelt Lambda jede Anfrage:

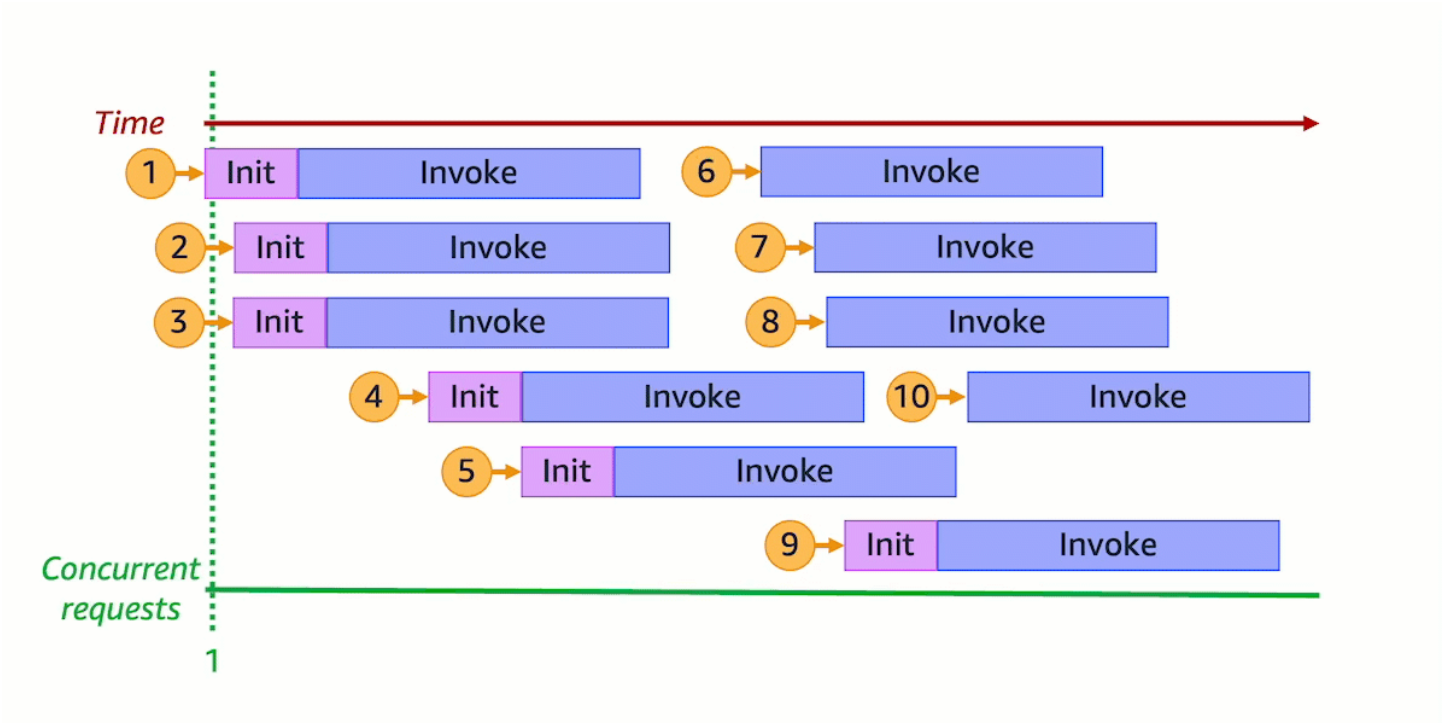
Lambda-Verhalten für Anfragen 1 bis 10

Anforderung	Lambda-Verhalten	Reasoning
1	Stellt neue Umgebung A bereit	Dies ist die erste Anfrage. Es sind keine Instances der Ausführungsumgebung verfügbar

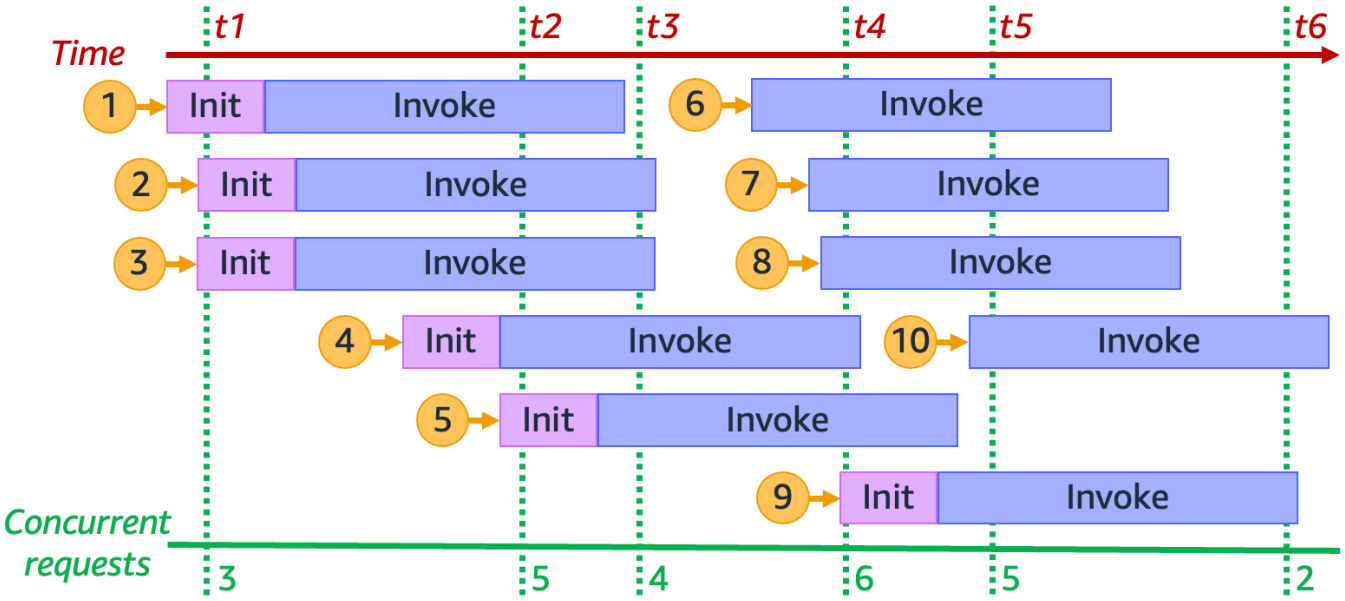
Anforderung	Lambda-Verhalten	Reasoning
2	Stellt neue Umgebung B bereit	Die vorhandene Instance der Ausführungsumgebung A ist ausgelastet
3	Stellt neue Umgebung C bereit	Die vorhandenen Instances der Ausführungsumgebung A und B sind beide ausgelastet
4	Stellt neue Umgebung D bereit	Die vorhandenen Instances der Ausführungsumgebung A, B und C sind alle ausgelastet
5	Stellt neue Umgebung E bereit	Die vorhandenen Instances der Ausführungsumgebung A, B, C und D sind alle ausgelast et
6	Wiederverwendung von Umgebung A	Die Instance der Ausführun gsumgebung A hat die Verarbeitung von Anfrage 1 abgeschlossen und ist jetzt verfügbar
7	Wiederverwendung von Umgebung B	Die Instance der Ausführun gsumgebung B hat die Verarbeitung von Anfrage 2 abgeschlossen und ist jetzt verfügbar
8	Wiederverwendung von Umgebung C	Die Instance der Ausführun gsumgebungB hat die Verarbeitung von Anfrage 3 abgeschlossen und ist jetzt verfügbar

Anforderung	Lambda-Verhalten	Reasoning
9	Stellt neue Umgebung F bereit	Die vorhandenen Instances der Ausführungsumgebung A, B, C, D und E sind alle ausgelastet
10	Wiederverwendung von Umgebung D	Die Instance der Ausführungsumgebung D hat die Verarbeitung von Anfrage 4 abgeschlossen und ist jetzt verfügbar

Wenn Ihre Funktion mehr gleichzeitige Anfragen erhält, erhöht Lambda als Reaktion darauf die Anzahl der Instances der Ausführungsumgebung. Die folgende Animation verfolgt die Anzahl der gleichzeitigen Anfragen im Laufe der Zeit:



Durch das Einfrieren der vorherigen Animation an sechs verschiedenen Zeitpunkten erhalten wir das folgende Diagramm:



Im vorherigen Diagramm können wir zu jedem Zeitpunkt eine vertikale Linie zeichnen und die Anzahl der Umgebungen zählen, die diese Linie schneiden. Dadurch erhalten wir die Anzahl der gleichzeitigen Anfragen zu diesem Zeitpunkt. Beispielsweise gibt es zum Zeitpunkt `t1` drei aktive Umgebungen, die drei gleichzeitige Anfragen bearbeiten. Die maximale Anzahl gleichzeitiger Anfragen in dieser Simulation wird zum Zeitpunkt `t4` erreicht, an dem sechs aktive Umgebungen sechs gleichzeitige Anfragen bearbeiten.

Zusammengefasst beschreibt die Gleichzeitigkeit Ihrer Funktion die Anzahl der Anfragen, die diese gleichzeitig verarbeitet. Als Reaktion auf eine Zunahme der Gleichzeitigkeit Ihrer Funktion stellt Lambda mehr Instances der Ausführungsumgebung bereit, um die Anfragenachfrage zu erfüllen.

Berechnung der Parallelität für eine Funktion

Im Allgemeinen ist die Gleichzeitigkeit eines Systems die Fähigkeit, mehr als eine Aufgabe gleichzeitig zu bearbeiten. In Lambda beschreibt die Gleichzeitigkeit die Anzahl der Anfragen, die Ihre Funktion gleichzeitig bearbeitet. Eine schnelle und praktische Methode zur Messung der Gleichzeitigkeit einer Lambda-Funktion ist die Verwendung der folgenden Formel:

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

Gleichzeitigkeit unterscheidet sich von Anfragen pro Sekunde. Nehmen wir beispielsweise an, Ihre Funktion erhält durchschnittlich 100 Anfragen pro Sekunde. Wenn die durchschnittliche Dauer einer Anfrage 1 Sekunde beträgt, beträgt die Nebenläufigkeit ebenfalls 100:

```
Concurrency = (100 requests/second) * (1 second/request) = 100
```

Wenn die durchschnittliche Anfragedauer jedoch 500 ms beträgt, liegt die Nebenläufigkeit bei 50:

```
Concurrency = (100 requests/second) * (0.5 second/request) = 50
```

Was bedeutet eine Gleichzeitigkeit von 50 in der Praxis? Wenn die durchschnittliche Anfragedauer 500 ms beträgt, können Sie davon ausgehen, dass eine Instance Ihrer Funktion zwei Anfragen pro Sekunde verarbeiten kann. Dementsprechend sind 50 Instances Ihrer Funktion erforderlich, um eine Last von 100 Anfragen pro Sekunde zu verarbeiten. Eine Gleichzeitigkeit von 50 bedeutet, dass Lambda 50 Instances der Ausführungsumgebung bereitstellen muss, um diesen Workload ohne Drosselung effizient zu bewältigen. So drückt man dies in Gleichungsform aus:

```
Concurrency = (100 requests/second) / (2 requests/second) = 50
```

Wenn Ihre Funktion die doppelte Anzahl von Anfragen empfängt (200 Anfragen pro Sekunde), aber nur die Hälfte der Zeit benötigt, um jede Anfrage zu verarbeiten (250 ms), beträgt die Nebenläufigkeit immer noch 50:

```
Concurrency = (200 requests/second) * (0.25 second/request) = 50
```

Testen Sie Ihr Verständnis von Gleichzeitigkeit

Angenommen, Sie haben eine Funktion, deren Ausführung im Durchschnitt 200 ms benötigt. Während der Spitzenlast beobachten Sie 5 000 Anfragen pro Sekunde. Wie hoch ist die Gleichzeitigkeit Ihrer Funktion während der Spitzenlast?

Antwort

Die durchschnittliche Funktionsdauer beträgt 200 ms oder 0,2 Sekunden. Mithilfe der Nebenläufigkeitsformel können Sie die Zahlen einfügen, um eine Nebenläufigkeit von 1 000 zu erhalten:

```
Concurrency = (5,000 requests/second) * (0.2 seconds/request) = 1,000
```

Alternativ bedeutet eine durchschnittliche Funktionsdauer von 200 ms, dass Ihre Funktion 5 Anfragen pro Sekunde verarbeiten kann. Um den Workload von 5 000 Anfragen pro Sekunde zu bewältigen, benötigen Sie 1 000 Instances der Ausführungsumgebung. Die Gleichzeitigkeit beträgt also 1 000:

```
Concurrency = (5,000 requests/second) / (5 requests/second) = 1,000
```

Unterscheidung zwischen Parallelität und Anfragen pro Sekunde

Wie im vorherigen Abschnitt erwähnt, unterscheidet sich die Gleichzeitigkeit von den Anforderungen pro Sekunde. Diese Unterscheidung ist besonders wichtig, wenn Sie mit Funktionen arbeiten, die eine durchschnittliche Anforderungsdauer von weniger als 100 ms haben.

In der Regel kann jede Instance Ihrer Ausführungsumgebung maximal 10 Anforderungen pro Sekunde bearbeiten. Dieser Grenzwert gilt für synchrone On-Demand-Funktionen sowie für Funktionen, die bereitgestellte Nebenläufigkeit verwenden. Wenn Sie mit diesem Grenzwert nicht vertraut sind, wissen Sie vielleicht nicht, warum es bei solchen Funktionen in bestimmten Szenarien zu einer Drosselung kommen kann.

Stellen Sie sich etwa eine Funktion mit einer durchschnittlichen Anforderungsdauer von 50 ms vor. Bei 200 Anforderungen pro Sekunde lautet die Gleichzeitigkeit dieser Funktion wie folgt:

```
Concurrency = (200 requests/second) * (0.05 second/request) = 10
```

Aufgrund dieses Ergebnisses ließe sich davon ausgehen, dass Sie nur 10 Instances der Ausführungsumgebung benötigen, um diese Last zu bewältigen. Die jeweilige Ausführungsumgebung kann jedoch nur 10 Ausführungen pro Sekunde verarbeiten. Das bedeutet, dass Ihre Funktion bei 10 Ausführungsumgebungen von insgesamt 200 Anforderungen nur 100 Anforderungen pro Sekunde verarbeiten kann. Bei dieser Funktion kommt es zu einer Drosselung.

Fazit: Sie müssen bei der Konfiguration der Nebenläufigkeitseinstellungen für Ihre Funktionen sowohl Nebenläufigkeit als auch Anforderungen pro Sekunde berücksichtigen. In diesem Fall benötigen Sie 20 Ausführungsumgebungen für Ihre Funktion, obwohl sie nur eine Nebenläufigkeit von 10 hat.

Testen Sie Ihr Verständnis von Gleichzeitigkeit (Funktionen unter 100 ms)

Angenommen, Sie haben eine Funktion, deren Ausführung im Durchschnitt 20 ms benötigt. Während der Spitzenlast beobachten Sie 3 000 Anfragen pro Sekunde. Wie hoch ist die Gleichzeitigkeit Ihrer Funktion während der Spitzenlast?

Antwort

Die durchschnittliche Funktionsdauer beträgt 20 ms oder 0,02 Sekunden. Mit der Gleichzeitigkeitsformel können Sie die Zahlen einfügen, um eine Gleichzeitigkeit von 60 zu erhalten:

```
Concurrency = (3,000 requests/second) * (0.02 seconds/request) = 60
```

Die jeweilige Ausführungsumgebung kann jedoch nur 10 Anforderungen pro Sekunde verarbeiten. Bei 60 Ausführungsumgebungen kann Ihre Funktion maximal 600 Anforderungen pro Sekunde verarbeiten. Um die 3 000 Anforderungen vollständig bearbeiten zu können, benötigt Ihre Funktion mindestens 300 Instances der Ausführungsumgebung.

Grundlegendes zur reservierten Parallelität und zur bereitgestellten Parallelität

Standardmäßig verfügt Ihr Konto über eine Nebenläufigkeitsgrenze von 1 000 gleichzeitigen Ausführungen für alle Funktionen in einer Region. Ihre Funktionen teilen sich diesen Pool von 1 000 gleichzeitigen Anwendungen auf Bedarfsbasis. Ihre Funktionen werden gedrosselt (d. h. sie beginnen, Anfragen zu verwerfen), wenn Ihnen die verfügbare Nebenläufigkeit ausgeht.

Einige Ihrer Funktionen sind möglicherweise kritischer als andere. Daher sollten Sie die Nebenläufigkeitseinstellungen konfigurieren, um sicherzustellen, dass kritische Funktionen die benötigte Gleichzeitigkeit erhalten. Es gibt zwei Arten von Gleichzeitigkeitskontrollen: reservierte Gleichzeitigkeit und bereitgestellte Gleichzeitigkeit.

- Verwenden Sie die reservierte Gleichzeitigkeit, um einen Teil der Gleichzeitigkeit Ihres Kontos für eine Funktion zu reservieren. Dies ist nützlich, wenn Sie nicht möchten, dass andere Funktionen die gesamte verfügbare nicht reservierte Gleichzeitigkeit in Anspruch nehmen.
- Verwenden Sie die bereitgestellte Gleichzeitigkeit, um eine Reihe von Umgebungs-Instances für eine Funktion vorab zu initialisieren. Dies ist nützlich, um Kaltstartlatenzen zu reduzieren.

Reservierte Gleichzeitigkeit

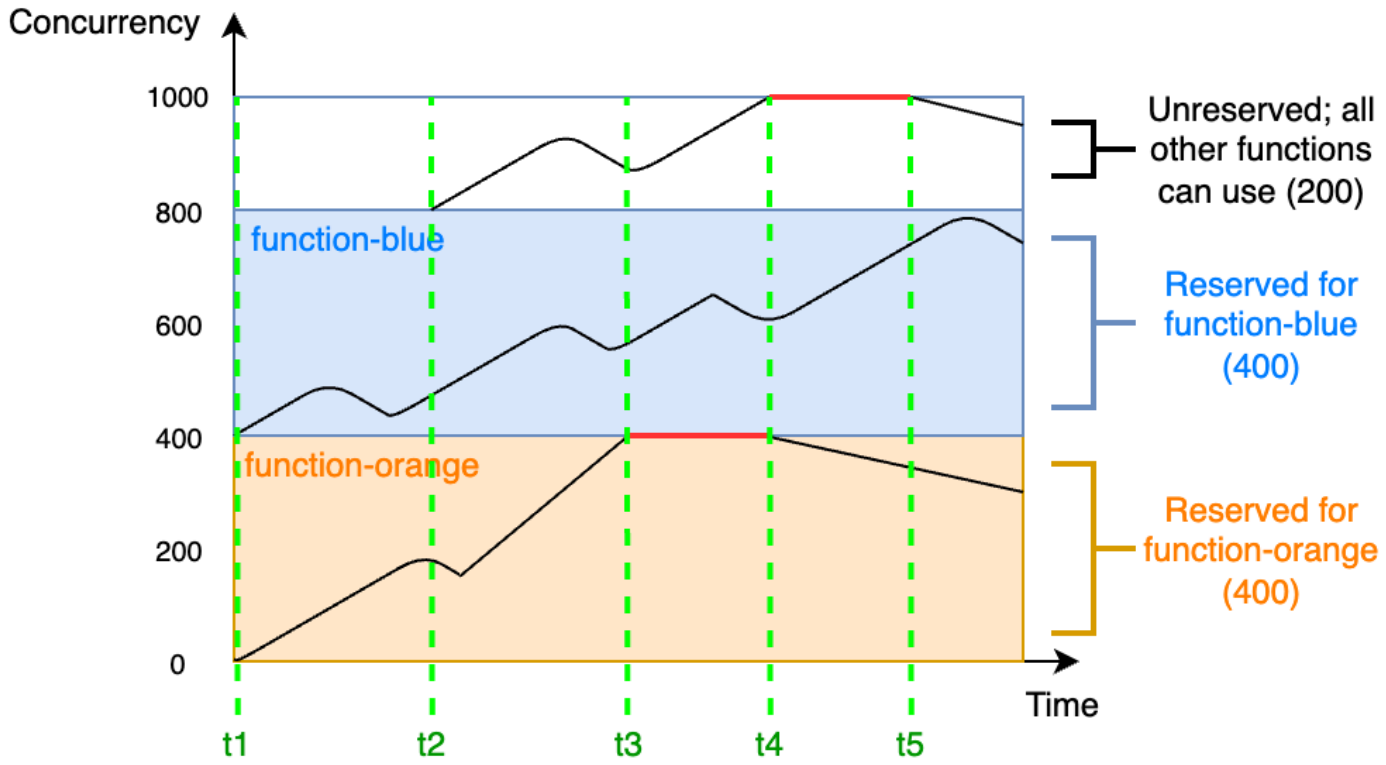
Wenn Sie sicherstellen möchten, dass für Ihre Funktion jederzeit ein gewisses Maß an Gleichzeitigkeit verfügbar ist, verwenden Sie reservierte Gleichzeitigkeit.

Reservierte Nebenläufigkeit ist die maximale Anzahl der gleichzeitigen Instances, die Sie Ihrer Funktion zuweisen möchten. Wenn Sie einer Funktion reservierte Gleichzeitigkeit zuweisen,

kann keine andere Funktion diese Gleichzeitigkeit nutzen. Mit anderen Worten, das Festlegen von reservierter Gleichzeitigkeit kann sich auf den Gleichzeitigkeits-Pool auswirken, der anderen Funktionen zur Verfügung steht. Funktionen, die nicht über reservierte Gleichzeitigkeit verfügen, teilen sich den verbleibenden Pool an nicht reservierter Gleichzeitigkeit.

Das Konfigurieren der reservierten Gleichzeitigkeit wird auf das gesamte Gleichzeitigkeitslimit Ihres Kontos angerechnet. Für die Konfiguration reservierter Gleichzeitigkeit für eine Funktion wird keine Gebühr erhoben.

Betrachten Sie das folgende Diagramm, um die reservierte Gleichzeitigkeit besser zu verstehen:



In diesem Diagramm ist das Gleichzeitigkeitslimit Ihres Kontos für alle Funktionen in diesem Bereich auf das Standardlimit von 1 000 festgelegt. Angenommen, Sie haben zwei kritische Funktionen, `function-blue` und `function-orange`, die routinemäßig hohe Aufrufvolumina erwarten. Sie entscheiden sich, 400 Einheiten reservierter Gleichzeitigkeit für `function-blue` und 400 Einheiten reservierter Gleichzeitigkeit für `function-orange` einzusetzen. In diesem Beispiel müssen sich alle anderen Funktionen in Ihrem Konto die verbleibenden 200 Einheiten an nicht reservierter Gleichzeitigkeit teilen.

Das Diagramm enthält fünf wichtige Punkte:

- Bei `t1` beginnen sowohl `function-orange` als auch `function-blue` mit dem Empfang von Anfragen. Jede Funktion beginnt, ihren zugewiesenen Teil der reservierten Gleichzeitigkeitseinheiten zu verbrauchen.
- Bei `t2` erhalten `function-orange` und `function-blue` stetig mehr Anfragen. Gleichzeitig stellen Sie einige andere Lambda-Funktionen bereit, die mit dem Empfang von Anfragen beginnen. Sie weisen diesen anderen Funktionen keine reservierte Nebenläufigkeit zu. Diese beginnen mit der Verwendung der verbleibenden 200 Einheiten der nicht reservierten Gleichzeitigkeit.
- Bei `t3` erreicht `function-orange` die maximale Gleichzeitigkeit von 400. Obwohl es an anderer Stelle in Ihrem Konto ungenutzte Gleichzeitigkeit gibt, kann `function-orange` nicht darauf zugreifen. Die rote Linie zeigt an, dass `function-orange` gedrosselt wird und Lambda-Anfragen möglicherweise verwirft.
- Bei `t4` beginnt `function-orange` weniger Anfragen zu erhalten und wird nicht mehr gedrosselt. Ihre anderen Funktionen erfahren jedoch einen Anstieg des Datenverkehrs und werden gedrosselt. Obwohl es an anderer Stelle in Ihrem Konto ungenutzte Gleichzeitigkeit gibt, können diese anderen Funktionen nicht darauf zugreifen. Die rote Linie zeigt an, dass Ihre anderen Funktionen gedrosselt werden.
- Bei `t5` beginnen andere Funktionen weniger Anfragen zu erhalten und werden nicht mehr gedrosselt.

Anhand dieses Beispiels können Sie sehen, dass die Reservierung von Gleichzeitigkeit folgende Auswirkungen hat:

- Ihre Funktion kann unabhängig von anderen Funktionen in Ihrem Konto skaliert werden. Alle Funktionen Ihres Kontos in derselben Region, die über keine reservierte Gleichzeitigkeit verfügen, teilen sich den Pool an nicht reservierter Gleichzeitigkeit. Ohne reservierte Gleichzeitigkeit können andere Funktionen möglicherweise Ihre gesamte verfügbare Gleichzeitigkeit verbrauchen. Dadurch wird verhindert, dass kritische Funktion bei Bedarf hochskalieren.
- Ihre Funktion kann nicht unkontrolliert aufskaliert werden. Die reservierte Nebenläufigkeit legt eine Obergrenze für die maximale Gleichzeitigkeit Ihrer Funktion fest. Dies bedeutet, dass Ihre Funktion keine für andere Funktionen reservierte Gleichzeitigkeit oder Gleichzeitigkeit aus dem nicht reservierten Pool verwenden kann. Sie können Gleichzeitigkeit reservieren, um zu verhindern, dass Ihre Funktion die gesamte verfügbare Gleichzeitigkeit in Ihrem Konto verwendet oder nachgelagerte Ressourcen überlastet.
- Möglicherweise können Sie nicht die gesamte verfügbare Gleichzeitigkeit Ihres Kontos nutzen. Das Reservieren von Gleichzeitigkeit wird auf Ihr Kontolimit für Gleichzeitigkeit angerechnet, aber

das bedeutet auch, dass andere Funktionen diesen Teil der reservierten Gleichzeitigkeit nicht verwenden können. Wenn Ihre Funktion nicht die gesamte Gleichzeitigkeit verbraucht, die Sie dafür reservieren, verschwenden Sie diese Gleichzeitigkeit effektiv. Das ist kein Problem, es sei denn, andere Funktionen in Ihrem Konto könnten von der ungenutzten Gleichzeitigkeit profitieren.

Informationen zur Verwaltung der reservierten Nebenläufigkeitseinstellungen für Ihre Funktionen finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.

Bereitgestellte Gleichzeitigkeit

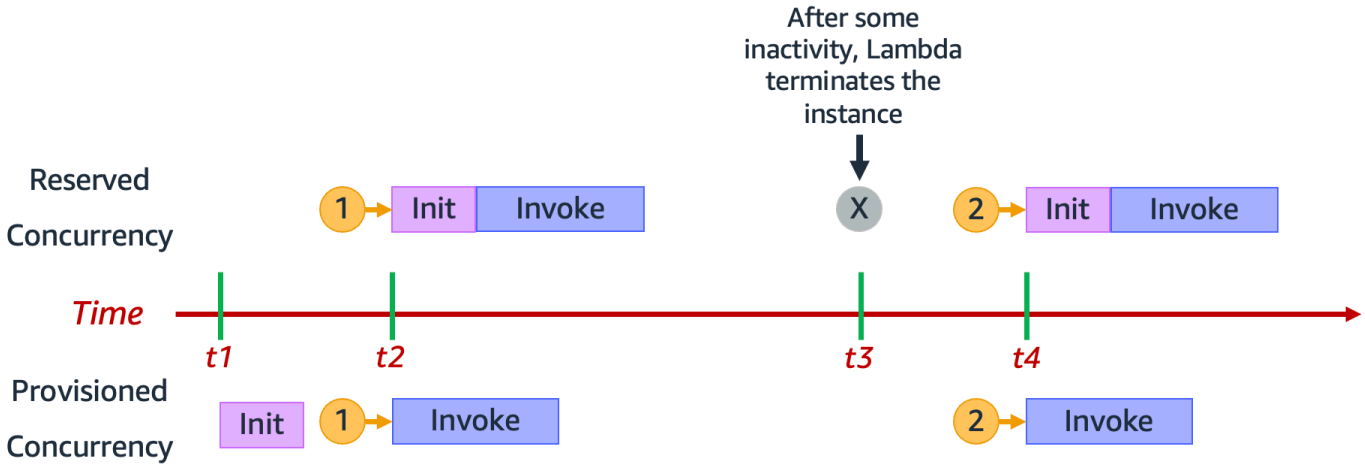
Sie verwenden die reservierte Gleichzeitigkeit, um die maximale Anzahl der für eine Lambda-Funktion reservierten Ausführungsumgebungen festzulegen. Keine dieser Umgebungen ist jedoch vorinitialisiert. Infolgedessen können Ihre Funktionsaufrufe länger dauern, da Lambda zuerst die neue Umgebung initialisieren muss, bevor diese zum Aufrufen Ihrer Funktion verwendet werden kann. Wenn Lambda eine neue Umgebung initialisieren muss, um einen Aufruf auszuführen, wird dies als Kaltstart bezeichnet. Um Kaltstarts zu vermeiden, können Sie die bereitgestellte Gleichzeitigkeit verwenden.

Die bereitgestellte Nebenläufigkeit beschreibt die Anzahl der vorinitialisierten Ausführungsumgebungen, die Sie Ihrer Funktion zuweisen möchten. Wenn Sie bereitgestellte Gleichzeitigkeit für eine Funktion festlegen, initialisiert Lambda diese Anzahl von Ausführungsumgebungen, damit sie bereit sind, sofort auf Funktionsanfragen zu reagieren.

> **Note**
>
> Die Verwendung von bereitgestellter Gleichzeitigkeit verursacht zusätzliche Gebühren für Ihr Konto. Wenn Sie mit den Laufzeiten Java 11 oder Java 17 arbeiten, können Sie Lambda auch verwenden, SnapStart um Kaltstartprobleme ohne zusätzliche Kosten zu beheben. SnapStart verwendet zwischengespeicherte Snapshots Ihrer Ausführungsumgebung, um die Startleistung erheblich zu verbessern. Sie können nicht beide SnapStart und die bereitgestellte Parallelität auf derselben Funktionsversion verwenden. Weitere Informationen zu SnapStart Funktionen, Einschränkungen und unterstützten Regionen finden Sie unter. Verbesserung der Startleistung mit Lambda SnapStart

Bei der Verwendung von bereitgestellter Gleichzeitigkeit erneuert Lambda weiterhin die Ausführungsumgebung im Hintergrund. Lambda stellt jedoch zu jedem Zeitpunkt sicher, dass die Anzahl der vorinitialisierten Umgebungen dem Wert der von Ihrer Funktion bereitgestellten

Gleichzeitigkeitseinstellung entspricht. Dieses Verhalten unterscheidet sich von reservierter Gleichzeitigkeit, bei der Lambda eine Umgebung nach einem Zeitraum der Inaktivität vollständig beenden kann. Das folgende Diagramm veranschaulicht dies, indem der Lebenszyklus einer einzelnen Ausführungsumgebung beim Konfigurieren Ihrer Funktion mit reservierter Gleichzeitigkeit mit bereitgestellter Gleichzeitigkeit verglichen wird.

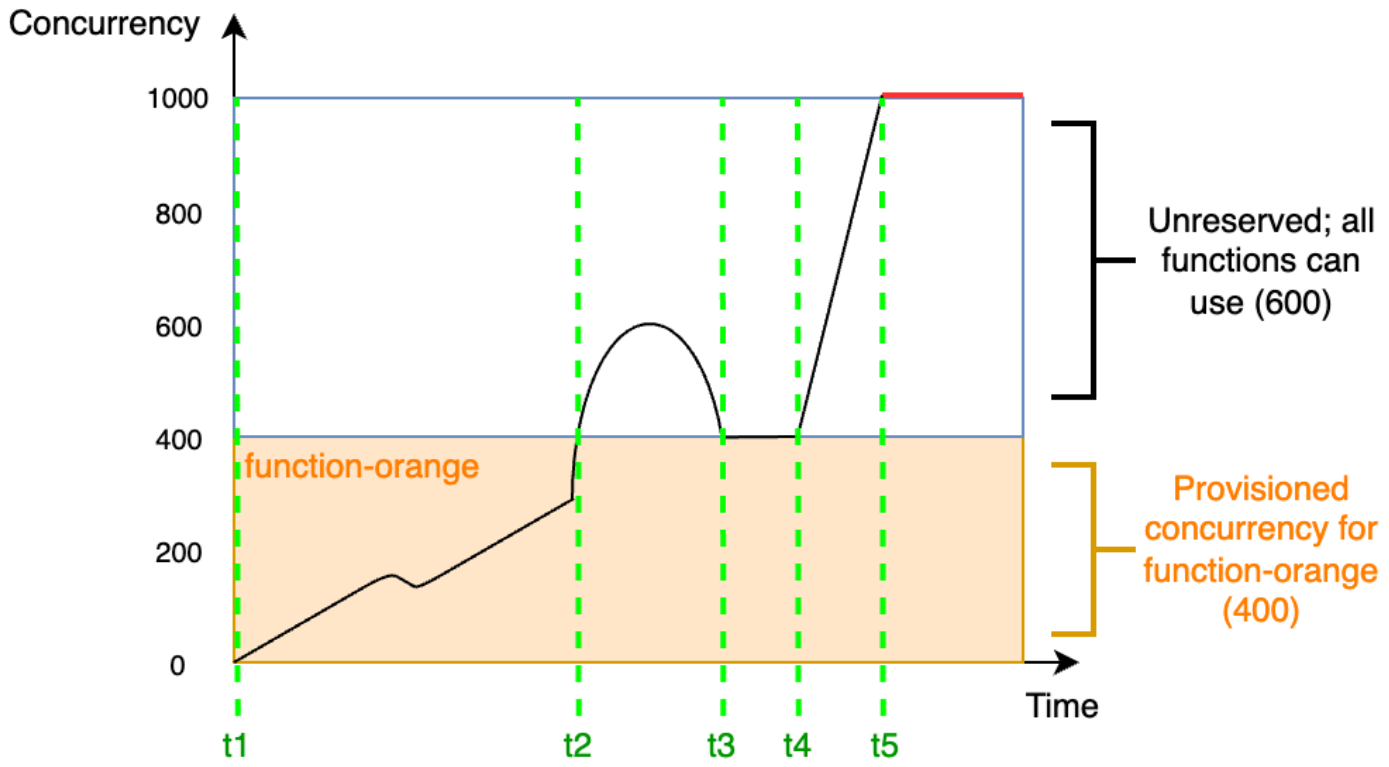


Das Diagramm enthält vier wichtige Punkte:

Zeit	Reservierte Gleichzeitigkeit	Bereitgestellte Gleichzeitigkeit
t1	Es passiert nichts.	Lambda initialisiert eine Instance der Ausführun gsumgebung vorab.
t2	Anfrage 1 wird empfangen . Lambda muss eine neue Instance der Ausführun gsumgebung initialisieren.	Anfrage 1 wird empfangen . Lambda verwendet die vorinitialisierte Umgebungs-Instance.
t3	Nach einer gewissen Inaktivit ät beendet Lambda die aktive Umgebungs-Instance.	Es passiert nichts.
t4	Anfrage 2 wird empfangen . Lambda muss eine neue	Anfrage 2 wird empfangen . Lambda verwendet die

Zeit	Reservierte Gleichzeitigkeit	Bereitgestellte Gleichzeitigkeit
	Instance der Ausführungsumgebung initialisieren.	vorinitialisierte Umgebungs-Instance.

Betrachten Sie das folgende Diagramm, um die bereitgestellte Gleichzeitigkeit besser zu verstehen:



In diesem Diagramm haben Sie eine Kontogleichzeitigkeitslimit von 1 000. Sie entscheiden sich, 400 Einheiten der bereitgestellten Gleichzeitigkeit an `function-orange` zu vergeben. Alle Funktionen in Ihrem Konto, einschließlich `function-orange`, können die verbleibenden 600 Einheiten der nicht reservierten Gleichzeitigkeit nutzen.

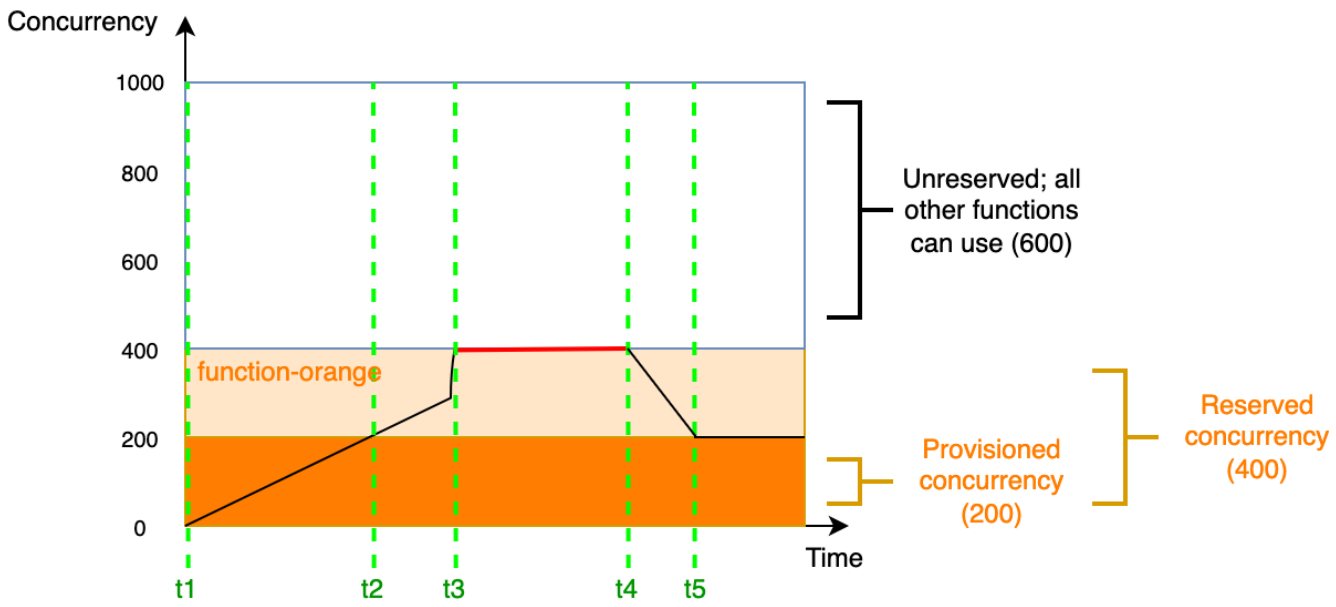
Das Diagramm enthält fünf wichtige Punkte:

- Bei `t1` beginnt `function-orange` mit dem Empfang von Anfragen. Da Lambda 400 Instances der Ausführungsumgebung vorinitialisiert hat, ist `function-orange` für den sofortigen Aufruf bereit.
- Bei `t2` erreicht `function-orange` 400 gleichzeitige Anfragen. Infolgedessen geht `function-orange` die bereitgestellte Gleichzeitigkeit aus. Da jedoch immer noch keine nicht reservierte

Gleichzeitigkeit verfügbar ist, kann Lambda dies verwenden, um zusätzliche Anfragen an `function-orange` zu verarbeiten (es gibt keine Drosselung). Lambda muss neue Instances erstellen, um diese Anfragen zu bearbeiten und bei Ihrer Funktion kann es zu Kaltstartlatenzen kommen.

- Bei `t3` kehrt `function-orange` nach einem kurzen Anstieg des Datenverkehrs zu 400 gleichzeitigen Anfragen zurück. Lambda ist wieder in der Lage, alle Anfragen ohne Kaltstartlatenzen zu bearbeiten.
- Bei `t4` kommt es bei Funktionen in Ihrem Konto zu einem starken Anstieg des Datenverkehrs. Dieser Anstieg kann von `function-orange` oder einer anderen Funktion in Ihrem Konto stammen. Lambda verwendet nicht reservierte Gleichzeitigkeit, um diese Anfragen zu bearbeiten.
- Bei `t5` erreichen die Funktionen in Ihrem Konto das maximale Gleichzeitigkeitslimit von 1 000 und es kommt zu Drosselungen.

Im vorherigen Beispiel wurde nur die bereitgestellte Nebenläufigkeit berücksichtigt. In der Praxis können Sie für eine Funktion sowohl die bereitgestellte als auch die reservierte Gleichzeitigkeit festlegen. Sie können dies beispielsweise tun, wenn Sie eine Funktion haben, die wochentags eine konstante Anzahl von Aufrufen verarbeitet, aber an den Wochenenden regelmäßig Datenverkehrsspitzen aufweist. In diesem Fall könnten Sie die bereitgestellte Gleichzeitigkeit verwenden, um eine Basismenge an Umgebungen festzulegen, die Anfragen an Wochentagen verarbeiten, und die reservierte Gleichzeitigkeit verwenden, um die Spitzenlasten am Wochenende zu verarbeiten. Betrachten Sie das folgende Diagramm:



Nehmen wir in diesem Diagramm an, dass Sie 200 Einheiten bereitgestellter Gleichzeitigkeit und 400 Einheiten reservierter Gleichzeitigkeit für `function-orange` konfigurieren. Da Sie die reservierte Gleichzeitigkeit konfiguriert haben, kann `function-orange` keine der 600 Einheiten der nicht reservierten Gleichzeitigkeit verwenden.

Dieses Diagramm enthält fünf wichtige Punkte:

- Bei `t1` beginnt `function-orange` mit dem Empfang von Anfragen. Da Lambda 200 Instances der Ausführungsumgebung vorinitialisiert hat, ist `function-orange` für den sofortigen Aufruf bereit.
- Bei `t2` verbraucht `function-orange` die gesamte bereitgestellte Gleichzeitigkeit. `function-orange` kann weiterhin Anfragen über reservierte Gleichzeitigkeit bearbeiten, allerdings kann es bei diesen Anfragen zu Kaltstartlatenzen kommen.
- Bei `t3` erreicht `function-orange` 400 gleichzeitige Anfragen. Dadurch verbraucht `function-orange` die gesamte reservierte Gleichzeitigkeit. Da `function-orange` keine nicht reservierte Gleichzeitigkeit nutzen kann, werden die Anfragen gedrosselt.
- Bei `t4` beginnt `function-orange` weniger Anfragen zu erhalten und wird nicht mehr gedrosselt.
- Bei `t5` sinkt `function-orange` auf 200 gleichzeitige Anfragen, sodass alle Anfragen wieder bereitgestellte Nebenläufigkeit verwenden können (d. h. keine Kaltstartlatenzen).

Sowohl die reservierte Gleichzeitigkeit als auch die bereitgestellte Gleichzeitigkeit werden auf das Gleichzeitigkeitslimit Ihres Kontos und die regionalen Kontingente angerechnet. Mit anderen Worten, die Zuweisung von reservierter und bereitgestellter Gleichzeitigkeit kann sich auf den Gleichzeitigkeit -Pool auswirken, der anderen Funktionen zur Verfügung steht. Für die Konfiguration der bereitgestellten Parallelität fallen Gebühren für Sie an. AWS-Konto

> **Note**
>
> Wenn die Menge der bereitgestellten Nebenläufigkeit für die Versionen und Aliase einer Funktion zur reservierten Nebenläufigkeit der Funktion hinzukommt, werden alle Aufrufe mit bereitgestellter Nebenläufigkeit ausgeführt. Diese Konfiguration hat auch zur Folge, dass die nicht veröffentlichte Version der Funktion (`$LATEST`) gedrosselt wird, was die Ausführung verhindert. Sie können nicht mehr bereitgestellte Gleichzeitigkeit als reservierte Gleichzeitigkeit für eine Funktion zuweisen.

Informationen zur Verwaltung der Einstellungen für reservierte Nebenläufigkeit für Ihre Funktionen finden Sie unter Konfiguration der bereitgestellten Parallelität für eine Funktion. Informationen zum Automatisieren der bereitgestellten Gleichzeitigkeitsskalierung basierend auf einem Zeitplan oder der Anwendungsnutzung finden Sie unter Verwenden von Application Auto Scaling zur Automatisierung des bereitgestellten Parallelitätsmanagements.

So weist Lambda bereitgestellte Gleichzeitigkeit zu

Bereitgestellte Gleichzeitigkeit wird nicht sofort nach der Konfiguration online geschaltet. Lambda beginnt die Zuweisung bereitgestellter Gleichzeitigkeit nach ein oder zwei Minuten Vorbereitung. Für jede Funktion kann Lambda jede Minute bis zu 6.000 Ausführungsumgebungen bereitstellen, unabhängig davon AWS-Region. Dies entspricht exakt der Skalierungsrate für Nebenläufigkeit für Funktionen.

Wenn Sie eine Anforderung zur Zuweisung bereitgestellter Gleichzeitigkeit einreichen, können Sie erst wieder auf diese Umgebungen zugreifen, wenn Lambda die Zuweisung vollständig abgeschlossen hat. Wenn Sie beispielsweise 5.000 bereitgestellte Parallelität anfordern, kann keine Ihrer Anfragen bereitgestellte Parallelität verwenden, bis Lambda die Zuweisung der 5.000 Ausführungsumgebungen vollständig abgeschlossen hat.

Vergleich zwischen reservierter und bereitgestellter Gleichzeitigkeit

Die folgende Tabelle fasst reservierte und bereitgestellte Nebenläufigkeit zusammen und vergleicht sie.

Thema	Reservierte Gleichzeitigkeit	Bereitgestellte Gleichzeitigkeit
Definition	Maximale Anzahl von Instances in der Ausführun gsumgebung für Ihre Funktion.	Festgelegte Anzahl von vorbereiteten Instances in der Ausführungsumgebung für Ihre Funktion.
Bereitstellungsverhalten	Lambda stellt neue Instances auf On-Demand-Basis bereit.	Lambda stellt Instances vorab bereit (d. h. bevor Ihre Funktion mit dem Empfang von Anfragen beginnt).
Kaltstartverhalten	Kaltstartlatenz möglich, da Lambda bei Bedarf neue Instances erstellen muss.	Eine Kaltstartlatenz ist nicht möglich, da Lambda keine Instances On-Demand erstellen muss.
Drosselungsverhalten	Die Funktion wurde gedrossel t, als das reservierte Gleichzei tigkeitslimit erreicht wurde.	Wenn die reservierte Gleichzei tigkeit nicht festgelegt ist: Die Funktion verwendet die nicht reservierte Gleichzei tigkeit, wenn das bereitges tellte Gleichzeitigkeitslimit erreicht ist. Wenn reservierte Gleichzei tigkeit festgelegt ist: Funktion wird gedrosselt, wenn das Limit für reservierte Gleichzei tigkeit erreicht wird.

Thema	Reservierte Gleichzeitigkeit	Bereitgestellte Gleichzeitigkeit
Standardverhalten, falls nicht festgelegt	Die Funktion verwendet nicht reservierte Gleichzeitigkeit, die in Ihrem Konto verfügbar ist.	Lambda stellt keine Instances vorab bereit. Wenn die reservierte Gleichzeitigkeit nicht festgelegt ist, verwendet die Funktion stattdessen die nicht reservierte Gleichzei tigkeit, die in Ihrem Konto verfügbar ist. Wenn reservierte Gleichzei tigkeit festgelegt ist: die Funktion verwendet reservier te Gleichzeitigkeit.
Preisgestaltung	Keine zusätzlichen Gebühren.	Verursacht zusätzliche Gebühren.

Gleichzeitigkeitskontingente

Lambda legt Kontingente für die Gesamtmenge der Nebenläufigkeit fest, die Sie für alle Funktionen in einer Region verwenden können. Diese Kontingente bestehen auf zwei Ebenen:

- Auf Kontoebene können Ihre Funktionen standardmäßig bis zu 1 000 Einheiten an Gleichzeitigkeit verwenden. Informationen zum Erhöhen dieses Limits finden Sie unter Anfordern einer Kontingenterhöhung im Benutzerhandbuch für Service Quotas.
- Auf Funktionsebene können Sie standardmäßig bis zu 900 Nebenläufigkeitseinheiten für alle Ihre Funktionen reservieren. Unabhängig von Ihrem Gesamtlimit für die Kontonebenläufigkeit reserviert Lambda immer 100 Nebenläufigkeitseinheiten für Ihre Funktionen, die Nebenläufigkeit nicht explizit reservieren. Wenn Sie beispielsweise Ihr Limit für die Nebenläufigkeit Ihres Kontos auf 2 000 erhöht haben, können Sie auf Funktionsebene bis zu 1 900 Einheiten an Nebenläufigkeit reservieren.

Um Ihr aktuelles Kontingent für Parallelität auf Kontoebene zu überprüfen, verwenden Sie AWS Command Line Interface ()AWS CLI, um den folgenden Befehl auszuführen:

```
aws lambda get-account-settings
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
{
    "AccountLimit": {
        "TotalCodeSize": 80530636800,
        "CodeSizeUnzipped": 262144000,
        "CodeSizeZipped": 52428800,
        "ConcurrentExecutions": 1000,
        "UnreservedConcurrentExecutions": 900
    },
    "AccountUsage": {
        "TotalCodeSize": 410759889,
        "FunctionCount": 8
    }
}
```

`ConcurrentExecutions` ist Ihr Gesamtkontingent für die Nebenläufigkeit auf Kontoebene. `UnreservedConcurrentExecutions` ist die Menge an verbleibender Nebenläufigkeit, die Sie Ihren Funktionen noch zuweisen können.

Erhält Ihre Funktion mehr Anfragen, sorgt Lambda automatisch für die Skalierung der Anzahl der Ausführungsumgebungen, bis Ihr Konto das Nebenläufigkeitskontingent erreicht. Zum Schutz vor einer Überskalierung als Reaktion auf plötzliche Datenverkehrsspitzen begrenzt Lambda jedoch, wie schnell Ihre Funktionen skaliert werden können. Diese Skalierungsrate für Parallelität ist die maximale Rate, mit der Funktionen in Ihrem Konto als Reaktion auf erhöhte Anfragen skaliert werden können. (Das heißt, sie gibt an, wie schnell Lambda neue Ausführungsumgebungen erstellen kann.) Die Skalierungsrate für Parallelität unterscheidet sich vom Parallelitätslimit auf Kontoebene, das der Gesamtmenge an Parallelität entspricht, die Ihren Funktionen zur Verfügung steht.

In jeder AWS-Region Funktion beträgt Ihre Parallelitätsskalierungsrate 1.000 Instanzen der Ausführungsumgebung alle 10 Sekunden. Mit anderen Worten, alle 10 Sekunden kann Lambda jeder Ihrer Funktionen maximal 1 000 zusätzliche Instances der Ausführungsumgebung zuweisen.

Normalerweise müssen Sie sich über diese Einschränkung keine Gedanken machen. Die Skalierungsrate von Lambda ist für die meisten Anwendungsfälle ausreichend.

Wichtig ist, dass es sich bei der Skalierungsrate der Parallelität um eine Grenze auf Funktionsebene handelt. Das bedeutet, dass jede Funktion in Ihrem Konto unabhängig von anderen Funktionen skaliert werden kann.

Weitere Informationen zum Skalierungsverhalten finden Sie unter Lambda-Skalierungsverhalten.

Reservierte Parallelität für eine Funktion konfigurieren

In Lambda beschreibt die Gleichzeitigkeit die Anzahl der In-Flight-Anfragen, die Ihre Funktion gleichzeitig bearbeitet. Es gibt zwei Arten von Gleichzeitigkeitskontrollen:

- Reservierte Gleichzeitigkeit ist die maximale Anzahl der gleichzeitigen Instances, die Ihrer Funktion zugewiesen sind. Wenn für eine Funktion Gleichzeitigkeit reserviert ist, kann keine andere Funktion diese Gleichzeitigkeit nutzen. Reservierte Parallelität ist nützlich, um sicherzustellen, dass Ihre wichtigsten Funktionen immer über genügend Parallelität verfügen, um eingehende Anfragen zu bearbeiten. Für die Konfiguration reservierter Gleichzeitigkeit für eine Funktion wird keine zusätzliche Gebühr erhoben.
- Die bereitgestellte Gleichzeitigkeit beschreibt die Anzahl der vorinitialisierten Ausführungsumgebungen, die Ihrer Funktion zugewiesen sind. Diese Ausführungsumgebungen sind bereit, sofort auf eingehende Funktionsanforderungen zu reagieren. Bereitgestellte Parallelität ist nützlich, um die Latenzen beim Kaltstart von Funktionen zu reduzieren. Für die Konfiguration der bereitgestellten Parallelität fallen zusätzliche Gebühren für Sie an. AWS-Konto

In diesem Thema wird beschrieben, wie Sie reservierte Gleichzeitigkeit verwalten und konfigurieren. Eine konzeptionelle Übersicht über diese beiden Arten von Gleichzeitigkeitssteuerungen finden Sie unter Reservierte Gleichzeitigkeit und bereitgestellte Gleichzeitigkeit. Weitere Informationen zum Konfigurieren der bereitgestellten Gleichzeitigkeit finden Sie unter the section called “Konfigurieren von Provisioned Concurrency”.

> **Note**
>
> Lambda-Funktionen, die mit einer Amazon-MQ-Ereignisquellenzuordnung verknüpft sind, haben standardmäßig die maximale Gleichzeitigkeit. Für Apache Active MQ ist die maximale Anzahl der gleichzeitigen Instances 5. Für Rabbit MQ ist die maximale Anzahl der gleichzeitigen Instances 1. Wenn Sie für Ihre Funktion eine reservierte oder bereitgestellte Parallelität festlegen, werden diese Grenzwerte nicht geändert. Um eine Erhöhung der standardmäßigen maximalen Parallelität bei der Verwendung von Amazon MQ zu beantragen, wenden Sie sich an. AWS Support

Sections

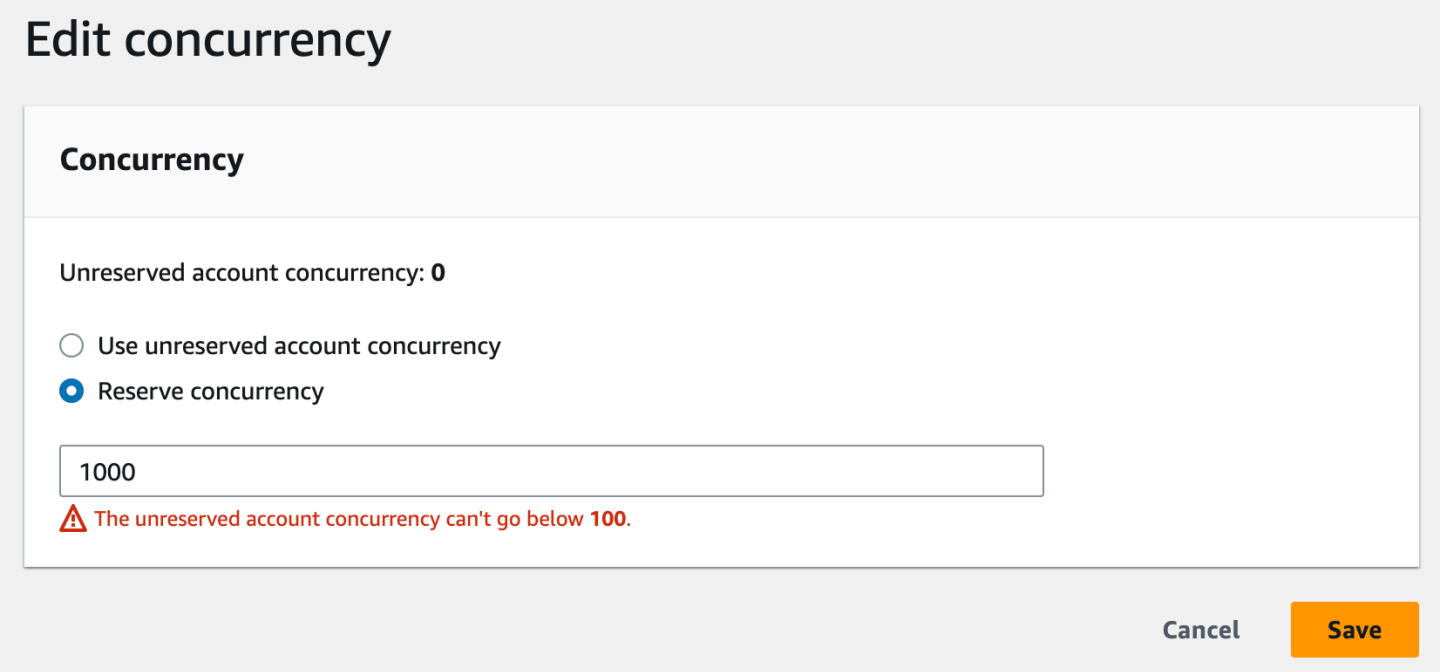
Konfigurieren reservierter Gleichzeitigkeit

Sie können die Einstellungen der reservierten Gleichzeitigkeit für eine Funktion in der Lambda-Konsole oder mit der Lambda-API konfigurieren.

Reservieren von Gleichzeitigkeit für eine Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, für sie Sie Gleichzeitigkeit reservieren möchten.
3. Wählen Sie Konfiguration und anschließend Gleichzeitigkeit aus.
4. Wählen Sie unter Concurrency (Parallelität) die Option Edit (Bearbeiten).
5. Wählen Sie Reserve concurrency (Parallelität reservieren). Geben Sie die Menge an Gleichzeitigkeit an, die für die Funktion reserviert werden soll.
6. Wählen Sie Save aus.

Sie können bis zum Wert von Nicht reservierte Kontonebenläufigkeit minus 100 reservieren. Die verbleibenden 100 Gleichzeitigkeitseinheiten sind für Funktionen bestimmt, die keine reservierte Gleichzeitigkeit verwenden. Wenn für Ihr Konto beispielsweise eine Gleichzeitigkeitsbeschränkung von 1 000 gilt, können Sie nicht alle 1 000 Gleichzeitigkeitseinheiten für eine einzelne Funktion reservieren.



Das Reservieren von Gleichzeitigkeit für eine Funktion hat Auswirkungen auf den Pool, der für andere Funktionen verfügbar ist. Wenn Sie beispielsweise 100 Gleichzeitigkeitseinheiten für `function-a` reservieren, müssen sich andere Funktionen in Ihrem Konto die verbleibenden 900 Gleichzeitigkeitseinheiten teilen, auch wenn `function-a` nicht alle 100 reservierten Gleichzeitigkeitseinheiten verwendet.

Um eine Funktion absichtlich zu drosseln, setzen Sie die reservierte Gleichzeitigkeit dafür auf 0. Dadurch kann die Funktion keine Ereignisse mehr verarbeiten, bis Sie die Beschränkung aufheben.

Verwenden Sie für die Konfiguration von reservierter Gleichzeitigkeit mithilfe der Lambda-API die folgenden API-Vorgänge:

- PutFunctionParallelität
- GetFunctionParallelität
- DeleteFunctionParallelität

Um beispielsweise reservierte Parallelität mit der AWS Command Line Interface (CLI) zu konfigurieren, verwenden Sie den `put-function-concurrency` Befehl. Der folgende Befehl reserviert 100 Gleichzeitigkeitseinheiten für eine Funktion namens `my-function`:

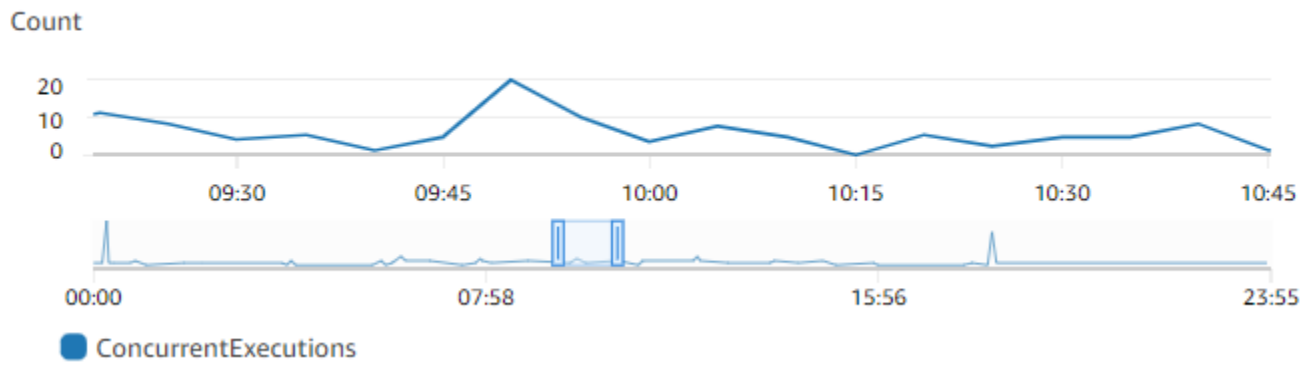
```
aws lambda put-function-concurrency --function-name my-function \
    --reserved-concurrent-executions 100
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
{
    "ReservedConcurrentExecutions": 100
}
```

Genaue Schätzung der erforderlichen reservierten Parallelität für eine Funktion

Wenn Ihre Funktion derzeit Traffic verarbeitet, können Sie die zugehörigen Parallelitätskennzahlen einfach anhand von Metriken einsehen. CloudWatch Insbesondere zeigt Ihnen die `ConcurrentExecutions`-Metrik die Anzahl der gleichzeitigen Aufrufe für jede Funktion in Ihrem Konto.



Aus dem vorstehenden Diagramm geht hervor, dass diese Funktion jederzeit im Durchschnitt 5 bis 10 gleichzeitige Anforderungen verarbeitet und an einem typischen Tag Spitzenwerte von 20 Anforderungen erreicht. Angenommen, Ihr Konto enthält viele andere Funktionen. Wenn diese Funktion für Ihre Anwendung von entscheidender Bedeutung ist und Sie keine Anforderungen abbrechen möchten, verwenden Sie mindestens 20 als Einstellung für die reservierte Gleichzeitigkeit.

Denken Sie alternativ daran, dass Sie die Gleichzeitigkeit auch mit der folgenden Formel berechnen können:

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

Wenn Sie die durchschnittlichen Anforderungen pro Sekunde mit der durchschnittlichen Anforderungsdauer in Sekunden multiplizieren, erhalten Sie eine grobe Schätzung, wie viel Gleichzeitigkeit Sie reservieren müssen. Sie können die durchschnittlichen Anfragen pro Sekunde anhand der `Invocation`-Metrik und die durchschnittliche Anfragedauer in Sekunden anhand der `Duration`-Metrik schätzen. Weitere Details finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Konfiguration der bereitgestellten Parallelität für eine Funktion

In Lambda beschreibt die Gleichzeitigkeit die Anzahl der In-Flight-Anfragen, die Ihre Funktion gleichzeitig bearbeitet. Es gibt zwei Arten von Gleichzeitigkeitskontrollen:

- Reservierte Gleichzeitigkeit ist die maximale Anzahl der gleichzeitigen Instances, die Ihrer Funktion zugewiesen sind. Wenn für eine Funktion Gleichzeitigkeit reserviert ist, kann keine andere Funktion diese Gleichzeitigkeit nutzen. Reservierte Parallelität ist nützlich, um sicherzustellen, dass Ihre wichtigsten Funktionen immer über genügend Parallelität verfügen, um eingehende Anfragen zu bearbeiten. Für die Konfiguration reservierter Gleichzeitigkeit für eine Funktion wird keine zusätzliche Gebühr erhoben.
- Die bereitgestellte Gleichzeitigkeit beschreibt die Anzahl der vorinitialisierten Ausführungsumgebungen, die Ihrer Funktion zugewiesen sind. Diese Ausführungsumgebungen sind bereit, sofort auf eingehende Funktionsanforderungen zu reagieren. Bereitgestellte Parallelität ist nützlich, um die Latenzen beim Kaltstart von Funktionen zu reduzieren. Für die Konfiguration der bereitgestellten Parallelität fallen zusätzliche Gebühren für Sie an. AWS-Konto

In diesem Thema wird beschrieben, wie Sie bereitgestellte Gleichzeitigkeit verwalten und konfigurieren. Eine konzeptionelle Übersicht über diese beiden Arten von Gleichzeitigkeitssteuerungen finden Sie unter Reservierte Gleichzeitigkeit und bereitgestellte Gleichzeitigkeit. Weitere Informationen zur Konfiguration der reservierten Gleichzeitigkeit finden Sie unter the section called “Konfigurieren reservierter Gleichzeitigkeit”.

> **Note**
>
> Lambda-Funktionen, die mit einer Amazon-MQ-Ereignisquellenzuordnung verknüpft sind, haben standardmäßig die maximale Gleichzeitigkeit. Für Apache Active MQ ist die maximale Anzahl der gleichzeitigen Instances 5. Für Rabbit MQ ist die maximale Anzahl der gleichzeitigen Instances 1. Wenn Sie für Ihre Funktion eine reservierte oder bereitgestellte Parallelität festlegen, werden diese Grenzwerte nicht geändert. Um eine Erhöhung der standardmäßigen maximalen Parallelität bei der Verwendung von Amazon MQ zu beantragen, wenden Sie sich an. AWS Support

Sections

- Optimierung des Funktionscodes bei Verwendung der bereitgestellten Parallelität
- Verwendung von Umgebungsvariablen zur Anzeige und Steuerung des Parallelitätsverhaltens bei der Bereitstellung
- Grundlegendes zum Protokollierungs- und Abrechnungsverhalten bei bereitgestellter Parallelität
- Verwenden von Application Auto Scaling zur Automatisierung des bereitgestellten Parallelitätsmanagements

Konfigurieren von Provisioned Concurrency

Sie können die Einstellungen der bereitgestellten Gleichzeitigkeit für eine Funktion mit der Lambda-Konsole oder mit der Lambda-API konfigurieren.

So weisen Sie einer Funktion bereitgestellte Gleichzeitigkeit zu (Konsole)

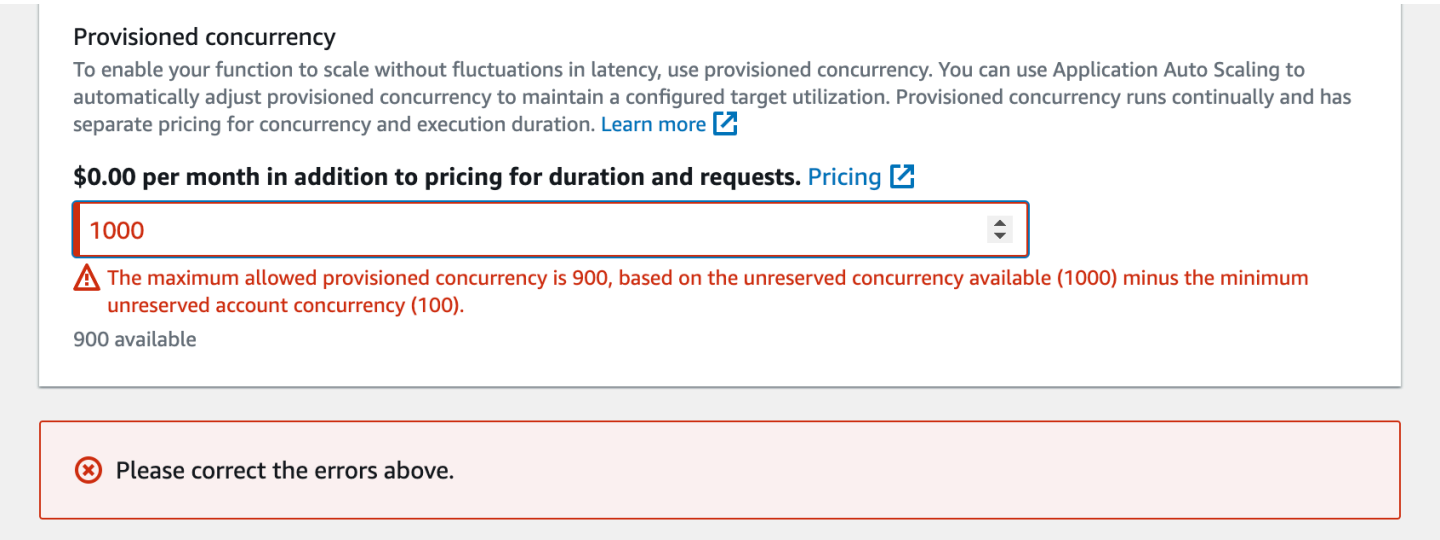
1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, der Sie bereitgestellte Gleichzeitigkeit zuweisen möchten.
3. Wählen Sie Konfiguration und anschließend Gleichzeitigkeit aus.
4. Wählen Sie unter Provisioned concurrency configurations (Bereitgestellte Gleichzeitigkeitskonfigurationen) die Option Add (Hinzufügen) aus.
5. Wählen Sie den Qualifizierungstyp und den Alias oder die Version aus.

   > **Note**
   >
   > Sie können die bereitgestellte Gleichzeitigkeit nicht mit der $LATEST-Version einer Funktion verwenden.
   > Wenn Ihre Funktion eine Ereignisquelle hat, müssen Sie sicherstellen, dass die Ereignisquelle auf den richtigen Funktionsalias bzw. die richtige Funktionsversion verweist. Anderenfalls verwendet Ihre Funktion keine bereitgestellten Gleichzeitigkeitsumgebungen.

6. Geben Sie unter Bereitgestellte Gleichzeitigkeit eine Zahl ein. Lambda bietet eine Schätzung der monatlichen Kosten.
7. Wählen Sie Speichern.

Sie können in Ihrem Konto Gleichzeitigkeit bis zur nicht reservierten Konto-Gleichzeitigkeit minus 100 konfigurieren. Die verbleibenden 100 Gleichzeitigkeitseinheiten sind für Funktionen

bestimmt, die keine reservierte Gleichzeitigkeit verwenden. Wenn Ihr Konto beispielsweise einen Gleichzeitigkeitsgrenzwert von 1 000 aufweist und Sie keiner anderen Funktion reservierte oder bereitgestellte Gleichzeitigkeit zugewiesen haben, können Sie maximal 900 bereitgestellte Gleichzeitigkeitseinheiten für eine einzelne Funktion konfigurieren.



Die Konfiguration der bereitgestellten Gleichzeitigkeit für eine Funktion wirkt sich auf den Pool für die Gleichzeitigkeit aus, der für andere Funktionen verfügbar ist. Wenn Sie beispielsweise 100 bereitgestellte Gleichzeitigkeitseinheiten für `function-a` konfigurieren, müssen sich andere Funktionen in Ihrem Konto die verbleibenden 900 Gleichzeitigkeitseinheiten teilen. Das gilt auch, wenn `function-a` nicht alle 100 Einheiten verwendet.

Sie können für eine Funktion sowohl reservierte als auch bereitgestellte Gleichzeitigkeit festlegen. In solchen Fällen darf die bereitgestellte Gleichzeitigkeit die reservierte Gleichzeitigkeit nicht überschreiten.

Dieser Grenzwert gilt auch für Funktionsversionen. Die maximale Menge an bereitgestellter Gleichzeitigkeit, die Sie einer bestimmten Funktionsversion zuweisen können, entspricht der reservierten Gleichzeitigkeit der Funktion abzüglich der in anderen Funktionsversionen bereitgestellten Gleichzeitigkeit.

Verwenden Sie für die Konfiguration der bereitgestellten Gleichzeitigkeit mithilfe der Lambda-API die folgenden API-Operationen:

- PutProvisionedConcurrencyConfig
- GetProvisionedConcurrencyConfig
- ListProvisionedConcurrencyConfigs

- DeleteProvisionedConcurrencyConfig

Verwenden Sie beispielsweise den Befehl, um die bereitgestellte Parallelität mit der AWS Command Line Interface (CLI) zu konfigurieren. `put-provisioned-concurrency-config` Der folgende Befehl weist 100 Einheiten bereitgestellter Gleichzeitigkeit für den Alias `BLUE` einer Funktion namens `my-function` zu:

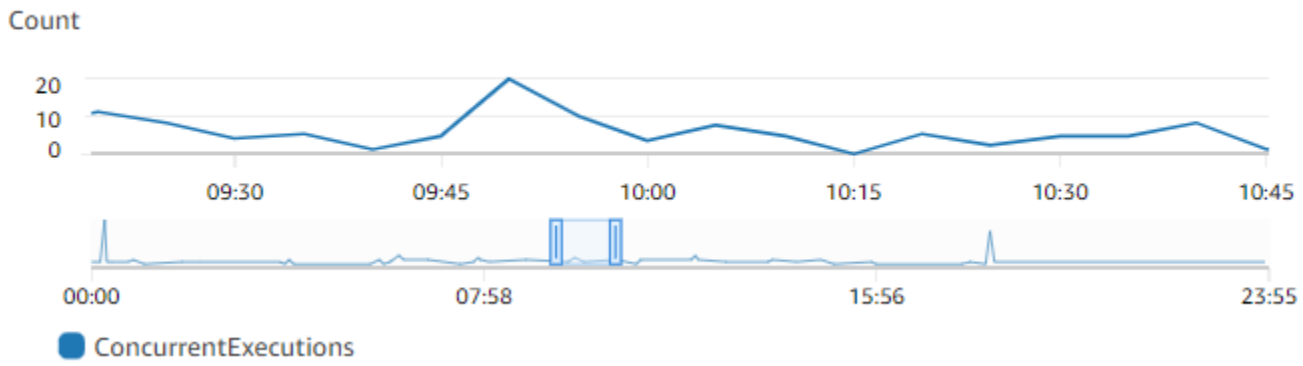
```
aws lambda put-provisioned-concurrency-config --function-name my-function \
  --qualifier BLUE \
  --provisioned-concurrent-executions 100
```

Die Ausgabe sollte ungefähr wie folgt aussehen:

```
{
  "Requested ProvisionedConcurrentExecutions": 100,
  "Allocated ProvisionedConcurrentExecutions": 0,
  "Status": "IN_PROGRESS",
  "LastModified": "2023-01-21T11:30:00+0000"
}
```

Genaue Schätzung der erforderlichen bereitgestellten Parallelität für eine Funktion

Sie können die Parallelitätsmetriken jeder aktiven Funktion mithilfe von Metriken anzeigen. CloudWatch Insbesondere zeigt Ihnen die `ConcurrentExecutions`-Metrik die Anzahl der gleichzeitigen Aufrufe für Funktionen in Ihrem Konto.



Aus dem vorstehenden Diagramm geht hervor, dass diese Funktion jederzeit im Durchschnitt 5 bis 10 gleichzeitige Anforderungen verarbeitet und Spitzenwerte von 20 Anforderungen erreicht. Angenommen, Ihr Konto enthält viele andere Funktionen. Wenn diese Funktion für Ihre Anwendung

von entscheidender Bedeutung ist und Sie bei jedem Aufruf eine Reaktion mit geringer Latenz wünschen, legen Sie für die bereitgestellte Gleichzeitigkeit eine Zahl fest, die größer oder gleich 20 ist.

Denken Sie daran, dass Sie die Gleichzeitigkeit auch mit der folgenden Formel berechnen können:

```
Concurrency = (average requests per second) * (average request duration in seconds)
```

Um abzuschätzen, wie viel Gleichzeitigkeit Sie benötigen, multiplizieren Sie die durchschnittlichen Anfragen pro Sekunde mit der durchschnittlichen Anfragedauer in Sekunden. Sie können die durchschnittlichen Anfragen pro Sekunde anhand der `Invocation`-Metrik und die durchschnittliche Anfragedauer in Sekunden anhand der `Duration`-Metrik schätzen.

Beim Konfigurieren der bereitgestellten Gleichzeitigkeit schlägt Lambda vor, einen Puffer von 10 % zusätzlich zu der Menge an Gleichzeitigkeit einzuplanen, die Ihre Funktion normalerweise benötigt. Wenn die Funktion normalerweise bei 200 gleichzeitigen Anforderungen Spitzenwerte erreicht, sollten Sie die bereitgestellte Gleichzeitigkeit auf 220 festlegen (200 gleichzeitige Anforderungen + 10 % = 220 bereitgestellte Gleichzeitigkeit).

Optimierung des Funktionscodes bei Verwendung der bereitgestellten Parallelität

Wenn Sie bereitgestellte Parallelität verwenden, sollten Sie erwägen, Ihren Funktionscode umzustrukturieren, um ihn für eine geringe Latenz zu optimieren. Für Funktionen, die bereitgestellte Parallelität verwenden, führt Lambda während der Zuweisungszeit jeden Initialisierungscode aus, z. B. das Laden von Bibliotheken und das Instanziieren von Clients. Daher bietet es sich an, möglichst viele Initialisierungen außerhalb des Hauptfunktionshandlers zu verschieben, um bei tatsächlichen Funktionsaufrufen Latenzprobleme zu vermeiden. Im Gegensatz dazu bedeutet das Initialisieren von Bibliotheken oder das Instanziieren von Clients innerhalb Ihres Haupthandlercodes, dass Ihre Funktion dies bei jedem Aufruf ausführen muss (dies geschieht unabhängig davon, ob Sie die bereitgestellte Parallelität verwenden).

Bei On-Demand-Aufrufen muss Lambda den Initialisierungscode möglicherweise jedes Mal neu ausführen, wenn die Funktion einen Kaltstart durchführt. In diesem Fall können Sie die Initialisierung einzelner Fähigkeiten verschieben, bis Ihre Funktion sie benötigt. Sehen Sie sich zum Beispiel den folgenden Steuerungsablauf für einen Lambda-Handler an:

```
def handler(event, context):
    ...
```

```
    if ( some_condition ):
        // Initialize CLIENT_A to perform a task
    else:
        // Do nothing
```

Im vorherigen Beispiel entschied sich der Entwickler dagegen, `CLIENT_A` außerhalb des Haupthandlers zu initialisieren, und initialisierte ihn stattdessen innerhalb der `if`-Anweisung. Auf diese Weise führt Lambda diesen Code nur aus, wenn die Bedingung `some_condition` erfüllt wird. Wenn `CLIENT_A` außerhalb des Haupthandlers initialisiert wird, führt Lambda diesen Code bei jedem Kaltstart aus. Das kann die Gesamtlatenz erhöhen.

Verwendung von Umgebungsvariablen zur Anzeige und Steuerung des Parallelitätsverhaltens bei der Bereitstellung

Es ist möglich, dass Ihre Funktion die gesamte bereitgestellte Gleichzeitigkeit verbraucht. Lambda verwendet On-Demand-Instances, um zusätzlichen Datenverkehr zu verarbeiten. Um festzustellen, welche Art von Initialisierung Lambda für eine bestimmte Umgebung verwendet hat, überprüfen Sie den Wert der Umgebungsvariable `AWS_LAMBDA_INITIALIZATION_TYPE`. Diese Variable hat zwei mögliche Werte: `provisioned-concurrency` oder `on-demand`. Der Wert von `AWS_LAMBDA_INITIALIZATION_TYPE` ist unveränderlich und bleibt während der gesamten Lebensdauer der Umgebung konstant. Informationen zum Überprüfen des Werts einer Umgebungsvariablen in Ihrem Funktionscode finden Sie unter. ???

Bei Verwendung der .NET 6- oder .NET 7-Laufzeit können Sie die Umgebungsvariable `AWS_LAMBDA_DOTNET_PREJIT` konfigurieren, um die Latenz für Funktionen zu verbessern, auch wenn diese keine bereitgestellte Gleichzeitigkeit verwenden. Die .NET-Laufzeitumgebung führt für jede Bibliothek, die der Code zum ersten Mal aufruft, eine verzögerte Kompilierung und Initialisierung durch. Daher kann der erste Aufruf einer Lambda-Funktion länger dauern als nachfolgende Aufrufe. Um dies zu verhindern, können Sie einen von drei Werten für `AWS_LAMBDA_DOTNET_PREJIT` wählen:

- `ProvisionedConcurrency`: Lambda führt die ahead-of-time JIT-Kompilierung für alle Umgebungen mithilfe der bereitgestellten Parallelität durch. Dies ist der Standardwert.
- `Always`: Lambda führt die ahead-of-time JIT-Kompilierung für jede Umgebung durch, auch wenn die Funktion keine bereitgestellte Parallelität verwendet.
- `Never`: Lambda deaktiviert die ahead-of-time JIT-Kompilierung für alle Umgebungen.

Grundlegendes zum Protokollierungs- und Abrechnungsverhalten bei bereitgestellter Parallelität

Für bereitgestellte Gleichzeitigkeitsumgebungen wird der Initialisierungscode Ihrer Funktion während der Zuordnung und alle paar Stunden ausgeführt, da Lambda aktive Instances Ihrer Umgebung recycelt. Sie können die Initialisierungszeit in Protokollen und Ablaufverfolgungsdaten anzeigen, nachdem eine Umgebungs-Instance eine Anforderung verarbeitet hat. Beachten Sie jedoch, dass Lambda die Initialisierung auch dann abrechnet, wenn die Umgebungs-Instance niemals eine Anforderung verarbeitet. Die bereitgestellte Gleichzeitigkeit wird laufend ausgeführt und getrennt von den Initialisierungs- und Aufrufkosten in Rechnung gestellt. Weitere Einzelheiten finden Sie unter AWS Lambda -Preise.

Wenn Sie eine Lambda-Funktion mit bereitgestellter Parallelität konfigurieren, initialisiert Lambda außerdem diese Ausführungsumgebung vor, sodass sie vor Funktionsaufrufanforderungen verfügbar ist. Ihre Funktion veröffentlicht Aufrufprotokolle jedoch nur dann, wenn die Funktion tatsächlich aufgerufen wird. CloudWatch Daher erscheint das Feld Init Duration in der `REPORT` Protokollzeile des ersten Funktionsaufrufs, obwohl die Initialisierung im Voraus erfolgte. Dies bedeutet nicht, dass die Funktion einen Kaltstart erlitten hat.

Verwenden von Application Auto Scaling zur Automatisierung des bereitgestellten Parallelitätsmanagements

Application Auto Scaling ermöglicht es Ihnen, die bereitgestellte Gleichzeitigkeit nach einem Zeitplan oder basierend auf der Auslastung zu verwalten. Wenn Sie vorhersehbare Auslastungsmuster für Ihre Funktion beobachten, verwenden Sie die geplante Skalierung. Wenn Sie möchten, dass Ihre Funktion einen bestimmten Auslastungsprozentsatz beibehält, verwenden Sie eine Richtlinie für die Zielverfolgungsskalierung.

Geplante Skalierung

Application Auto Scaling ermöglicht es Ihnen, Ihren eigenen Skalierungsplan entsprechend vorhersehbarer Laständerungen festzulegen. Weitere Informationen und Beispiele finden Sie unter Geplante Skalierung für Application Auto Scaling im Application Auto Scaling Scaling-Benutzerhandbuch und Scheduling AWS Lambda Provisioned Concurrency für wiederkehrende Spitzennutzung im AWS Compute-Blog.

Zielverfolgung

Mit der Zielverfolgung erstellt und verwaltet Application Auto Scaling eine Reihe von CloudWatch Alarmen, die darauf basieren, wie Sie Ihre Skalierungsrichtlinie definieren. Wenn diese Alarme

aktiviert werden, passt Application Auto Scaling mithilfe der bereitgestellten Gleichzeitigkeit automatisch die Anzahl der zugewiesenen Umgebungen an. Verwenden Sie die Zielverfolgung für Anwendungen, die keine vorhersehbaren Auslastungsmuster aufweisen.

Verwenden Sie die API-Operationen `RegisterScalableTarget` und `PutScalingPolicy` Application Auto Scaling, um die bereitgestellte Gleichzeitigkeit mithilfe der Zielverfolgung zu skalieren. Wenn Sie beispielsweise die AWS Command Line Interface (CLI) verwenden, gehen Sie wie folgt vor:

1. Registrieren Sie den Alias einer Funktion als Skalierungsziel. Im folgenden Beispiel wird der BLUE-Alias einer Funktion mit dem Namen `my-function` registriert:

```
aws application-autoscaling register-scalable-target --service-namespace lambda \
    --resource-id function:my-function:BLUE --min-capacity 1 --max-capacity 100 \
    --scalable-dimension lambda:function:ProvisionedConcurrency
```

2. Wenden Sie eine Skalierungsrichtlinie auf das Ziel an. Im folgenden Beispiel wird Application Auto Scaling so konfiguriert, dass die bereitgestellte Parallelitätskonfiguration für einen Alias so angepasst wird, dass die Auslastung nahezu 70 Prozent beträgt. Sie können jedoch jeden Wert zwischen 10 und 90% anwenden.

```
aws application-autoscaling put-scaling-policy \
    --service-namespace lambda \
    --scalable-dimension lambda:function:ProvisionedConcurrency \
    --resource-id function:my-function:BLUE \
    --policy-name my-policy \
    --policy-type TargetTrackingScaling \
    --target-tracking-scaling-policy-configuration '{ "TargetValue":
 0.7, "PredefinedMetricSpecification": { "PredefinedMetricType":
 "LambdaProvisionedConcurrencyUtilization" }}'
```

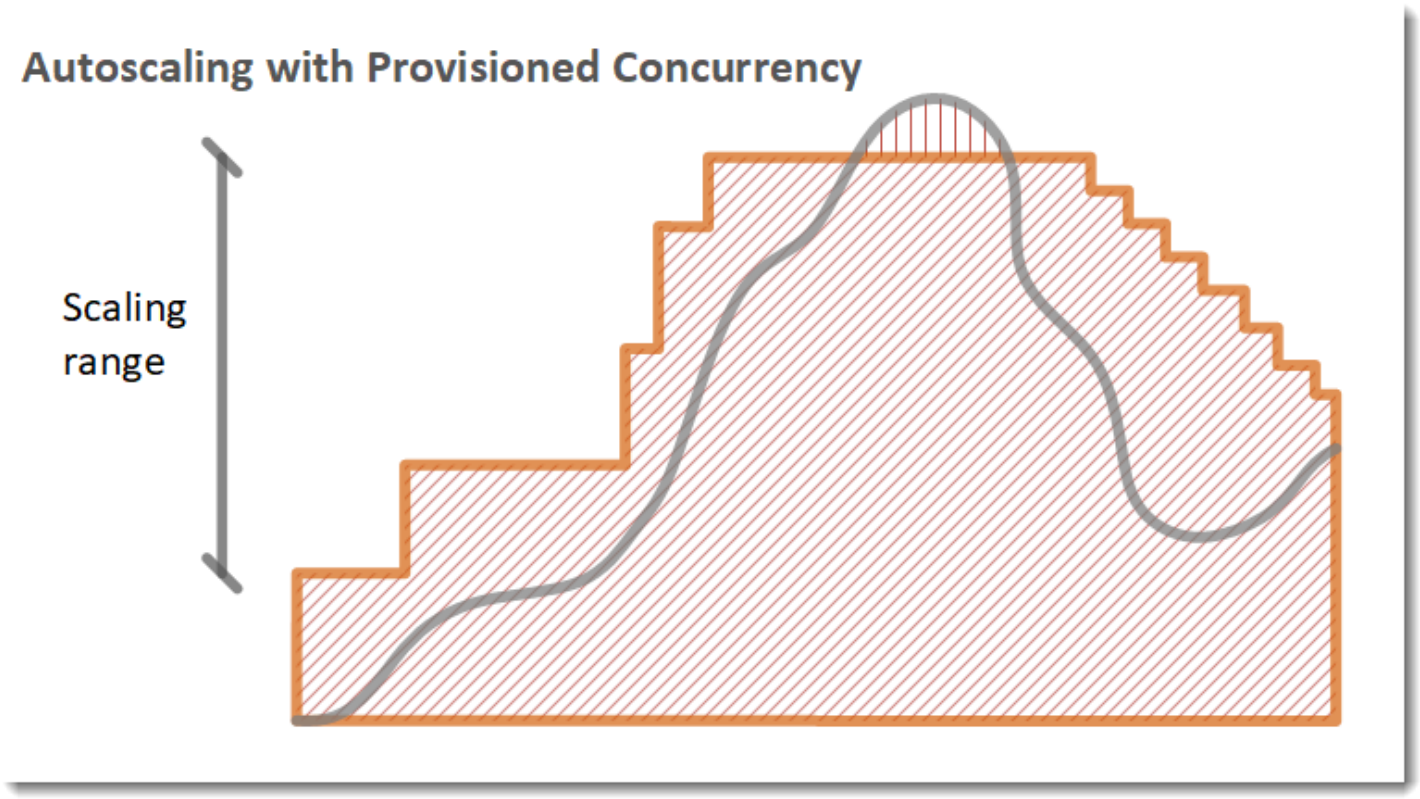
Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "PolicyARN": "arn:aws:autoscaling:us-
east-2:123456789012:scalingPolicy:12266dbb-1524-xmpl-a64e-9a0a34b996fa:resource/lambda/
function:my-function:BLUE:policyName/my-policy",
    "Alarms": [
        {
```

```
            "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7",
            "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmHigh-aed0e274-
xmpl-40fe-8cba-2e78f000c0a7"
        },
        {
            "AlarmName": "TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66",
            "AlarmARN": "arn:aws:cloudwatch:us-
east-2:123456789012:alarm:TargetTracking-function:my-function:BLUE-AlarmLow-7e1a928e-
xmpl-4d2b-8c01-782321bc6f66"
        }
    ]
}
```

Application Auto Scaling erstellt zwei Alarme in CloudWatch. Der erste Alarm wird ausgelöst, wenn die Auslastung der bereitgestellten Gleichzeitigkeit konstant 70 % überschreitet. In diesem Fall weist Application Auto Scaling mehr bereitgestellte Gleichzeitigkeit zu, um die Auslastung zu reduzieren. Der zweite Alarm wird ausgelöst, wenn die Auslastung konstant unter 63 % (90 % des 70-%-Ziels) liegt. In diesem Fall reduziert Application Auto Scaling wird die bereitgestellte Gleichzeitigkeit des Alias.

Im folgenden Beispiel skaliert eine Funktion basierend auf der Auslastung zwischen einem minimalen und einem maximalen Umfang bereitgestellter Gleichzeitigkeit.



Legende

- Funktions-Instances
- Offene Anforderungen
- Bereitgestellte Concurrency
- Standard-Gleichzeitigkeit

Wenn die Anzahl der offenen Anforderungen zunimmt, erhöht Application Auto Scaling die bereitgestellte Gleichzeitigkeit in großen Schritten, bis sie das konfigurierte Maximum erreicht. Danach kann die Funktion weiter die standardmäßige, nicht reservierte Gleichzeitigkeit skalieren, falls das Kontogleichzeitigkeitslimit nicht erreicht ist. Wenn die Auslastung sinkt und niedrig bleibt, verringert Application Auto Scaling die bereitgestellte Gleichzeitigkeit in kleineren periodischen Schritten.

Beide Alarme für Application Auto Scaling verwenden standardmäßig die Durchschnittsstatistik. Funktionen, die in kurzen Abständen auftretende Auslastungsmuster aufweisen, lösen diese Alarme möglicherweise nicht aus. Nehmen wir zum Beispiel an, Ihre Lambda-Funktion wird schnell ausgeführt (d. h. 20–100 ms) und der Datenverkehr kommt in kurzen Schüben (Bursts). In diesem Fall übersteigt die Anzahl der Anfragen die zugewiesene, bereitgestellte Gleichzeitigkeit während eines Bursts. Beim Application Auto Scaling muss die Burst-Last jedoch mindestens 3 Minuten lang aufrechterhalten werden, um zusätzliche Umgebungen bereitzustellen. Darüber hinaus benötigen beide CloudWatch Alarme 3 Datenpunkte, die den Zieldurchschnitt erreichen, um die Auto Scaling-Richtlinie zu aktivieren. Wenn Ihre Funktion schnell stark ausgelastet ist, kann die Verwendung der Maximum-Statistik anstelle der Durchschnittsstatistik effektiver sein, um die bereitgestellte Parallelität zu skalieren und so Kaltstarts zu minimieren.

Weitere Informationen zu Zielverfolgungs-Skalierungsrichtlinien finden Sie unter Zielverfolgungs-Skalierungsrichtlinien für das Application Auto Scaling.

Lambda-Skalierungsverhalten

Erhält Ihre Funktion mehr Anfragen, sorgt Lambda automatisch für die Skalierung der Anzahl der Ausführungsumgebungen, bis Ihr Konto das Nebenläufigkeitskontingent erreicht. Zum Schutz vor einer Überskalierung als Reaktion auf plötzliche Datenverkehrsspitzen begrenzt Lambda jedoch, wie schnell Ihre Funktionen skaliert werden können. Diese Nebenläufigkeitsskalierungsrate ist die maximale Rate, mit der Funktionen in Ihrem Konto als Reaktion auf erhöhte Anfragen skalieren können. (Das heißt, sie gibt an, wie schnell Lambda neue Ausführungsumgebungen erstellen kann.) Die Nebenläufigkeitsskalierungsrate unterscheidet sich vom Nebenläufigkeitslimit auf Kontoebene, bei dem es sich um die Gesamtmenge der für Ihre Funktionen verfügbaren Nebenläufigkeit handelt.

Nebenläufigkeitsskalierungsrate

In jeder AWS-Region-Funktion beträgt Ihre Skalierungsrate für Nebenläufigkeit 1 000 Instances der Ausführungsumgebung alle 10 Sekunden. Mit anderen Worten, alle 10 Sekunden kann Lambda jeder Ihrer Funktionen maximal 1 000 zusätzliche Instances der Ausführungsumgebung zuweisen.

Normalerweise müssen Sie sich über diese Einschränkung keine Gedanken machen. Die Skalierungsrate von Lambda ist für die meisten Anwendungsfälle ausreichend.

Wichtig ist, dass die Nebenläufigkeitsskalierungsrate ein Limit auf Funktionsebene ist. Das bedeutet, dass jede Funktion in Ihrem Konto unabhängig von anderen Funktionen skaliert werden kann.

> **Note**
>
> In der Praxis versucht Lambda, Ihre Nebenläufigkeitsskalierungsrate kontinuierlich im Laufe der Zeit aufzufüllen, anstatt alle 10 Sekunden eine einzige Nachfüllung von 1 000 Einheiten durchzuführen.

Lambda sammelt keine ungenutzten Teile Ihrer Nebenläufigkeitsskalierungsrate an. Das bedeutet, dass Ihre Skalierungsrate zu jedem Zeitpunkt immer maximal 1 000 Nebenläufigkeitseinheiten beträgt. Wenn Sie beispielsweise in einem 10-Sekunden-Intervall keine der verfügbaren 1 000 Nebenläufigkeitseinheiten verwenden, werden Sie im nächsten 10-Sekunden-Intervall keine 1 000 zusätzlichen Einheiten ansammeln. Ihre Skalierungsrate für Nebenläufigkeit liegt im nächsten 10-Sekunden-Intervall immer noch bei 1 000.

Solange Ihre Funktion weiterhin eine steigende Anzahl von Anfragen erhält, skaliert Lambda mit der schnellsten Rate, die Ihnen zur Verfügung steht, bis zum Nebenläufigkeitslimit Ihres Kontos. Sie

können das Volumen der Nebenläufigkeit einschränken, die einzelne Funktionen verwenden können, indem Sie die reservierte Nebenläufigkeit konfigurieren. Wenn Anforderungen schneller eingehen, als Ihre Funktion sie skalieren kann, oder wenn Ihre Funktion die maximale Nebenläufigkeit erreicht hat, schlagen weitere Anforderungen mit einem Drosselungsfehler (Statuscode 429) fehl.

Überwachen der Gleichzeitigkeit

Lambda gibt Amazon- CloudWatch Metriken aus, um Ihnen bei der Überwachung der Gleichzeitigkeit für Ihre Funktionen zu helfen. In diesem Thema werden diese Metriken und ihre Interpretation erläutert.

Sections

Allgemeine Metriken für Gleichzeitigkeit

Verwenden Sie die folgenden Metriken, um die Gleichzeitigkeit Ihrer Lambda-Funktionen zu überwachen. Die Granularität für jede Metrik ist 1 Minute.

- `ConcurrentExecutions` – Die Anzahl der aktiven gleichzeitigen Aufrufe zu einem bestimmten Zeitpunkt. Lambda gibt diese Metrik für alle Funktionen, Versionen und Aliasse aus. Für jede Funktion in der Lambda-Konsole zeigt Lambda das Diagramm für `ConcurrentExecutions` nativ auf der Registerkarte Überwachung unter Metriken an. Sehen Sie sich diese Metrik mit MAX an.
- `UnreservedConcurrentExecutions` – Die Anzahl der aktiven gleichzeitigen Aufrufe, die nicht reservierte Gleichzeitigkeit verwenden. Lambda gibt diese Metriken for alle Funktionen in einer Region aus. Sehen Sie sich diese Metrik mit MAX an.
- `ClaimedAccountConcurrency` – Die Menge an Gleichzeitigkeit, die für On-Demand-Aufrufe nicht verfügbar ist. `ClaimedAccountConcurrency` entspricht `UnreservedConcurrentExecutions` plus dem Betrag der zugewiesenen Gleichzeitigkeit (d. h. der gesamten reservierten Gleichzeitigkeit plus der gesamten bereitgestellten Gleichzeitigkeit). Wenn das Kontogleichzeitigkeitslimit für `ClaimedAccountConcurrency` überschritten wird, können Sie ein höheres Kontogleichzeitigkeitslimit beantragen. Sehen Sie sich diese Metrik mit MAX an. Weitere Informationen finden Sie unter Die Metrik `ClaimedAccountConcurrency`.

Metriken für Provisioned Concurrency

Verwenden Sie die folgenden Metriken, um Lambda-Funktionen mit bereitgestellter Gleichzeitigkeit zu überwachen. Die Granularität für jede Metrik ist 1 Minute.

- `ProvisionedConcurrentExecutions` – Die Anzahl der Instances der Ausführungsumgebung, die einen Aufruf bei bereitgestellter Gleichzeitigkeit aktiv verarbeiten. Lambda gibt diese Metrik für jede Funktionsversion und jeden Alias aus, wobei die bereitgestellte Gleichzeitigkeit konfiguriert ist. Sehen Sie sich diese Metrik mit MAX an.

`ProvisionedConcurrentExecutions` entspricht nicht der Gesamtzahl der bereitgestellten Gleichzeitigkeit, die Sie zuweisen. Nehmen wir zum Beispiel an, Sie weisen einer Funktionsversion 100 Einheiten der bereitgestellten Gleichzeitigkeit zu. Wenn in einer bestimmten Minute höchstens 50 dieser 100 Ausführungsumgebungen gleichzeitig Aufrufe verarbeiten, dann ist der Wert von MAX(`ProvisionedConcurrentExecutions`) 50.

- `ProvisionedConcurrentInvocations` – Die Häufigkeit, mit der Lambda Ihren Funktionscode mit bereitgestellter Gleichzeitigkeit aufruft. Lambda gibt diese Metrik für jede Funktionsversion und jeden Alias aus, wobei die bereitgestellte Gleichzeitigkeit konfiguriert ist. Sehen Sie sich diese Metrik mit SUM an.

`ProvisionedConcurrentInvocations` unterscheidet sich von `ProvisionedConcurrentExecutions` dadurch, dass `ProvisionedConcurrentInvocations` die Gesamtzahl der Aufrufe zählt, während `ProvisionedConcurrentExecutions` die Anzahl der aktiven Umgebungen zählt. Um diesen Unterschied zu verstehen, betrachten Sie das folgende Szenario:

In diesem Beispiel nehmen wir an, dass Sie 1 Aufruf pro Minute erhalten und jeder Aufruf 2 Minuten dauert. Jeder orangefarbene horizontale Balken steht für eine einzelne Anfrage. Nehmen wir an,

dass Sie dieser Funktion 10 Einheiten der bereitgestellten Gleichzeitigkeit zuweisen, sodass jede Anforderung mit bereitgestellter Gleichzeitigkeit ausgeführt wird.

Zwischen den Minuten 0 und 1 trifft `Request 1` ein. Bei Minute 1 ist der Wert für MAX(`ProvisionedConcurrentExecutions`) 1, da in der vergangenen Minute höchstens 1 Ausführungsumgebung aktiv war. Der Wert für SUM(`ProvisionedConcurrentInvocations`) ist ebenfalls 1, da in der letzten Minute 1 neue Anforderung eingegangen ist.

Zwischen den Minuten 1 und 2 trifft `Request 2` ein, während `Request 1` weiterläuft. Bei Minute 2 ist der Wert für MAX(`ProvisionedConcurrentExecutions`) 2, da in der letzten Minute höchstens 2 Ausführungsumgebungen aktiv waren. Der Wert für SUM(`ProvisionedConcurrentInvocations`) ist jedoch 1, da in der letzten Minute nur 1 neue Anforderung eingegangen ist. Dieses Verhalten der Metrik setzt sich bis zum Ende des Beispiels fort.

- `ProvisionedConcurrencySpilloverInvocations` – Die Häufigkeit, mit der Lambda Ihre Funktion bei standardmäßiger (reservierter oder nicht reservierter) Gleichzeitigkeit aufruft, wenn die gesamte bereitgestellte Gleichzeitigkeit verwendet wird. Lambda gibt diese Metrik für jede Funktionsversion und jeden Alias aus, wobei die bereitgestellte Gleichzeitigkeit konfiguriert ist. Sehen Sie sich diese Metrik mit SUM an. Der Wert von `ProvisionedConcurrentInvocations` + `ProvisionedConcurrencySpilloverInvocations` sollte der Gesamtzahl der Funktionsaufrufe (d. h. der `Invocations`-Metrik) entsprechen.

  `ProvisionedConcurrencyUtilization` – Der prozentuale Anteil der bereitgestellten Gleichzeitigkeit, der genutzt wird (d. h. der Wert von `ProvisionedConcurrentExecutions` geteilt durch die Gesamtmenge der bereitgestellten Gleichzeitigkeit). Lambda gibt diese Metrik für jede Funktionsversion und jeden Alias aus, wobei die bereitgestellte Gleichzeitigkeit konfiguriert ist. Sehen Sie sich diese Metrik mit MAX an.

Nehmen wir zum Beispiel an, Sie teilen einer Funktionsversion 100 Einheiten der bereitgestellten Gleichzeitigkeit zu. Wenn in einer bestimmten Minute höchstens 60 dieser 100 Ausführungsumgebungen gleichzeitig Aufrufe verarbeiten, dann ist der Wert von MAX(`ProvisionedConcurrentExecutions`) 60 und der Wert von MAX(`ProvisionedConcurrentUtilization`) ist 0,6.

Ein hoher Wert für `ProvisionedConcurrencySpilloverInvocations` kann darauf hinweisen, dass Sie zusätzliche bereitgestellte Gleichzeitigkeit für Ihre Funktion zuteilen müssen. Alternativ können Sie Application Auto Scaling konfigurieren, um die automatische Skalierung der bereitgestellten Gleichzeitigkeit auf der Grundlage von vordefinierten Schwellenwerten zu steuern.

Umgekehrt können konstant niedrige Werte für `ProvisionedConcurrencyUtilization` darauf hindeuten, dass Sie Ihrer Funktion zu viel bereitgestellte Gleichzeitigkeit zugeteilt haben.

Die Metrik `ClaimedAccountConcurrency`

Lambda verwendet die Metrik `ClaimedAccountConcurrency`, um zu ermitteln, wie viel Gleichzeitigkeit in Ihrem Konto für On-Demand-Aufrufe verfügbar ist. Lambda berechnet `ClaimedAccountConcurrency` mit der folgenden Formel:

```
ClaimedAccountConcurrency = UnreservedConcurrentExecutions + (allocated concurrency)
```

`UnreservedConcurrentExecutions` ist die Anzahl der aktiven gleichzeitigen Aufrufe, die nicht reservierte Gleichzeitigkeit verwenden. Die zugewiesene Gleichzeitigkeit ist die Summe der folgenden beiden Teile (wobei RC für „reservierte Gleichzeitigkeit“ und PC für „bereitgestellte Gleichzeitigkeit“ steht):

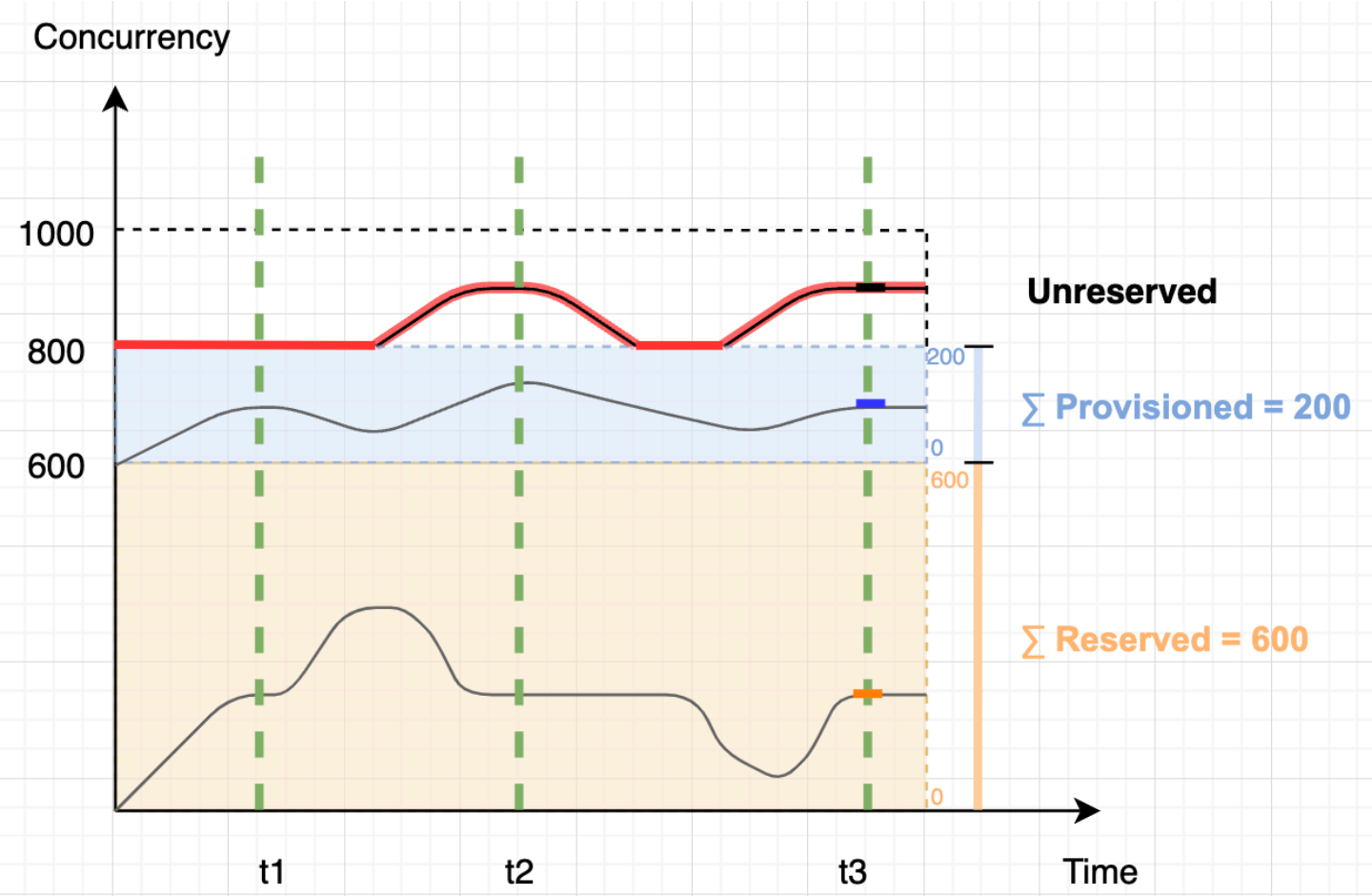
- Die gesamte RC aller Funktionen in einer Region.
- Die gesamte PC aller Funktionen in einer Region, die PC verwenden, ohne Funktionen, die RC verwenden.

> **Note**
>
> Sie können einer Funktion nicht mehr PC als RC zuweisen. Somit ist die RC einer Funktion immer größer oder gleich der PC. Um den Beitrag zur zugewiesenen Gleichzeitigkeit für solche Funktionen mit PC und RC zu berechnen, berücksichtigt Lambda nur RC, welches das Maximum der beiden ist.

Lambda verwendet die Metrik `ClaimedAccountConcurrency` anstelle von `ConcurrentExecutions`, um zu ermitteln, wie viel Gleichzeitigkeit für On-Demand-Aufrufe verfügbar ist. Die Metrik `ConcurrentExecutions` ist zwar nützlich, um die Anzahl der aktiven gleichzeitigen Aufrufe nachzuverfolgen, spiegelt jedoch nicht immer die tatsächliche Verfügbarkeit von Gleichzeitigkeit wider. Das liegt daran, dass Lambda bei der Bestimmung der Verfügbarkeit auch die reservierte und die bereitgestellte Gleichzeitigkeit berücksichtigt.

Stellen Sie sich zur Veranschaulichung von `ClaimedAccountConcurrency` ein Szenario vor, in dem Sie sehr viel reservierte und bereitgestellte Gleichzeitigkeit für Ihre Funktionen

konfigurieren, die weitgehend ungenutzt bleiben. Gehen Sie im folgenden Beispiel nun davon aus, dass Ihr Kontogleichzeitigkeitslimit 1 000 beträgt und dass Ihr Konto über zwei Hauptfunktionen verfügt: `function-orange` und `function-blue`. Sie weisen `function-orange` 600 reservierte Gleichzeitigkeitseinheiten zu. Sie weisen `function-blue` 200 bereitgestellte Gleichzeitigkeitseinheiten zu. Nehmen wir an, dass Sie im Laufe der Zeit zusätzliche Funktionen bereitstellen und das folgende Datenverkehrsmuster beobachten:



Im vorherigen Diagramm stehen die schwarzen Linien für die tatsächliche Nutzung der Gleichzeitigkeit im Zeitverlauf, und die rote Linie für den Wert `ClaimedAccountConcurrency` im Zeitverlauf. In diesem Szenario beträgt der Wert von `ClaimedAccountConcurrency` mindestens 800, obwohl die tatsächliche Gleichzeitigkeitsauslastung aller Funktionen gering ist. Das liegt daran, dass Sie insgesamt 800 Gleichzeitigkeitseinheiten für `function-orange` und `function-blue` zugewiesen haben. Aus Sicht von Lambda haben Sie diese Gleichzeitigkeit zur Nutzung „beansprucht“, sodass Ihnen praktisch nur noch 200 Gleichzeitigkeitseinheiten für andere Funktionen zur Verfügung stehen.

Für dieses Szenario beträgt die zugewiesene Gleichzeitigkeit in der `ClaimedAccountConcurrency`-Formel 800. Daraus können wir den Wert von `ClaimedAccountConcurrency` an verschiedenen Stellen im Diagramm ableiten:

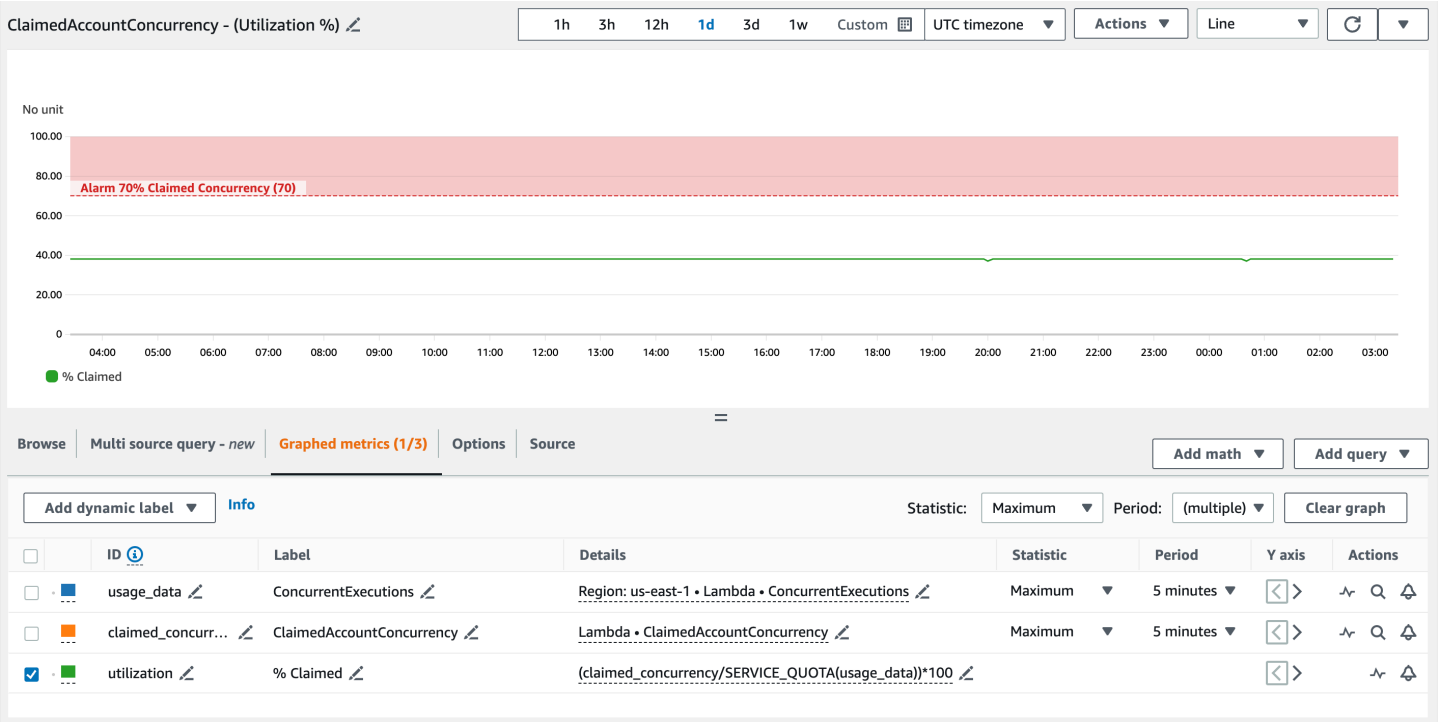
- Bei `t1`, `ClaimedAccountConcurrency` ist der Wert 800 (800 + 0 `UnreservedConcurrentExecutions`).
- Bei `t2`, `ClaimedAccountConcurrency` ist der Wert 900 (800 + 100 `UnreservedConcurrentExecutions`).
- Bei `t3`, `ClaimedAccountConcurrency` ist der Wert wieder 900 (800 + 100 `UnreservedConcurrentExecutions`).

Einrichten der -**`ClaimedAccountConcurrency`**Metrik in CloudWatch

Lambda gibt die `ClaimedAccountConcurrency` Metrik in aus CloudWatch. Verwenden Sie diese Metrik zusammen mit dem Wert von `SERVICE_QUOTA(ConcurrentExecutions)`, um die prozentuale Nutzung der Gleichzeitigkeit in Ihrem Konto zu ermitteln, wie in der folgenden Formel dargestellt:

```
Utilization = (ClaimedAccountConcurrency/SERVICE_QUOTA(ConcurrentExecutions)) * 100%
```

Der folgende Screenshot zeigt, wie Sie diese Formel in grafisch darstellen können CloudWatch. Die grüne `claim_utilization`-Linie steht für die Gleichzeitigkeitsauslastung in diesem Konto, die bei etwa 40 % liegt:



Der vorherige Screenshot enthält auch einen CloudWatch Alarm, der in den `ALARM` Status wechselt, wenn die Gleichzeitigkeitsauslastung 70 % überschreitet. Sie können die `ClaimedAccountConcurrency`-Metrik zusammen mit ähnlichen Alarmen verwenden, um proaktiv zu bestimmen, wann Sie möglicherweise ein höheres Kontengleichzeitigkeitslimit beantragen müssen.

Konfigurieren der Codesignatur für AWS Lambda

Codesignatur für AWS Lambda hilft sicherzustellen, dass nur vertrauenswürdiger Code in Ihren Lambda-Funktionen ausgeführt wird. Wenn Sie die Codesignatur für eine Funktion aktivieren, überprüft Lambda jede Codebereitstellung und überprüft, ob das Codepaket von einer vertrauenswürdigen Quelle signiert wurde.

> **Note**
>
> Funktionen, die als Container-Images definiert sind, unterstützen keine Codesignatur.

Um die Codeintegrität zu überprüfen, erstellen Sie mit AWS Signer digital signierte Code-Pakete für Funktionen und Ebenen. Wenn ein Benutzer versucht, ein Code-Paket bereitzustellen, führt Lambda Validierungsprüfungen für das Codepaket durch, bevor es die Bereitstellung akzeptiert. Da die Validierungsprüfungen von Codesignatur zum Zeitpunkt der Bereitstellung ausgeführt werden, gibt es keine Auswirkungen auf die Ausführung der Funktion.

Sie verwenden AWS Signer auch, um Signaturprofile zu erstellen. Sie verwenden ein Signaturprofil, um das signierte Codepaket zu erstellen. Verwenden Sie AWS Identity and Access Management (IAM), um zu steuern, wer Codepakete signieren und Signaturprofile erstellen kann. Weitere Informationen finden Sie unter Authentication and Access Control im AWS -Entwicklerhandbuch.

Um die Codesignatur für eine Funktion zu aktivieren, erstellen Sie eine Codesignatur-Konfiguration und hängen sie an die Funktion an. Eine Codesignatur-Konfiguration definiert eine Liste der zulässigen Signaturprofile und die Richtlinienaktion, die durchgeführt werden soll, wenn eine der Validierungsprüfungen fehlschlägt.

Lambda-Ebenen folgen demselben signierten Code-Paketformat wie Funktionscode-Pakete. Wenn Sie einer Funktion, für die die Codesignatur von Code aktiviert ist, überprüft Lambda, ob die Ebene von einem zulässigen Signaturprofil signiert wurde. Wenn Sie die Codesignatur für eine Funktion aktivieren, müssen alle Ebenen, die der Funktion hinzugefügt werden, auch von einem der zulässigen Signaturprofile signiert werden.

Verwenden Sie IAM, um zu steuern, wer Codesignatur-Konfigurationen erstellen kann. In der Regel erlauben Sie nur bestimmten administrativen Benutzern, diese Fähigkeit zu nutzen. Darüber hinaus können Sie IAM-Richtlinien einrichten, die durchsetzen, dass Entwickler nur Funktionen erstellen, für die die Codesignatur aktiviert ist.

Sie können die Codesignatur so konfigurieren, dass Änderungen in aufgezeichnet werde AWS CloudTrail. Erfolgreiche und blockierte Bereitstellungen für -Funktionen werden in CloudTrail mit Informationen über die Signatur- und Validierungsprüfungen protokolliert.

Sie können die Codesignatur für Ihre Funktionen mithilfe der Lambda-Konsole, der AWS Command Line Interface (AWS CLI) AWS CloudFormation und der AWS Serverless Application Model () konfigurieren AWS SAM.

Für die Verwendung von AWS Signer oder die Codesignatur für fallen keine zusätzlichen Gebühren an AWS Lambda.

Sections

Signaturvalidierung

Lambda führt die folgenden Validierungsprüfungen durch, wenn Sie ein signiertes Codepaket für Ihre Funktion bereitstellen:

1. Integrität – Überprüft, dass das Codepaket seit seiner Unterzeichnung nicht geändert wurde. Lambda vergleicht den Hash des Pakets mit dem Hash aus der Signatur.
2. Ablauf – Bestätigt, dass die Signatur des Codepakets nicht abgelaufen ist.
3. Diskrepanz – Bestätigt, dass das Codepaket mit einem der zulässigen Signaturprofile für die Lambda-Funktion signiert ist. Eine Diskrepanz tritt auch auf, wenn keine Signatur vorhanden ist.
4. Widerruf – Bestätigt, dass die Signatur des Codepakets nicht widerrufen wurde.

Die in der Codesignatur-Konfiguration definierte Richtlinie zur Signaturüberprüfung legt fest, welche der folgenden Aktionen Lambda durchführt, wenn eine der Validierungsprüfungen fehlschlägt:

- Warnung – Lambda ermöglicht die Bereitstellung des Codepakets, gibt jedoch eine Warnung aus. Lambda gibt eine neue Amazon- CloudWatch Metrik aus und speichert auch die Warnung im CloudTrail Protokoll.
- Durchsetzung – Lambda gibt eine Warnung aus (wie bei der Warn-Aktion) und blockiert die Bereitstellung des Codepakets.

Sie können die Richtlinie für Ablauf-, Diskrepanz- und Widerrufsvalidierung konfigurieren. Beachten Sie, dass Sie eine Richtlinie für die Integritätsvalidierung nicht konfigurieren können. Schlägt die Integritätsvalidierung fehl, blockiert Lambda die Bereitstellung.

Voraussetzungen für die Konfiguration

Bevor Sie die Codesignatur für eine Lambda-Funktion konfigurieren können, verwenden Sie AWS Signer, um Folgendes zu tun:

- Erstellen Sie ein oder mehrere Signaturprofile.
- Verwenden Sie ein Signaturprofil, um ein signiertes Codepaket für Ihre Funktion zu erstellen.

Weitere Informationen finden Sie unter Creating Signing Profiles (Console) im AWS Signer-Entwicklerhandbuch.

Erstellen von Codesignatur-Konfigurationen

Mit einer Codesignatur-Konfiguration wird eine Liste der zulässigen Signaturprofile und die Richtlinie für Signaturvalidierung definiert.

So erstellen Sie eine Codesignatur-Konfiguration (Konsole)

1. Öffnen Sie die Seite Codesignatur-Konfigurationen der Lambda-Konsole.
2. Wählen Sie Create configuration (Konfiguration erstellen).
3. Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen für die Konfiguration ein.
4. Fügen Sie der Konfiguration unter Signaturprofile bis zu 20 Signaturprofile hinzu.
    a. Wählen Sie für ARN der Signaturprofilversion den Amazon-Ressourcennamen (ARN) einer Profilversion aus oder geben Sie den ARN ein.
    b. Um ein zusätzliches Signaturprofil hinzuzufügen, wählen Sie Signaturprofil hinzufügen aus.

5. Wählen Sie unter Richtlinie zur Signaturvalidierung die Option Warnen oder Durchsetzen aus.
6. Wählen Sie Create configuration (Konfiguration erstellen).

Aktualisieren der Codesignatur-Konfiguration

Wenn Sie eine Codesignatur-Konfiguration aktualisieren, wirken sich die Änderungen auf die zukünftigen Bereitstellungen von Funktionen aus, an die die Codesignatur-Konfiguration angehängt ist.

So aktualisieren Sie eine Codesignatur-Konfiguration (Konsole)

1. Öffnen Sie die Seite Codesignatur-Konfigurationen der Lambda-Konsole.
2. Wählen Sie eine zu aktualisierende Codesignatur-Konfiguration aus und klicken Sie dann auf Bearbeiten.
3. Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen für die Konfiguration ein.
4. Fügen Sie der Konfiguration unter Signaturprofile bis zu 20 Signaturprofile hinzu.
    a. Wählen Sie für ARN der Signaturprofilversion den Amazon-Ressourcennamen (ARN) einer Profilversion aus oder geben Sie den ARN ein.
    b. Um ein zusätzliches Signaturprofil hinzuzufügen, wählen Sie Signaturprofil hinzufügen aus.
5. Wählen Sie unter Richtlinie zur Signaturvalidierung die Option Warnen oder Durchsetzen aus.
6. Wählen Sie Änderungen speichern aus.

Löschen einer Codesignatur-Konfiguration

Sie können eine Codesignatur-Konfiguration nur löschen, wenn sie keine Funktionen verwenden.

So löschen Sie eine Codesignaturigning-Konfiguration (Konsole)

1. Öffnen Sie die Seite Codesignatur-Konfigurationen der Lambda-Konsole.
2. Wählen Sie eine zu löschende Codesignatur-Konfiguration aus und klicken Sie dann auf Löschen.
3. Um dies zu bestätigen, wählen Sie erneut Löschen .

Aktivieren der Codesignatur für eine Funktion

Um die Codesignatur für eine Funktion zu aktivieren, verknüpfen Sie eine Codesignatur-Konfiguration mit der Funktion.

So verknüpfen Sie eine Codesignatur-Konfiguration mit einer Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, für die Sie die Codesignatur aktivieren möchten.
3. Öffnen Sie die Registerkarte Configuration (Konfiguration).
4. Scrollen Sie nach unten und wählen Sie Codesignatur aus.
5. Wählen Sie Bearbeiten aus.
6. Wählen Sie i n Codesignatur bearbeiten eine Codesignatur-Konfiguration für diese Funktion aus.
7. Wählen Sie Save aus.

Konfigurieren von IAM-Richtlinien

Um einem Benutzer die Berechtigung zum Zugriff auf die Codesignatur-API-Vorgänge zu erteilen, fügen Sie der Benutzerrichtlinie eine oder mehrere Richtlinienanweisungen bei. Weitere Informationen zu Benutzerrichtlinien finden Sie unter Arbeiten mit identitätsbasierten IAM-Richtlinien in Lambda.

Die folgende Beispiel-Richtlinienanweisung gewährt die Berechtigung zum Erstellen, Aktualisieren und Abrufen von Codesignatur-Konfigurationen.

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

```
}
```

Administratoren können den `CodeSigningConfigArn`-Bedingungsschlüssel verwenden, um die Codesignatur-Konfigurationen anzugeben, mit denen Entwickler Ihre Funktionen erstellen oder aktualisieren müssen.

Die folgende Beispielrichtlinienanweisung gewährt die Berechtigung zum Erstellen einer Funktion. Die Richtlinienanweisung enthält eine `lambda:CodeSigningConfigArn`-Bedingung, um die zulässige Konfiguration für die Codesignierung anzugeben. Lambda blockiert alle `CreateFunction`-API-Anfrage, wenn der `CodeSigningConfigArn`-Paramter fehlt oder nicht mit dem Wert in der Bedingung übereinstimmt.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReferencingCodeSigningConfig",
      "Effect": "Allow",
      "Action": [
          "lambda:CreateFunction",
        ],
      "Resource": "*",
      "Condition": {
          "StringEquals": {
              "lambda:CodeSigningConfigArn":
                  “arn:aws:lambda:us-west-2:123456789012:code-signing-
config:csc-0d4518bd353a0a7c6”
          }
      }
    }
  ]
}
```

Konfigurieren der Codesignatur mit der Lambda API

Verwenden Sie die folgenden API-Operationen, um Codesignaturkonfigurationen mit der AWS CLI oder dem AWS SDK zu verwalten:

- ListCodeSigningConfigs
- CreateCodeSigningConfig

- GetCodeSigningConfig
- UpdateCodeSigningConfig
- DeleteCodeSigningConfig

Um die Codesignatur-Konfiguration für eine Funktion zu verwalten, verwenden Sie die folgenden API-Vorgänge:

- CreateFunction
- GetFunctionCodeSigningConfig
- PutFunctionCodeSigningConfig
- DeleteFunctionCodeSigningConfig
- ListFunctionsByCodeSigningConfig

Verwenden von Tags für Lambda-Funktionen

Sie können AWS Lambda-Funktionen markieren, um die attributbasierte Zugriffskontrolle (ABAC) zu aktivieren und sie nach Eigentümer, Projekt oder Abteilung zu organisieren. Tags sind frei formulierte Schlüssel-Wert-Paare, die von AWS-Services zur Verwendung in ABAC, zum Filtern von Ressourcen und zum Hinzufügen von Details zu Abrechnungsberichten unterstützt werden.

Tags gelten für die Funktionsebene, nicht für Versionen oder Aliase. Tags sind nicht Teil der versionspezifischen Konfiguration, von der Lambda einen Snapshot erstellt, wenn Sie eine Version veröffentlichen.

Sections

Erforderliche Berechtigungen zum Arbeiten mit Tags

Gewähren Sie der AWS Identity and Access Management (IAM)-Identität (Benutzer, Gruppe oder Rolle) für die Person, die mit der Funktion arbeitet, die entsprechenden Berechtigungen:

- lambda:ListTags – Wenn eine Funktion Tags hat, erteilen Sie diese Berechtigung jedem, der `GetFunction` oder aufrufen mussListTags.
- lambda:TagResource – Erteilen Sie diese Berechtigung jedem, der `CreateFunction` oder aufrufen mussTagResource.

Weitere Informationen finden Sie unter Arbeiten mit identitätsbasierten IAM-Richtlinien in Lambda.

Verwendung von Tags mit der Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um Funktionen mit Tags zu erstellen, Tags zu vorhandenen Funktionen hinzuzufügen und Funktionen nach von Ihnen hinzugefügten Tags zu filtern.

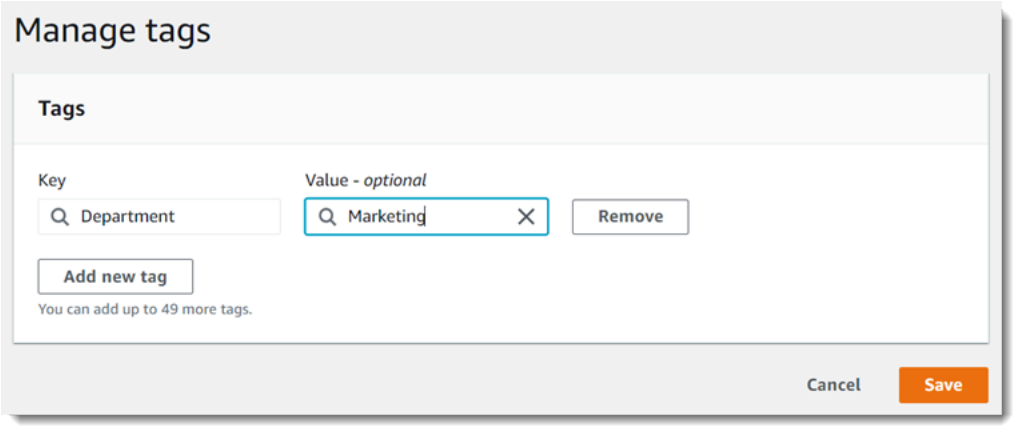
Hinzufügen von Tags beim Erstellen einer Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie Funktion erstellen.
3. Klicken Sie auf Ohne Vorgabe erstellen oder Container-Image.
4. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie für Funktionsname den Funktionsnamen ein. Funktionsnamen sind auf eine Länge von 64 Zeichen beschränkt.
   b. Wählen Sie für Laufzeit die Sprachversion aus, die für Ihre Funktion verwendet werden soll.
   c. (Optional) Wählen Sie für Architecture (Architektur) die Befehlssatz-Architektur aus, die Sie für Ihre Funktion verwenden möchten. Die Standardarchitektur ist x86_64. Stellen Sie beim Erstellen des Bereitstellungspakets für Ihre Funktion sicher, dass es mit der von Ihnen gewählten Befehlssatzarchitektur kompatibel ist.
5. Erweitern Sie Advanced settings (Erweiterte Einstellungen) und wählen Sie dann Enable tags (Tags aktivieren) aus.
6. Wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie dann einen Key (Schlüssel) und einen optionalen Value (Wert) ein. Wiederholen Sie diesen Schritt, um weitere Tags hinzuzufügen.
7. Wählen Sie Funktion erstellen.

Hinzufügen von Tags zu einer bestehenden Funktion

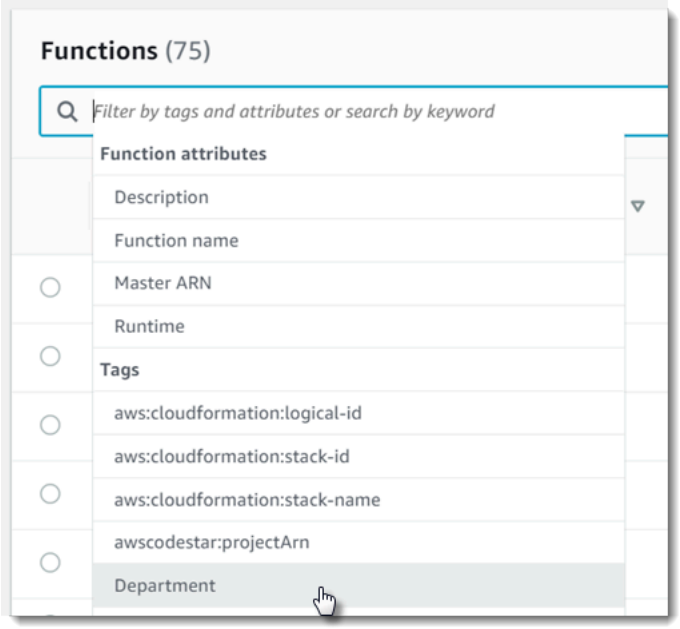
1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie Configuraton (Konfiguration) und dann Tags aus.
4. Wählen Sie unter Tags die Option Manage tags (Tags verwalten) aus.
5. Wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie dann einen Key (Schlüssel) und einen optionalen Value (Wert) ein. Wiederholen Sie diesen Schritt, um weitere Tags hinzuzufügen.



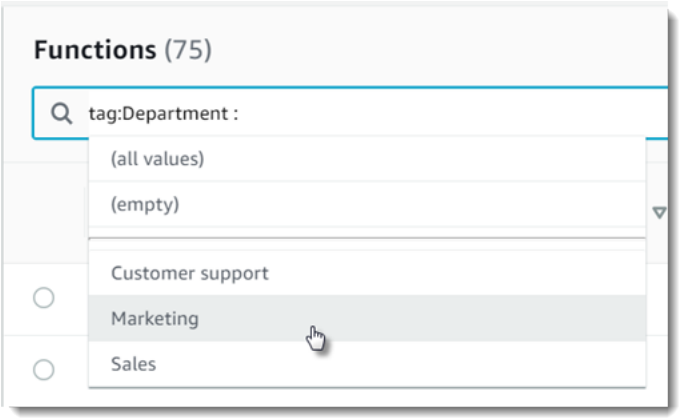
6. Wählen Sie Save aus.

So filtern Sie Funktionen mit Tags

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Suchleiste aus, um eine Liste mit Funktionsattributen und Tag-Schlüsseln anzuzeigen.



3. Wählen Sie einen Tag-Schlüssel aus, um eine Liste der Werte anzuzeigen, die in der aktuellen AWS-Region verwendet werden.
4. Wählen Sie einen Wert aus, um Funktionen mit diesem Wert anzuzeigen, oder wählen Sie (all Values) (alle Werte) aus, um alle Funktionen anzuzeigen, die ein Tag mit diesem Schlüssel haben.



Die Suchleiste unterstützt auch die Suche nach Tag-Schlüsseln. Geben Sie `tag` ein, um nur eine Liste der Tag-Schlüssel anzuzeigen, oder geben Sie den Namen eines Schlüssels ein, um ihn in der Liste zu suchen.

Verwenden von Tags mit AWS CLI

Hinzufügen und Entfernen von Tags

Um eine neue Lambda-Funktion mit Tags zu erstellen, verwenden Sie den create-function-Befehl mit der Option --tags.

```
aws lambda create-function --function-name my-function
--handler index.js --runtime nodejs20.x \
--role arn:aws:iam::123456789012:role/lambda-role \
--tags Department=Marketing,CostCenter=1234ABCD
```

Verwenden Sie den Befehl tag-resource, um Tags zu einer bestehenden Funktion hinzuzufügen.

```
aws lambda tag-resource \
--resource arn:aws:lambda:us-east-2:123456789012:function:my-function \
--tags Department=Marketing,CostCenter=1234ABCD
```

Mit dem Befehl untag-resource können Sie Tags entfernen.

```
aws lambda untag-resource --resource arn:aws:lambda:us-east-1:123456789012:function:my-
function \
--tag-keys Department
```

Anzeigen von Tags in einer Funktion

Wenn Sie die Tags anzeigen möchten, die auf eine bestimmte Lambda-Funktion angewendet werden, können Sie einen der folgenden AWS CLI-Befehle verwenden:

- ListTags – Um eine Liste der dieser Funktion zugeordneten Tags anzuzeigen, fügen Sie Ihren Lambda-Funktions-ARN (Amazon-Ressourcenname) ein:

```
aws lambda list-tags --resource arn:aws:lambda:us-east-1:123456789012:function:my-function
```

- GetFunction – Um eine Liste der Tags anzuzeigen, die dieser Funktion zugeordnet sind, geben Sie Ihren Lambda-Funktionsnamen an:

```
aws lambda get-function --function-name my-function
```

Filtern von Funktionen nach Tag

Sie können die AWS Resource Groups Tagging API GetResources -API-Operation verwenden, um Ihre Ressourcen nach Tags zu filtern. Die `GetResources`-Operation empfängt bis zu 10 Filter, wobei jeder Filter einen Tag-Schlüssel und bis zu 10 Tag-Werte enthält. Sie stellen `GetResources` mit einem `ResourceType` zur Verfügung, um nach bestimmten Ressourcentypen zu filtern.

Weitere Informationen zu AWS Resource Groups finden Sie unter Was sind Ressourcengruppen? im AWS Resource Groups- und im Tags-Benutzerhandbuch.

Anforderungen für Tags

Für Tags gelten folgende Anforderungen:

- Maximale Anzahl von Tags pro Ressource: 50
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden.
- Verwenden Sie in Tag-Namen oder -Werten nicht das Präfix `aws:`, da es für die AWS-Verwendung reserviert ist. Sie können keine Tag-Namen oder Werte mit diesem Präfix bearbeiten oder löschen. Tags mit diesem Präfix werden nicht als Ihre Tags pro Ressourcenlimit angerechnet.

- Wenn Sie Ihr Tagging-Schema in mehreren Services und Ressourcen verwenden wollen, denken Sie daran, dass andere Services möglicherweise Einschränkungen bei den zulässigen Zeichen haben. Im allgemeinen zulässige Zeichen: Buchstaben, Leerzeichen und Zahlen, die in UTF-8 darstellbar sind, sowie die folgenden Sonderzeichen: + - = . _ : / @.

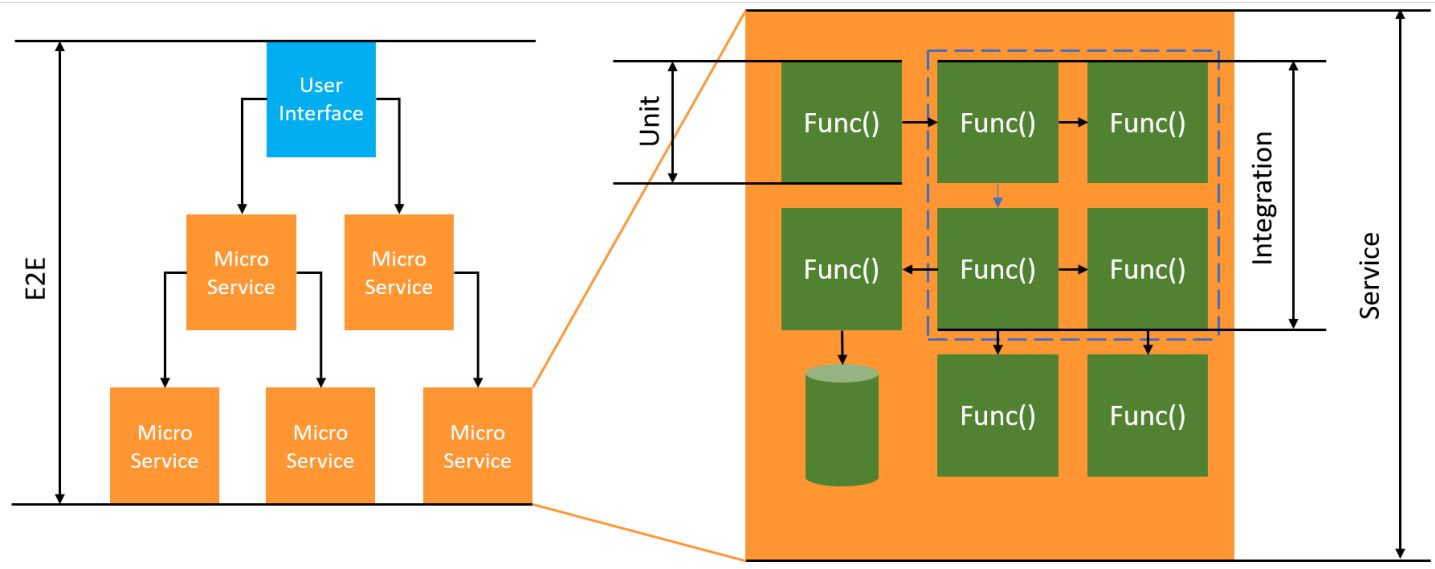
So testen Sie serverlose Funktionen und Anwendungen

Beim Testen der Serverless-Funktionen werden herkömmliche Testtypen und -techniken verwendet. Erwägen Sie jedoch auch das Testen der Serverless-Anwendungen als Ganzes. Cloud-basierte Tests bieten das genaueste Maß für die Qualität sowohl Ihrer Funktionen als auch Ihrer Serverless-Anwendungen.

Eine Serverless-Anwendungsarchitektur umfasst verwaltete Services, die über API-Aufrufe wichtige Anwendungsfunktionen bereitstellen. Aus diesem Grund muss Ihr Entwicklungszyklus automatisierte Tests beinhalten, die bei der Interaktion Ihrer Funktionen und Services die Funktionalität überprüfen.

Wenn Sie keine cloud-basierten Tests erstellen, können aufgrund von Unterschieden zwischen Ihrer lokalen Umgebung und der bereitgestellten Umgebung Probleme auftreten. Ihr kontinuierlicher Integrationsprozess muss Tests anhand einer Reihe von Ressourcen durchführen, die in der Cloud bereitgestellt werden, bevor Ihr Code in die nächste Bereitstellungsumgebung wie QA, Staging oder Produktion übertragen wird.

Lesen Sie diesen kurzen Leitfaden weiter, um weitere Informationen zu Teststrategien für Serverless-Anwendungen zu erhalten, oder besuchen Sie das Serverless Test Samples Repository, um praktische Beispiele zu finden, die sich speziell auf die gewählte Sprache und Laufzeit beziehen.



Für Serverless-Tests schreiben Sie weiterhin Einheiten-, Integrations- und End-to-End-Tests.

- Einheitentests — Tests, die an einem isolierten Codeblock ausgeführt werden. Zum Beispiel die Überprüfung der Geschäftslogik zur Berechnung der Bereitstellungskosten für einen bestimmten Artikel und Bestimmungsort.

- Integrationstests — Tests, an denen zwei oder mehr Komponenten oder Dienste beteiligt sind, die interagieren, in der Regel in einer Cloud-Umgebung. Bei der Überprüfung einer Funktion werden beispielsweise Ereignisse aus einer Warteschlange verarbeitet.
- nd-to-end E-Tests — Tests, die das Verhalten einer gesamten Anwendung überprüfen. Stellen Sie beispielsweise sicher, dass die Infrastruktur korrekt eingerichtet ist und die Ereignisse zwischen den Services wie erwartet ablaufen, um die Bestellungen der Kunden aufzuzeichnen.

Gezielte Geschäftsergebnisse

Beim Testen von Serverless-Lösungen kann das Einrichten von Tests, die ereignisgesteuerte Interaktionen zwischen Services überprüfen, etwas mehr Zeit in Anspruch nehmen. Denken Sie beim Lesen dieses Leitfadens an die folgenden praktischen Geschäftsgründe:

- Erhöhen Sie die Qualität Ihrer Anwendung
- Verkürzen Sie die Zeit für das Entwickeln von Features und das Beheben von Fehlern

Die Qualität einer Anwendung hängt davon ab, ob zur Überprüfung der Funktionalität verschiedene Szenarien getestet werden. Durch sorgfältiges Abwägen der Geschäftsszenarien und die Automatisierung dieser Tests für die Ausführung mit Cloud-Services lässt sich die Qualität Ihrer Anwendung erhöhen.

Softwarefehler und Konfigurationsprobleme haben die geringsten Auswirkungen auf Kosten und Zeitplan, wenn sie während eines iterativen Entwicklungszyklus entdeckt werden. Wenn Probleme während der Entwicklung unentdeckt bleiben, erfordert das Erkennen und Beheben in der Produktion mehr Aufwand durch mehr Mitarbeiter.

Eine gut geplante Serverless-Teststrategie erhöht die Softwarequalität und verbessert die Iterationszeit, indem überprüft wird, dass Ihre Lambda-Funktionen und -Anwendungen in einer Cloud-Umgebung wie erwartet funktionieren.

Was muss getestet werden?

Wir empfehlen, eine Teststrategie anzuwenden, die das Verhalten der verwalteten Services, die Cloud-Konfiguration, Sicherheitsrichtlinien und die Integration in Ihren Code testet, um die Softwarequalität zu verbessern. Verhaltenstests, auch Blackbox-Tests genannt, verifizieren, dass ein System wie erwartet funktioniert, ohne dass alle internen Daten bekannt sind.

- Führen Sie Einheitentests durch, um die Geschäftslogik innerhalb der Lambda-Funktionen zu überprüfen.
- Stellen Sie sicher, dass die integrierten Services tatsächlich aufgerufen werden und die Eingabeparameter korrekt sind.
- Prüfen Sie, ob ein Ereignis alle erwarteten Dienste end-to-end in einem Workflow durchläuft.

In der traditionellen serverbasierten Architektur definieren Teams häufig einen Testumfang, der nur den Code umfasst, der auf dem Anwendungsserver ausgeführt wird. Andere Komponenten, Services oder Abhängigkeiten werden oft als extern betrachtet und liegen außerhalb des Testbereichs.

Serverless-Anwendungen bestehen oft aus kleinen Arbeitseinheiten, wie z. B. Lambda-Funktionen, die Produkte aus einer Datenbank abrufen oder Elemente aus einer Warteschlange verarbeiten oder die Größe eines Image im Speicher ändern. Jede Komponente läuft in ihrer eigenen Umgebung. Teams werden wahrscheinlich für viele dieser kleinen Einheiten innerhalb einer einzigen Anwendung zuständig sein.

Einige Anwendungsfunktionen können vollständig an verwaltete Services wie Amazon S3 delegiert oder ohne Verwendung von intern entwickeltem Code erstellt werden. Das Testen dieser verwalteten Services ist nicht erforderlich. Jedoch müssen Sie die Integration in diese Services testen.

So wird Serverless getestet

Wahrscheinlich sind Sie mit dem Testen lokal bereitgestellter Anwendungen vertraut: Sie schreiben Tests, die gegen Code laufen, der ausschließlich auf Ihrem Desktop-Betriebssystem oder in Containern ausgeführt wird. Beispielsweise können Sie eine lokale Web-Service-Komponente mit einer Anfrage aufrufen und dann Assertionen über die Antwort erstellen.

Serverless-Lösungen werden aus Ihrem Funktionscode und cloudbasierten verwalteten Services wie Warteschlangen, Datenbanken, Ereignisbussen und Messaging-Systemen erstellt. Diese Komponenten sind alle durch eine ereignisgesteuerte Architektur miteinander verbunden, in der Nachrichten, sogenannte Ereignisse, von einer Ressource zur anderen fließen. Diese Interaktionen können synchron sein, z. B. wenn ein Webdienst sofort Ergebnisse zurückgibt, oder eine asynchrone Aktion, die zu einem späteren Zeitpunkt abgeschlossen wird, z. B. das Platzieren von Elementen in eine Warteschlange oder das Starten eines Workflow-Schritts. Ihre Teststrategie muss beide Szenarien beinhalten und die Interaktionen zwischen den Services testen. Bei asynchronen Interaktionen müssen Sie möglicherweise Nebenwirkungen in nachgeschalteten Komponenten erkennen, die möglicherweise nicht sofort beobachtbar sind.

Die Replikation einer gesamten Cloud-Umgebung, einschließlich Warteschlangen, Datenbanktabellen, Ereignisbussen, Sicherheitsrichtlinien und mehr, ist nicht praktikabel. Aufgrund der Unterschiede zwischen Ihrer lokalen Umgebung und Ihren bereitgestellten Umgebungen in der Cloud werden Sie unweigerlich auf Probleme stoßen. Die Unterschiede zwischen Ihren Umgebungen verlängern die Zeit für die Reproduktion und das Beheben von Fehlern.

Bei Serverless-Anwendungen befinden sich die Architekturkomponenten in der Regel vollständig in der Cloud, sodass Tests mit Code und Services in der Cloud notwendig sind, um Features zu entwickeln und Fehler zu beheben.

Testmethoden

In der Realität wird Ihre Teststrategie wahrscheinlich eine Mischung von Techniken beinhalten, um die Qualität Ihrer Lösungen zu erhöhen. Sie werden schnelle interaktive Tests verwenden, um Funktionen in der Konsole zu debuggen, automatisierte Einheitentests, um isolierte Geschäftslogik zu überprüfen, Verifizierung von Aufrufen externer Services mit Mocks und gelegentliche Tests gegen Emulatoren, die einen Service imitieren.

- Testen in der Cloud — Sie stellen Infrastruktur und Code bereit, um mit tatsächlichen Services, Sicherheitsrichtlinien, Konfigurationen und infrastrukturspezifischen Parametern zu testen. Cloud-basierte Tests bieten das genaueste Maß für die Qualität Ihres Codes.

  Das Debuggen einer Funktion in der Konsole ist eine schnelle Möglichkeit, in der Cloud zu testen. Sie können aus einer Bibliothek mit Beispieltestereignissen wählen oder ein benutzerdefiniertes Ereignis erstellen, um eine Funktion isoliert zu testen. Sie können die Testereignisse auch über die Konsole mit Ihrem Team teilen.

  Um das Testen während des Entwicklungs- und Build-Lebenszyklus zu automatisieren, müssen Sie außerhalb der Konsole testen. In den Abschnitten zum sprachspezifischen Testen in diesem Handbuch finden Sie Automatisierungsstrategien und Ressourcen.
- Testen mit Mocks (auch Fakes genannt) — Mocks sind Objekte in Ihrem Code, die einen externen Dienst simulieren und diesen repräsentieren. Mocks bieten vordefiniertes Verhalten zur Überprüfung von Service-Aufrufen und Parametern. Ein Fake ist eine Scheinimplementierung, die Abkürzungen verwendet, um die Leistung zu vereinfachen oder zu verbessern. Beispielsweise könnte ein gefälschtes Datenzugriffsobjekt Daten aus einem In-Memory-Datenspeicher zurückgeben. Mocks können komplexe Abhängigkeiten nachahmen und vereinfachen, können aber auch zu weiteren Mocks führen, um verschachtelte Abhängigkeiten zu ersetzen.
- Testen mit Emulatoren — Sie können Anwendungen (manchmal von Drittanbietern) einrichten, um einen Cloud-Dienst in Ihrer lokalen Umgebung nachzuahmen. Geschwindigkeit ist ihre Stärke,

aber die Einrichtung und die Parität mit Produktions-Services ist ihre Schwäche. Verwenden Sie Emulatoren sparsam.

Testen in der Cloud

Das Testen in der Cloud ist für alle Testphasen nützlich, einschließlich Unit-Tests, Integrationstests und end-to-end Tests. Wenn Sie Tests mit cloud-basiertem Code durchführen, der auch mit cloud-basierten Diensten interagiert, erhalten Sie das genaueste Maß für die Qualität Ihres Codes.

Eine bequeme Möglichkeit, eine Lambda-Funktion in der Cloud auszuführen, ist ein Testereignis in der AWS Management Console. Ein Testereignis ist eine JSON-Eingabe für Ihre Funktion. Wenn Ihre Funktion keine Eingabe erfordert, kann das Ereignis ein leeres JSON-Dokument (`{}`) sein. Die Konsole bietet Beispielereignisse für eine Vielzahl von Service-Integrationen. Nachdem Sie ein Ereignis in der Konsole erstellt haben, können Sie es auch mit Ihrem Team teilen, um das Testen einfacher und einheitlicher zu gestalten.

Erfahren Sie, wie Sie eine Beispielfunktion in der Konsole debuggen.

> **Note**
>
> Obwohl das Ausführen von Funktionen in der Konsole eine schnelle Möglichkeit zum Debuggen ist, ist die Automatisierung Ihrer Testzyklen unerlässlich, um die Anwendungsqualität und die Entwicklungsgeschwindigkeit zu erhöhen.

Beispiele für die Testautomatisierung sind im Serverless Test Samples Repository verfügbar. Mit der folgenden Befehlszeile wird ein Beispiel für einen Python-Integrationstest automatisch ausgeführt:

```
python -m pytest -s tests/integration -v
```

Obwohl der Test lokal ausgeführt wird, interagiert er mit cloud-basierten Ressourcen. Diese Ressourcen wurden mithilfe des AWS SAM Befehlszeilentools AWS Serverless Application Model und bereitgestellt. Der Testcode ruft zunächst die bereitgestellten Stack-Ausgaben ab, zu denen der API-Endpunkt, die Funktions-ARN und die Sicherheitsrolle gehören. Als Nächstes sendet der Test eine Anfrage an den API-Endpunkt, der mit einer Liste von Amazon-S3-Buckets antwortet. Dieser Test wird ausschließlich mit cloud-basierten Ressourcen ausgeführt, um sicherzustellen, dass diese Ressourcen bereitgestellt und gesichert sind und wie erwartet funktionieren.

```
========================= test session starts ==========================
```

```
      platform darwin -- Python 3.10.10, pytest-7.3.1, pluggy-1.0.0
      -- /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-lambda/
venv/bin/python
      cachedir: .pytest_cache
      rootdir: /Users/t/code/aws/serverless-test-samples/python-test-samples/apigw-
lambda
      plugins: mock-3.10.0
      collected 1 item


      tests/integration/test_api_gateway.py::TestApiGateway::test_api_gateway

      --> Stack outputs:

        HelloWorldApi
        = https://p7teqs3162.execute-api.us-west-2.amazonaws.com/Prod/hello/
        > API Gateway endpoint URL for Prod stage for Hello World function

        PythonTestDemo
        = arn:aws:lambda:us-west-2:1234567890:function:testing-apigw-lambda-
PythonTestDemo-iSij8evaTdxl
        > Hello World Lambda Function ARN

        PythonTestDemoIamRole
        = arn:aws:iam::1234567890:role/testing-apigw-lambda-PythonTestDemoRole-
IZELQQ9MG4HQ
        > Implicit IAM Role created for Hello World function

      --> Found API endpoint for "testing-apigw-lambda" stack...
      --> https://p7teqs3162.execute-api.us-west-2.amazonaws.com/Prod/hello/
      API Gateway response:
      amplify-dev-123456789-deployment|myapp-prod-p-loggingbucket-123456|s3-java-
bucket-123456789
      PASSED

      ========================= 1 passed in 1.53s =========================
```

Für die Entwicklung cloudnativer Anwendungen bietet das Testen in der Cloud die folgenden Vorteile:

- Sie können jeden verfügbaren Service testen.
- Sie verwenden immer die neuesten Service-APIs und Rückgabewerte.
- Eine Cloud-Testumgebung ähnelt stark Ihrer Produktionsumgebung.

- Tests können Sicherheitsrichtlinien, Service Quotas, Konfigurationen und infrastrukturspezifische Parameter umfassen.
- Jeder Entwickler kann schnell eine oder mehrere Testumgebungen in der Cloud erstellen.
- Cloud-Tests erhöhen die Sicherheit, dass Ihr Code in der Produktion korrekt ausgeführt wird.

Das Testen in der Cloud hat einige Nachteile. Der offensichtlichste Nachteil von Tests in der Cloud ist, dass Bereitstellungen in Cloud-Umgebungen in der Regel länger dauern als Bereitstellungen in lokalen Desktop-Umgebungen.

Zum Glück reduzieren Tools wie AWS Serverless Application Model (AWS SAM) Accelerate, AWS Cloud Development Kit (AWS CDK) Watch Mode und SST (3rd Party) die Latenz, die mit Iterationen der Cloud-Implementierung einhergeht. Diese Tools können Ihre Infrastruktur und Ihren Code überwachen und inkrementelle Updates in Ihrer Cloud-Umgebung automatisch bereitstellen.

> **Note**
>
> Erfahren Sie im Serverless Developer Guide, wie Sie Infrastruktur als Code erstellen, um mehr über AWS Serverless Application Model, und zu erfahren. AWS CloudFormation AWS Cloud Development Kit (AWS CDK)

Im Gegensatz zu lokalen Tests sind beim Testen in der Cloud weitere Ressourcen erforderlich, wodurch Servicekosten entstehen können. Die Einrichtung isolierter Testumgebungen kann die Belastung Ihrer DevOps Teams erhöhen, insbesondere in Organisationen mit strengen Kontrollen in Bezug auf Konten und Infrastruktur. Bei der Arbeit mit komplexen Infrastrukturszenarien können die Kosten für die Einrichtung und Pflege einer komplizierten lokalen Umgebung jedoch ähnlich hoch sein wie bei der Verwendung von Einweg-Testumgebungen, die mit Automatisierungstools für Infrastruktur in Form von Code erstellt werden (oder sogar höher).

Tests in der Cloud sind trotz dieser Überlegungen immer noch der beste Weg, um die Qualität Ihrer Serverless-Lösungen zu gewährleisten.

Testen mit Mocks

Das Testen mit Mocks ist eine Technik, bei der Sie Ersatzobjekte in Ihrem Code erstellen, um das Verhalten eines Cloud-Services zu simulieren.

Sie könnten beispielsweise einen Test schreiben, der ein Modell des Amazon S3-Service verwendet, der bei jedem Aufruf der CreateObjectMethode eine bestimmte Antwort zurückgibt. Wenn ein Test

ausgeführt wird, gibt der Mock die programmierte Antwort zurück, ohne Amazon S3 oder andere Service-Endpunkte aufzurufen.

Mock-Objekte werden oft von einem Mock-Framework generiert, um den Entwicklungsaufwand zu reduzieren. Einige Mock-Frameworks sind generisch und andere wurden speziell für AWS SDKs entwickelt, wie Moto, eine Python-Bibliothek zum Mocken von AWS Diensten und Ressourcen.

Mock-Objekte unterscheiden sich von Emulatoren dadurch, dass Mocks in der Regel von einem Entwickler als Teil des Testcodes erstellt oder konfiguriert werden, wohingegen Emulatoren eigenständige Anwendungen sind, die die Funktionalität auf dieselbe Weise wie die Systeme, die sie emulieren, offenlegen.

Die Verwendung von Mocks bietet folgende Vorteile:

- Mocks können Dienste von Drittanbietern simulieren, die sich der Kontrolle Ihrer Anwendung entziehen, wie APIs und Software-as-a-Service (SaaS)-Anbieter, ohne dass ein direkter Zugriff auf diese Dienste erforderlich ist.
- Mocks sind nützlich für das Testen von Fehlerbedingungen, insbesondere wenn solche Bedingungen schwer zu simulieren sind, wie z. B. ein Service-Ausfall.
- Mocks können nach der Konfiguration schnelle lokale Tests ermöglichen.
- Mocks können Ersatzverhalten für praktisch jede Art von Objekt bereitstellen, so dass Mocking-Strategien eine breitere Palette von Diensten abdecken können als Emulatoren.
- Wenn neue Features oder Verhaltensweisen verfügbar werden, können Mock-Tests schneller reagieren. Durch die Verwendung eines generischen Mock-Frameworks können Sie neue Funktionen simulieren, sobald das aktualisierte AWS SDK verfügbar ist.

Mock-Tests haben die folgenden Nachteile:

- Mocks erfordern in der Regel einen nicht unerheblichen Einrichtungs- und Konfigurationsaufwand, insbesondere dann, wenn versucht wird, Rückgabewerte von verschiedenen Services zu ermitteln, um die Antworten korrekt nachzuahmen.
- Mocks werden von Entwicklern geschrieben, konfiguriert und müssen von ihnen gewartet werden, was ihre Verantwortung erhöht.
- Möglicherweise benötigen Sie Zugriff auf die Cloud, um die APIs und Rückgabewerte von Diensten zu verstehen.
- Mocks können schwierig zu warten sein. Wenn sich die Signaturen der nachgebildeten Cloud-APIs ändern oder die Rückgabewertschemata weiterentwickelt werden, müssen Sie Ihre Mocks

aktualisieren. Mocks erfordern auch Updates, wenn Sie Ihre Anwendungslogik erweitern, um Aufrufe an neue APIs zu tätigen.
- Tests, die Mocks verwenden, können in Desktop-Umgebungen erfolgreich sein, in der Cloud jedoch fehlschlagen. Die Ergebnisse stimmen möglicherweise nicht mit der aktuellen API überein. Die Servicekonfiguration und die Kontingente können nicht getestet werden.
- Schein-Frameworks können Richtlinien oder Kontingentbeschränkungen für AWS Identity and Access Management (IAM) nur begrenzt testen oder erkennen. Mocks können zwar besser simulieren, wenn die Autorisierung fehlschlägt oder ein Kontingent überschritten wird, aber Tests können nicht bestimmen, welches Ergebnis in einer Produktionsumgebung tatsächlich eintreten wird.

Testen mit Emulation

Emulatoren sind in der Regel eine lokal ausgeführte Anwendung, die einen Produktionsdienst nachahmt. AWS

Emulatoren verfügen über APIs, die ihren Cloud-Gegenstücken ähneln und ähnliche Rückgabewerte bereitstellen. Sie können auch Zustandsänderungen simulieren, die durch API-Aufrufe initiiert werden. Sie können beispielsweise eine Funktion mit AWS SAM local ausführen, AWS SAM um den Lambda-Dienst zu emulieren, sodass Sie schnell eine Funktion aufrufen können. Genauere Informationen finden Sie im AWS Serverless Application Model Entwicklerhandbuch unter AWS SAM lokal.

Tests mit Emulatoren bieten unter anderem folgende Vorteile:

- Emulatoren können schnelle lokale Entwicklungsiterationen und Tests ermöglichen.
- Emulatoren bieten Entwicklern, die es gewohnt sind, Code in einer lokalen Umgebung zu entwickeln, eine vertraute Umgebung. Wenn Sie beispielsweise mit der Entwicklung einer n-Tier-Anwendung sind, verfügen Sie möglicherweise über einen Datenbank-Engine und einen Webserver, ähnlich denen, die in der Produktion laufen, auf Ihrem lokalen Rechner, um schnelle, lokale, isolierte Testfunktionen bereitzustellen.
- Emulatoren erfordern keine Änderungen an der Cloud-Infrastruktur (z. B. Cloud-Konten für Entwickler), sodass sie einfach mit vorhandenen Testmustern implementiert werden können.

Das Testen mit Emulatoren hat folgende Nachteile:

- Emulatoren können schwierig einzurichten und zu replizieren sein, insbesondere wenn sie in CI/CD-Pipelines verwendet werden. Dies kann den Workload von IT-Mitarbeitern oder Entwicklern erhöhen, die ihre eigene Software verwalten.
- Emulierte Features und APIs hinken in der Regel den Service-Updates hinterher. Dies kann zu Fehlern führen, da der getestete Code nicht mit der tatsächlichen API übereinstimmt, und die Einführung neuer Features behindern.
- Emulatoren benötigen Unterstützung, Updates, Bugfixes und Verbesserungen der Featureparität. Diese liegen in der Verantwortung des Emulatorautors, bei dem es sich um ein Drittunternehmen handeln kann.
- Tests, die auf Emulatoren basieren, können lokal zu erfolgreichen Ergebnissen führen, schlagen in der Cloud jedoch aufgrund von Produktionssicherheitsrichtlinien, dienstübergreifenden Konfigurationen oder der Überschreitung von Lambda-Kontingenten fehl.
- Für viele AWS Dienste sind keine Emulatoren verfügbar. Wenn Sie sich auf Emulation verlassen, steht Ihnen möglicherweise keine zufriedenstellende Testoption für Teile Ihrer Anwendung zur Verfügung.

Bewährte Methoden

Die folgenden Abschnitte enthalten Empfehlungen für erfolgreiche Tests für Serverless-Anwendungen.

Praktische Beispiele für Tests und Testautomatisierung finden Sie im Serverless Test Samples Repository.

Priorisieren Sie Tests in der Cloud

Tests in der Cloud bieten die zuverlässigste, genaueste und vollständigste Testabdeckung. Durch die Durchführung von Tests im Kontext der Cloud werden nicht nur die Geschäftslogik, sondern auch Sicherheitsrichtlinien, Service-Konfigurationen, Kontingente und die aktuellsten API-Signaturen und Rückgabewerte umfassend getestet.

Strukturieren Sie Ihren Code zum Testen

Vereinfachen Sie Ihre Tests und Lambda-Funktionen, indem Sie Lambda-spezifischen Code von Ihrer Kerngeschäftslogik trennen.

Ihr Lambda-Funktions-Handler sollte ein schlanker Adapter sein, der Ereignisdaten aufnimmt und nur die Details an Ihre Geschäftslogikmethode(n) weiterleitet. Mit dieser Strategie können Sie

umfassende Tests rund um Ihre Geschäftslogik durchführen, ohne sich über Lambda-spezifische Details Gedanken machen zu müssen. Ihre AWS Lambda-Funktionen sollten nicht die Einrichtung einer komplexen Umgebung oder einer großen Anzahl von Abhängigkeiten erfordern, um die zu testende Komponente zu erstellen und zu initialisieren.

Im Allgemeinen sollten Sie einen Handler schreiben, der Daten aus den eingehenden Ereignis- und Kontext-Objekten extrahiert und validiert und diese Eingabe dann an Methoden sendet, die Ihre Geschäftslogik ausführen.

Entwicklungs-Feedback-Schleifen beschleunigen

Es gibt Tools und Techniken, um die Entwicklungs-Feedback-Schleifen zu beschleunigen. AWS SAM Accelerate und AWS CDK Watch Mode reduzieren beispielsweise beide die Zeit, die für die Aktualisierung von Cloud-Umgebungen benötigt wird.

In den Beispielen im GitHub Serverless Test Samples-Repository werden einige dieser Techniken untersucht.

Wir empfehlen außerdem, dass Sie Cloud-Ressourcen so früh wie möglich während der Entwicklung erstellen und testen — nicht erst, nachdem Sie sich bei der Quellverwaltung angemeldet haben. Diese Praxis ermöglicht ein schnelleres Erkunden und Experimentieren bei der Entwicklung von Lösungen. Darüber hinaus hilft Ihnen die Automatisierung der Bereitstellung von einem Entwicklungscomputer aus dabei, Probleme mit der Cloud-Konfiguration schneller zu erkennen und unnötigen Aufwand für Updates und Code-Review-Prozesse zu reduzieren.

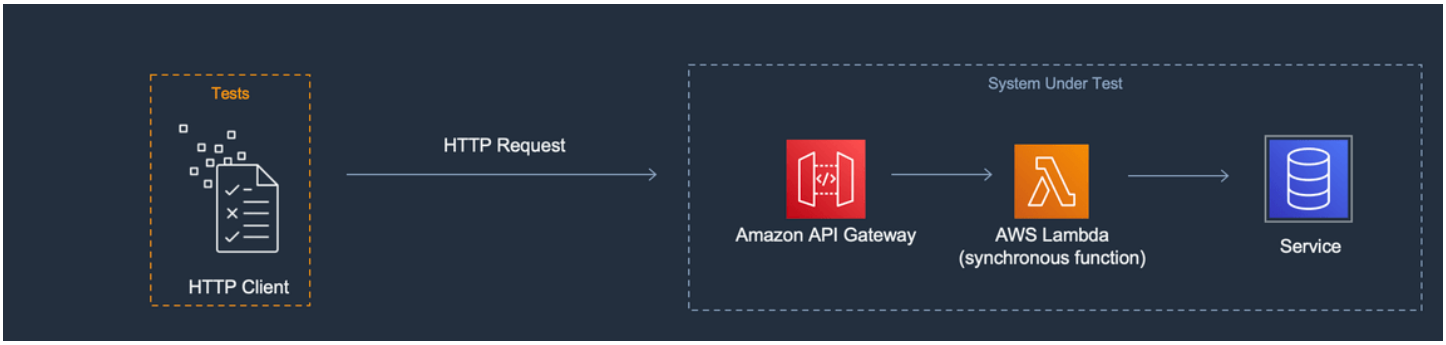
Fokus auf Integrationstests

Beim Erstellen von Anwendungen mit Lambda hat es sich bewährt, Komponenten gemeinsam zu testen.

Tests, die mit zwei oder mehr Architekturkomponenten ausgeführt werden, werden als Integrationstests bezeichnet. Das Ziel der Integrationstests besteht darin, nicht nur zu verstehen, wie Ihr Code komponentenübergreifend ausgeführt wird, sondern auch, wie sich die Umgebung, in der Ihr Code gehostet wird, verhält. nd-to-end E-Tests sind spezielle Arten von Integrationstests, mit denen das Verhalten einer gesamten Anwendung überprüft wird.

Um Integrationstests zu erstellen, stellen Sie Ihre Anwendung in einer Cloud-Umgebung bereit. Dies kann von einer lokalen Umgebung aus oder über eine CI/CD-Pipeline erfolgen. Schreiben Sie dann Tests, um das zu testende System (SUT) zu testen und das erwartete Verhalten zu validieren.

Das zu testende System könnte beispielsweise eine Anwendung sein, die API Gateway, Lambda und DynamoDB verwendet. Ein Test könnte einen synthetischen HTTP-Aufruf an einen API-Gateway-Endpunkt ausführen und überprüfen, ob die Antwort die erwartete Nutzlast enthielt. Dieser Test bestätigt, dass der AWS Lambda-Code korrekt ist und dass jeder Dienst korrekt konfiguriert ist, um die Anfrage zu verarbeiten, einschließlich der IAM-Berechtigungen zwischen ihnen. Darüber hinaus könnten Sie den Test so gestalten, dass Datensätze unterschiedlicher Größe geschrieben werden, um zu überprüfen, ob Ihre Service-Kontingente, wie z. B. die maximale Datensatzgröße in DynamoDB, korrekt eingerichtet sind.



Erstellen Sie isolierte Testumgebungen

Tests in der Cloud erfordern in der Regel isolierte Entwicklerumgebungen, sodass sich Tests, Daten und Ereignisse nicht überschneiden.

Ein Ansatz besteht darin, jedem Entwickler ein eigenes Konto zur Verfügung zu stellen. AWS Dadurch werden Konflikte mit der Ressourcenbenennung vermieden, die auftreten können, wenn mehrere Entwickler in einer gemeinsamen Codebasis arbeiten, versuchen, Ressourcen bereitzustellen oder eine API aufzurufen.

Automatisierte Testprozesse sollten für jeden Stapel eindeutig benannte Ressourcen erstellen. Sie können beispielsweise Skripts oder TOML-Konfigurationsdateien so einrichten, dass die AWS SAM CLI sam deploy - oder sam sync-Befehle automatisch einen Stack mit einem eindeutigen Präfix angeben.

In einigen Fällen teilen sich Entwickler ein AWS Konto. Dies kann daran liegen, dass in Ihrem Stack Ressourcen vorhanden sind, deren Betrieb oder Bereitstellung und Konfiguration teuer sind. Beispielsweise kann eine Datenbank gemeinsam genutzt werden, um die korrekte Einrichtung und Bereitstellung der Daten zu vereinfachen.

Wenn Entwickler ein Konto gemeinsam nutzen, müssen Sie Grenzen festlegen, um die Inhaberschaft zu ermitteln und Überschneidungen zu vermeiden. Eine Möglichkeit, dies zu tun, besteht darin,

den Stack-Namen die Benutzer-IDs der Entwickler voranzustellen. Ein weiterer beliebter Ansatz ist das Einrichten von Stacks, die auf Code-Branches basieren. Aufgrund der Filialgrenzen sind die Umgebungen isoliert, aber Entwickler können dennoch Ressourcen gemeinsam nutzen, z. B. eine relationale Datenbank. Dieser Ansatz ist eine bewährte Methode, wenn Entwickler an mehr als einer Verzweigung gleichzeitig arbeiten.

Das Testen in der Cloud ist für alle Testphasen wertvoll, einschließlich Unit-Tests, Integrationstests und end-to-end Tests. Das Aufrechterhalten einer ordnungsgemäßen Isolierung ist von entscheidender Bedeutung. Dennoch sollten Sie darauf achten, dass Ihre QA-Umgebung der Produktionsumgebung so nahe wie möglich kommt. Aus diesem Grund fügen Teams den QA-Umgebungen Änderungssteuerungsvorgänge hinzu.

In Vorproduktions- und Produktionsumgebungen werden die Grenzen in der Regel auf Kontoebene gezogen, um Arbeitslasten von „Noisy-Neighbor“-Problemen zu isolieren und Sicherheitskontrollen mit geringsten Berechtigungen zum Schutz sensibler Daten zu implementieren. Für Workloads gibt es Kontingente. Ihre Tests dürfen weder die für die Produktion zugewiesenen Kontingente verbrauchen („Noisy Neighbor“) noch Zugriff auf Kundendaten haben. Lasttests sind eine weitere Aktivität, die Sie von Ihrem Produktions-Stack isolieren sollten.

In jedem Fall müssen die Umgebungen mit Warnungen und Kontrollen konfiguriert werden, um unnötige Ausgaben zu vermeiden. Sie können beispielsweise die Art, Stufe oder Größe der Ressourcen einschränken, die erstellt werden können, und E-Mail-Benachrichtigungen einrichten, wenn die geschätzten Kosten einen bestimmten Schwellenwert überschreiten.

Mocks für isolierte Geschäftslogik verwenden

Mock-Frameworks sind ein wertvolles Tool zum Schreiben schneller Einheitentests. Sie sind besonders nützlich, wenn Tests komplexe interne Geschäftslogiken wie mathematische oder finanzielle Berechnungen oder Simulationen abdecken. Suchen Sie nach Einheitentests, die eine große Anzahl von Testfällen oder Eingabevariationen enthalten, bei denen diese Eingaben das Muster oder den Inhalt von Aufrufen an andere Cloud-Services nicht ändern.

Code, der durch Komponententests mit Mocks abgedeckt wird, muss auch durch Tests in der Cloud abgedeckt werden. Dies wird empfohlen, da ein Entwickler-Laptop oder eine Build-Machine-Umgebung anders konfiguriert werden kann als eine Produktionsumgebung in der Cloud. Beispielsweise beanspruchen Ihre Lambda-Funktionen möglicherweise mehr Speicher oder Zeit als zugewiesen, wenn sie mit bestimmten Eingabeparametern ausgeführt werden. Möglicherweise enthält Ihr Code auch Umgebungsvariablen, die nicht auf die gleiche Weise (oder überhaupt nicht)

konfiguriert sind, und die Unterschiede könnten dazu führen, dass sich der Code anders verhält oder fehlschlägt.

Der Nutzen von Mocks ist bei Integrationstests geringer, da der Aufwand für die Implementierung der notwendigen Mocks mit der Anzahl der Verbindungspunkte steigt. Beim nd-to-end Testen von E sollten keine Mocks verwendet werden, da sich diese Tests im Allgemeinen mit Zuständen und komplexer Logik befassen, die mit Mock-Frameworks nicht einfach simuliert werden können.

Vermeiden Sie schließlich die Verwendung von nachgebildeten Cloud-Services, um die ordnungsgemäße Implementierung von Service-Aufrufen zu überprüfen. Führen Sie stattdessen Cloud-Service-Aufrufe in der Cloud durch, um Verhalten, Konfiguration und funktionale Implementierung zu überprüfen.

Emulatoren sparsam verwenden

Emulatoren können für einige Anwendungsfälle praktisch sein, z. B. für ein Entwicklungsteam mit begrenztem, unzuverlässigem oder langsamem Internetzugang. In den meisten Fällen sollten Sie Emulatoren jedoch sparsam verwenden.

Indem Sie Emulatoren vermeiden, können Sie die neuesten Servicefeatures und aktuellen APIs entwickeln und Innovationen mit ihnen umsetzen. Sie werden nicht auf die Veröffentlichung von Anbietern warten müssen, um die Featureparität zu erreichen. Sie reduzieren Ihre Vorabkosten und laufenden Kosten für den Kauf und die Konfiguration mehrerer Entwicklungssysteme und bauen Maschinen. Darüber hinaus vermeiden Sie das Problem, dass bei vielen Cloud-Services einfach keine Emulatoren verfügbar sind. Eine Teststrategie, die auf Emulation basiert, macht es unmöglich, diese Services zu nutzen (was zu potenziell teureren Problemumgehungen führt) oder Code und Konfigurationen zu erstellen, die nicht gut getestet wurden.

Wenn Sie die Emulation zum Testen verwenden, müssen Sie dennoch in der Cloud testen, um die Konfiguration zu überprüfen und Interaktionen mit Cloud-Diensten zu testen, die in einer emulierten Umgebung nur simuliert oder nachgeahmt werden können.

Herausforderungen beim Testen vor Ort

Wenn Sie Emulatoren und simulierte Aufrufe verwenden, um auf Ihrem lokalen Desktop zu testen, können Testinkonsistenzen auftreten, wenn Ihr Code in Ihrer CI/CD-Pipeline von Umgebung zu Umgebung fortschreitet. Einheitentests zur Validierung der Geschäftslogik Ihrer Anwendung auf Ihrem Desktop testen möglicherweise wichtige Aspekte der Cloud-Services nicht genau.

Die folgenden Beispiele zeigen, worauf beim lokalen Testen mit Mocks und Emulatoren zu achten ist:

Beispiel: Die Lambda-Funktion erstellt einen S3-Bucket

Wenn die Logik einer Lambda-Funktion von der Erstellung eines S3-Buckets abhängt, sollte ein vollständiger Test bestätigen, dass Amazon S3 aufgerufen und der Bucket erfolgreich erstellt wurde.

- In einem Test-Setup können Sie eine Erfolgsreaktion simulieren und möglicherweise einen Testfall hinzufügen, um eine Fehlerreaktion zu behandeln.
- In einem Emulationstestszenario kann die CreateBucketAPI aufgerufen werden, aber Sie müssen sich bewusst sein, dass die Identität, die den lokalen Aufruf durchführt, nicht vom Lambda-Dienst stammt. Die Anrufindentität übernimmt keine Sicherheitsrolle wie in der Cloud. Daher wird stattdessen eine Platzhalterauthentifizierung verwendet, möglicherweise mit einer permissiveren Rolle oder Benutzeridentität, die bei Ausführung in der Cloud anders sein wird.

Die Mock- und Emulations-Setups testen, was die Lambda-Funktion tut, wenn sie Amazon S3 aufruft. Diese Tests überprüfen jedoch nicht, ob die Lambda-Funktion, wie konfiguriert, in der Lage ist, den Amazon-S3-Bucket erfolgreich zu erstellen. Sie müssen sicherstellen, dass der Rolle, die der Funktion zugewiesen ist, eine Sicherheitsrichtlinie angehängt ist, die es der Funktion ermöglicht, die `s3:CreateBucket`-Aktion auszuführen. Andernfalls schlägt die Funktion wahrscheinlich fehl, wenn sie in einer Cloud-Umgebung bereitgestellt wird.

Beispiel: Verwenden Sie eine Lambda-Funktion, um Nachrichten aus einer Amazon-SQS-Warteschlange zu verarbeiten.

Wenn eine Amazon-SQS-Warteschlange die Quelle einer Lambda-Funktion ist, muss durch einen vollständigen Test überprüft werden, ob die Lambda-Funktion erfolgreich aufgerufen wird, wenn eine Nachricht in eine Warteschlange gestellt wird.

Emulationstests und Mock-Tests werden in der Regel so eingerichtet, dass der Lambda-Funktionscode direkt ausgeführt wird und die Amazon-SQS-Integration simuliert wird, indem eine JSON-Event-Payload (oder ein deserialisiertes Objekt) als Eingabe des Funktions-Handlers übergeben wird.

Bei lokalen Tests, bei denen die Amazon-SQS-Integration simuliert wird, wird getestet, was die Lambda-Funktion tut, wenn sie von Amazon SQS mit einer bestimmten Nutzlast aufgerufen wird. Der Test bestätigt jedoch nicht, dass Amazon SQS die Lambda-Funktion erfolgreich aufruft, wenn sie in einer Cloud-Umgebung bereitgestellt wird.

Einige Beispiele für Konfigurationsprobleme, die bei Amazon SQS und Lambda auftreten können, sind die folgenden:

- Das Amazon-SQS-Sichtbarkeits-Timeout ist zu niedrig, was zu mehreren Aufrufen führt, obwohl nur einer vorgesehen war.
- Die Ausführungsrolle der Lambda-Funktion erlaubt es nicht, Nachrichten aus der Warteschlange zu lesen (durch `sqs:ReceiveMessage`,`sqs:DeleteMessage`, oder `sqs:GetQueueAttributes`).
- Das Beispielereignis, das an die Lambda-Funktion übergeben wird, überschreitet das Amazon-SQS-Nachrichtengrößenkontingent. Daher ist der Test ungültig, da Amazon SQS niemals in der Lage wäre, eine Nachricht dieser Größe zu senden.

Wie diese Beispiele zeigen, liefern Tests, die sich mit der Geschäftslogik, aber nicht mit den Konfigurationen zwischen Cloud-Services befassen, wahrscheinlich zu unzuverlässigen Ergebnissen.

Häufig gestellte Fragen

Ich habe eine Lambda-Funktion, die Berechnungen durchführt und ein Ergebnis zurückgibt, ohne andere Dienste aufzurufen. Muss ich es wirklich in der Cloud testen?

Ja. Lambda-Funktionen haben Konfigurationsparameter, die das Testergebnis verändern könnten. Der gesamte Lambda-Funktionscode ist von Timeout - und Speichereinstellungen abhängig, was dazu führen kann, dass die Funktion fehlschlägt, wenn diese Einstellungen nicht richtig eingestellt sind. Lambda-Richtlinien ermöglichen auch die Standardausgabeprotokollierung an Amazon CloudWatch. Auch wenn Ihr Code nicht CloudWatch direkt aufruft, ist eine Genehmigung erforderlich, um die Protokollierung zu aktivieren. Diese erforderliche Erlaubnis kann nicht korrekt verspottet oder nachgeahmt werden.

Wie können Tests in der Cloud beim Einheitentest helfen? Wenn es sich in der Cloud befindet und eine Verbindung zu anderen Ressourcen herstellt, ist das nicht ein Integrationstest?

Wir definieren Komponententests als Tests, die isoliert auf Architekturkomponenten ausgeführt werden. Dies hindert Tests jedoch nicht daran, Komponenten einzubeziehen, die möglicherweise andere Services aufrufen oder Netzwerkkommunikation nutzen.

Viele Serverless-Anwendungen verfügen über Architekturkomponenten, die isoliert getestet werden können, sogar in der Cloud. Ein Beispiel ist eine Lambda-Funktion, um Eingaben entgegenzunehmen, die Daten zu verarbeiten und eine Nachricht an eine Amazon-SQS-Warteschlange zu senden. Ein Komponententest dieser Funktion würde wahrscheinlich testen, ob Eingabewerte dazu führen, dass bestimmte Werte in der Nachricht in der Warteschlange vorhanden sind.

Stellen Sie sich einen Test vor, der nach dem Muster „Arrange, Act, Assert“ geschrieben wurde:

- Arrange: Zuweisung von Ressourcen (eine Warteschlange zum Empfang von Nachrichten und die zu testende Funktion).
- Act: Aufrufen der zu testenden Funktion.
- Assert: Abrufen der von der Funktion gesendeten Nachricht und Validieren der Ausgabe.

Ein Mock-Testansatz würde das Mocking der Warteschlange mit einem prozessinternen Mock-Objekt und das Erstellen einer prozessinternen Instance der Klasse oder des Moduls, das den Lambda-Funktionscode enthält, beinhalten. Während der Assert-Phase würde die Nachricht in der Warteschlange aus dem simulierten Objekt abgerufen.

Bei einem cloud-basierten Ansatz würde der Test eine Amazon-SQS-Warteschlange für die Testzwecke erstellen und die Lambda-Funktion mit Umgebungsvariablen bereitstellen, die so konfiguriert sind, dass sie die isolierte Amazon-SQS-Warteschlange als Ausgabeziel verwenden. Nach dem Ausführen der Lambda-Funktion würde der Test die Nachricht aus der Amazon-SQS-Warteschlange abrufen.

Der cloud-basierte Test würde denselben Code ausführen, dasselbe Verhalten bestätigen und die funktionale Korrektheit der Anwendung überprüfen. Er hätte jedoch den zusätzlichen Vorteil, dass die Einstellungen der Lambda-Funktion validiert werden könnten: die IAM-Rolle, die IAM-Richtlinien sowie die Timeout- und Speichereinstellungen der Funktion.

Nächste Schritte und Ressourcen

Verwenden Sie die folgenden Ressourcen, um weitere Informationen und praktische Testbeispiele zu erhalten.

Beispielimplementierungen

Das Serverless Test Samples Repository on GitHub enthält konkrete Beispiele für Tests, die den in diesem Handbuch beschriebenen Mustern und bewährten Methoden folgen. Das Repository enthält Beispielcode und Anleitungen zu den Mock-, Emulations- und Cloud-Testprozessen, die in den vorherigen Abschnitten beschrieben wurden. Verwenden Sie dieses Repository, um sich über die neuesten Anleitungen zu serverlosen Tests von zu informieren. AWS

Weitere Informationen

Besuchen Sie Serverless Land, um auf die neuesten Blogs, Videos und Schulungen für AWS serverlose Technologien zuzugreifen.

Es wird auch empfohlen, die folgenden AWS Blogbeiträge zu lesen:

- Beschleunigen Sie die serverlose Entwicklung mit AWS SAM Accelerate (AWS Blogbeitrag)
- Erhöhung der Entwicklungsgeschwindigkeit mit CDK Watch (Blogbeitrag)AWS
- Serviceintegrationen mit AWS Step Functions Local verspotten (Blogbeitrag)AWS
- Erste Schritte beim Testen serverloser Anwendungen (Blogbeitrag)AWS

Tools

- AWS SAM — Testen und Debuggen serverloser Anwendungen
- AWS SAM — Integration mit automatisierten Tests
- Lambda — Testen von Lambda-Funktionen mit Hilfe der Lambda-Konsole

Erstellen von Lambda-Funktionen mit Node.js

Sie können JavaScript Code mit Node.js in AWS Lambda ausführen. Lambda bietet Laufzeiten für Node.js, die Ihren Code ausführen, um Ereignisse zu verarbeiten. Ihr Code wird in einer Umgebung ausgeführt, die die Rolle AWS SDK for JavaScript, with credentials from a AWS Identity and Access Management (IAM) enthält, die Sie verwalten. Weitere Informationen zu den SDK-Versionen, die in den Laufzeiten von Node.js enthalten sind, finden Sie unter. the section called “SDK-Versionen, die Runtime enthalten”

Lambda unterstützt die folgenden Node.js-Laufzeiten.

Node.js

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Node.js 20	`nodejs20.x`	Amazon Linux 2023			
Node.js 18	`nodejs18.x`	Amazon Linux 2			
Node.js 16	`nodejs16.x`	Amazon Linux 2	12. Juni 2024	28. Februar 2025	31. März 2025

> **Note**
>
> Laufzeiten von Node.js 18 und höher verwenden AWS SDK für JavaScript v3. Um eine Funktion aus einer früheren Runtime zu migrieren, folgen Sie dem Migrations-Workshop unter GitHub. Weitere Informationen zum AWS SDK für JavaScript Version 3 finden Sie im Blogbeitrag Modular AWS SDK for JavaScript is now general available.

Erstellen einer Funktion Node.js.

1. Öffnen Sie die Lambda-Konsole.
2. Wählen Sie Funktion erstellen.

3. Konfigurieren Sie die folgenden Einstellungen:
   - Funktionsname: Geben Sie einen Namen für die Funktion ein.
   - Laufzeit: Wählen Sie Node.js 20.x aus.
4. Wählen Sie Funktion erstellen.
5. Um ein Testereignis zu konfigurieren, wählen Sie Test.
6. Geben Sie für Event name (Ereignisname) **`test`** ein.
7. Wählen Sie Änderungen speichern aus.
8. Wählen Sie Test, um die Funktion aufzurufen.

Die Konsole erstellt eine Lambda-Funktion mit einer einzigen Quelldatei mit dem Namen `index.js` oder `index.mjs`. Mit dem integrierten Code-Editor können Sie diese Datei bearbeiten und weitere Dateien hinzufügen. Klicken Sie auf Save (Speichern), um die Änderungen zu speichern. Um Ihren Code auszuführen, wählen Sie Test.

> **Note**
>
> Die Lambda-Konsole dient AWS Cloud9 dazu, eine integrierte Entwicklungsumgebung im Browser bereitzustellen. Sie können es auch verwenden AWS Cloud9 , um Lambda-Funktionen in Ihrer eigenen Umgebung zu entwickeln. Weitere Informationen finden Sie AWS Toolkit im AWS Cloud9 Benutzerhandbuch unter Arbeiten mit AWS Lambda Funktionen unter Verwendung von.

Die `index.js`- oder `index.mjs`-Datei exportiert eine Funktion mit dem Namen `handler`, die ein Ereignisobjekt und ein Kontext-Objekt übernimmt. Dies ist die Handler-Funktion, die bei einem Aufruf der Funktion von Lambda aufgerufen wird. Die Node.js-Funktionslaufzeit ruft Aufrufereignisse von Lambda ab und leitet sie an den Handler weiter. In der Konfiguration der Funktion lautet der Wert für den Handler `index.handler`.

Wenn Sie Ihren Funktionscode speichern, erstellt die Lambda-Konsole ein Bereitstellungspaket für das ZIP-Dateiarchiv. Wenn Sie Ihren Funktionscode außerhalb der Konsole (mit einer IDE) entwickeln, müssen Sie ein Bereitstellungspaket erstellen, um Ihren Code in die Lambda-Funktion hochzuladen.

> **Note**
>
> Um mit der Anwendungsentwicklung in Ihrer lokalen Umgebung zu beginnen, stellen Sie eine der Beispielanwendungen bereit, die im GitHub Repository dieses Handbuchs verfügbar sind.
>
> Lambda-Beispielanwendungen in Node.js
>
> - blank-nodejs — Eine Funktion von Node.js, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK zeigt. AWS
> - nodejs-apig – Eine Funktion mit einem öffentlichen API-Endpunkt, die ein Ereignis aus API Gateway verarbeitet und eine HTTP-Antwort zurückgibt.
> - efs-nodejs – Eine Funktion, die ein Amazon-EFS-Dateisystem in einer Amazon VPC nutzt. Dieses Beispiel umfasst eine VPC, ein Dateisystem, Bindungsbereitstellung-Ziele und einen Zugriffspunkt, der für die Verwendung mit Lambda konfiguriert ist.

Die Funktionslaufzeit übergibt neben dem Aufrufereignis ein Context-Objekt an den Handler. Das Context-Objekt enthält zusätzliche Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung. Weitere Informationen erhalten Sie über die Umgebungsvariablen.

Ihre Lambda-Funktion wird mit einer CloudWatch Logs-Protokollgruppe geliefert. Die Funktionslaufzeit sendet Details zu jedem Aufruf an CloudWatch Logs. Es leitet alle Protokolle weiter, die Ihre Funktion während des Aufrufs ausgibt. Wenn Ihre Funktion einen Fehler zurückgibt, formatiert Lambda den Fehler und gibt ihn an den Aufrufer zurück.

Themen

- Instrumentierung von Node.js Code in AWS Lambda

Initialisierung von Node.js

Node.js verfügt über ein eindeutiges Ereignisschleifenmodell, das bewirkt, dass sich das Initialisierungsverhalten von anderen Laufzeiten unterscheidet. Insbesondere verwendet Node.js ein nicht blockierendes I/O-Modell, das asynchrone Operationen unterstützt. Dieses Modell ermöglicht es Node.js, für die meisten Workloads effizient zu arbeiten. Wenn beispielsweise eine Node.js-Funktion einen Netzwerkaufruf durchführt, kann diese Anforderung als asynchrone Operation bezeichnet und in eine Callback-Warteschlange gestellt werden. Die Funktion verarbeitet möglicherweise andere Vorgänge innerhalb des Hauptaufruf-Batches, ohne blockiert zu werden, indem sie darauf wartet, dass der Netzwerkaufruf zurückgegeben wird. Sobald der Netzwerkaufruf abgeschlossen ist, wird sein Rückruf ausgeführt und dann aus der Rückrufwarteschlange entfernt.

Einige Initialisierungsaufgaben werden möglicherweise asynchron ausgeführt. Diese asynchronen Aufgaben garantieren nicht, dass sie die Ausführung vor einem Aufruf abschließen. Beispielsweise ist Code, der einen Netzwerkaufruf zum Abrufen eines Parameters aus dem AWS Parameterspeicher durchführt, möglicherweise nicht vollständig, wenn Lambda die Handler-Funktion ausführt. Infolgedessen kann die Variable während eines Aufrufs null sein. Um dies zu vermeiden, stellen Sie sicher, dass Variablen und anderer asynchroner Code vollständig initialisiert sind, bevor Sie mit der restlichen Kerngeschäftslogik der Funktion fortfahren.

Alternativ können Sie Ihren Funktionscode als ES-Modul bezeichnen, sodass Sie `await` auf der obersten Ebene der Datei außerhalb des Bereichs Ihres Funktionshandlers verwenden können. Wenn Sie `await` jedes `Promise` verwenden, wird der asynchrone Initialisierungscode vor den Handler-Aufrufen abgeschlossen, wodurch die Wirksamkeit der bereitgestellten Gleichzeitigkeit bei der Reduzierung der Kaltstart-Latenz maximiert wird. Weitere Informationen und ein Beispiel finden Sie unter Verwenden von Node.js-ES-Modulen und Erwarten auf oberster Ebene in AWS Lambda.

Designieren eines Funktionshandlers als ES-Modul

Standardmäßig behandelt Lambda Dateien mit dem `.js`-Suffix als CommonJS-Module. Optional können Sie Ihren Code als ES-Modul festlegen. Sie können dies auf zwei Arten tun: durch Angabe von `type` als `module` in der `package.json`-Datei der Funktion oder durch Verwendung der Dateinamenerweiterung `.mjs`. Im ersten Ansatz behandelt Ihr Funktionscode alle `.js`-Dateien als ES-Module, während im zweiten Szenario nur die Datei, die Sie mit `.mjs` angeben, ein ES-Modul ist. Sie können ES-Module und CommonJS-Module mischen, indem Sie sie als `.mjs` bzw. `.cjs`

benennen, da `.mjs`-Dateien immer ES-Module sind und `.cjs`-Dateien immer CommonJS-Module sind.

Lambda durchsucht beim Laden von ES-Modulen Ordner in der `NODE_PATH` Umgebungsvariablen. Sie können das AWS SDK, das in der Laufzeit enthalten ist, mithilfe von `import` ES-Modulanweisungen laden. Sie können ES-Module auch aus Ebenen laden.

SDK-Versionen, die Runtime enthalten

Die Version des AWS SDK, die in der Runtime von Node.js enthalten ist, hängt von der Runtime-Version und Ihrer ab. AWS-Region Um die Version des SDK zu finden, die in der von Ihnen verwendeten Runtime enthalten ist, erstellen Sie eine Lambda-Funktion mit dem folgenden Code.

> **Note**
>
> Der unten gezeigte Beispielcode für die Versionen 18 und höher von Node.js verwendet das CommonJS-Format. Wenn Sie die Funktion in der Lambda-Konsole erstellen, müssen Sie die Datei, die den Code enthält, unbedingt in umbenennen. `index.js`

Example Node.js 18 und höher

```
const { version } = require("@aws-sdk/client-s3/package.json");

exports.handler = async () => ({ version });
```

Dies gibt eine Antwort im folgenden Format zurück:

```
{
  "version": "3.462.0"
}
```

Verwenden von Keepalive für TCP-Verbindungen

Der standardmäßige Node.js-HTTP/HTTPS-Agent erstellt eine neue TCP-Verbindung für jede neue Anforderung. Um die Kosten für den Aufbau neuer Verbindungen `keepAlive: true` zu vermeiden, können Sie Verbindungen wiederverwenden, für die Ihre Funktion das AWS SDK

verwendet JavaScript. Keepalive kann die Anforderungszeiten für Lambda-Funktionen reduzieren, die mehrere API-Aufrufe unter Verwendung des SDK ausführen.

Im AWS SDK für JavaScript 3.x, das in `nodejs18.x` und späteren Lambda-Laufzeiten enthalten ist, ist Keep-Alive standardmäßig aktiviert. Informationen zur Deaktivierung von Keep-Alive finden Sie unter Wiederverwenden von Verbindungen mit Keep-Alive in Node.js im SDK for 3.x Developer Guide.AWS JavaScript Weitere Informationen zur Verwendung von Keep-Alive finden Sie im Developer Tools Blog unter HTTP keep-alive is default on in modular SDK. AWS JavaScript AWS

CA-Zertifikat wird geladen

Für Laufzeitversionen von Node.js bis Node.js 18 lädt Lambda automatisch Amazon-spezifische CA-Zertifikate (Certificate Authority), um Ihnen die Erstellung von Funktionen zu erleichtern, die mit anderen Diensten interagieren. AWS Lambda enthält beispielsweise die Amazon-RDS-Zertifikate, die für die Validierung des in Ihrer Amazon-RDS-Datenbank installierten Server-Identitätszertifikats erforderlich sind. Dieses Verhalten kann sich bei Kaltstarts auf die Leistung auswirken.

Ab Node.js 20 lädt Lambda standardmäßig keine zusätzlichen CA-Zertifikate mehr. Die Laufzeit Node.js 20 enthält eine Zertifikatsdatei mit allen Amazon-CA-Zertifikaten, die sich unter `/var/runtime/ca-cert.pem` befinden. Um dasselbe Verhalten aus Node.js 18 und früheren Laufzeiten wiederherzustellen, setzen Sie die Umgebungsvariable `NODE_EXTRA_CA_CERTS` auf `/var/runtime/ca-cert.pem`.

Für eine optimale Leistung empfehlen wir, nur die benötigten Zertifikate mit Ihrem Bereitstellungspaket zu bündeln und diese über die Umgebungsvariable `NODE_EXTRA_CA_CERTS` zu laden. Die Zertifikatsdatei sollte aus einem oder mehreren vertrauenswürdigen Stammzertifikaten oder Zertifikaten von Zwischenzertifizierungsstellen im PEM-Format bestehen. Fügen Sie für RDS die erforderlichen Zertifikate beispielsweise zusammen mit Ihrem Code als `certificates/rds.pem` hinzu. Laden Sie dann die Zertifikate, indem Sie `NODE_EXTRA_CA_CERTS` auf `/var/task/certificates/rds.pem` festlegen.

Definieren Sie den Lambda-Funktionshandler in Node.js

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Die folgende Beispielfunktion protokolliert den Inhalt des Ereignisobjekts und gibt den Speicherort der Protokolle zurück.

> **Note**
>
> Diese Seite zeigt Beispiele für CommonJS- und ES-Modulhandler. Weitere Informationen zu den Unterschieden zwischen diesen beiden Handler-Typen finden Sie unter Designieren eines Funktionshandlers als ES-Modul.

ES module handler

Example

```
export const handler = async (event, context) => {
  console.log("EVENT: \n" + JSON.stringify(event, null, 2));
  return context.logStreamName;
};
```

CommonJS module handler

Example

```
exports.handler = async function (event, context) {
  console.log("EVENT: \n" + JSON.stringify(event, null, 2));
  return context.logStreamName;
};
```

Wenn Sie eine Funktion konfigurieren, besteht der Wert der Handler-Einstellung aus dem Dateinamen und dem Namen der exportierten Handler-Methode, getrennt durch einen Punkt. Der Standardwert in der Konsole und für die Beispiele in diesem Handbuch ist `index.handler`. Dies deutet auf die `handler`-Methode hin, die aus der `index.js`-Datei wurde.

Die Laufzeit übergibt Argumente an die Handler-Methode. Das erste Argument ist das Objekt `event`, das Informationen aus dem Aufrufer enthält. Der Aufrufer übergibt diese Informationen als Zeichenfolge im JSON-Format, wenn er Invoke, aufruft, und die Laufzeit konvertiert sie in ein Objekt. Wenn ein AWS Dienst Ihre Funktion aufruft, variiert die Ereignisstruktur je nach Dienst.

Das zweite Argument ist das Context-Objekt, das Informationen über den Aufruf, die Funktion und die Ausführungsumgebung enthält. Im vorherigen Beispiel ruft die Funktion den Namen des Protokollstreams aus dem Context-Objekt ab und gibt ihn an den Aufrufer zurück.

Sie können ein Callback-Argument verwenden, ist eine Funktion, die Sie in nicht-asynchronen Handlern aufrufen können, um eine Antwort zu senden. Wir empfehlen Ihnen, Async/Await anstelle von Callback zu verwenden. Async/Await bietet eine verbesserte Lesbarkeit, Fehlerbehandlung und Effizienz. Weitere Informationen zu den Unterschieden zwischen Async/Await und Callbacks finden Sie unter Callbacks verwenden.

Benennung

Wenn Sie eine Funktion konfigurieren, besteht der Wert der Handler-Einstellung aus dem Dateinamen und dem Namen der exportierten Handler-Methode, getrennt durch einen Punkt. Die Standardeinstellung für Funktionen, die in der Konsole erstellt wurden, und für Beispiele in diesem Handbuch ist`index.handler`. Dies gibt die `handler` Methode an, die aus der `index.js` `index.mjs` OR-Datei exportiert wird.

Wenn Sie eine Funktion in der Konsole mit einem anderen Dateinamen oder Funktionshandlernamen erstellen, müssen Sie den Standardhandlernamen bearbeiten.

So ändern Sie den Funktionshandlernamen (Konsole)

1. Öffnen Sie die Seite Functions (Funktionen) der Lambda-Konsole und wählen Sie eine Funktion aus.
2. Wählen Sie die Registerkarte Code (Code).
3. Scrollen Sie nach unten zum Bereich Laufzeiteinstellungen und wählen Sie Bearbeiten.
4. Geben Sie unter Handler den neuen Namen für Ihren Funktionshandler ein.
5. Wählen Sie Speichern.

Verwenden von async/await

Wenn Ihr Code eine asynchrone Aufgabe ausführt, verwenden Sie das Async-/Await, um sicherzustellen, dass die Ausführung des Handler beendet wird. Async/Await ist eine präzise und lesbare Methode, um asynchronen Code in Node.js zu schreiben, ohne dass verschachtelte Callbacks oder Verkettungsversprechen erforderlich sind. Mit Async/Await können Sie Code schreiben, der sich wie synchroner Code liest, aber dennoch asynchron und blockierungsfrei ist.

Das `async`-Schlüsselwort kennzeichnet eine Funktion als asynchron, und das `await`-Schlüsselwort unterbricht die Ausführung der Funktion, bis `Promise` aufgelöst ist.

> **Note**
>
> Stellen Sie sicher, dass Sie warten, bis die asynchronen Ereignisse abgeschlossen sind. Wenn die Funktion zurückgibt, bevor die asynchronen Ereignisse abgeschlossen sind, könnte die Funktion fehlschlagen oder ein unerwartetes Verhalten in Ihrer Anwendung verursachen. Dies kann passieren, wenn eine `forEach`-Schleife ein asynchrones Ereignis enthält. `forEach`-Schleifen erwarten einen synchronen Aufruf. Weitere Informationen finden Sie unter Array.prototype.forEach () in der Mozilla-Dokumentation.

ES module handler

Example – HTTP-Anforderung mit async/await

```
const url = "https://aws.amazon.com/";

export const handler = async(event) => {
    try {
        // fetch is available in Node.js 18 and later runtimes
        const res = await fetch(url);
        console.info("status", res.status);
        return res.status;
    }
    catch (e) {
        console.error(e);
        return 500;
    }
};
```

CommonJS module handler

Example – HTTP-Anforderung mit async/await

```
const https = require("https");
let url = "https://aws.amazon.com/";

exports.handler = async function (event) {
  let statusCode;
  await new Promise(function (resolve, reject) {
    https.get(url, (res) => {
        statusCode = res.statusCode;
        resolve(statusCode);
      }).on("error", (e) => {
        reject(Error(e));
      });
  });
  console.log(statusCode);
  return statusCode;
};
```

Das nächste Beispiel verwendet Async/Await, um Ihre Buckets von Amazon Simple Storage Service aufzulisten.

> **Note**
>
> Bevor Sie dieses Beispiel verwenden, stellen Sie sicher, dass die Ausführungsrolle Ihrer Funktion über Amazon-S3-Leseberechtigungen verfügt.

ES module handler

Example — AWS SDK v3 mit Async/Await

In diesem Beispiel wird AWS SDK for JavaScript Version 3 verwendet, die in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

```
import {S3Client, ListBucketsCommand} from '@aws-sdk/client-s3';
const s3 = new S3Client({region: 'us-east-1'});
```

```
export const handler = async(event) => {
  const data = await s3.send(new ListBucketsCommand({}));
  return data.Buckets;

};
```

CommonJS module handler

Example — AWS SDK v3 mit Async/Await

In diesem Beispiel wird AWS SDK for JavaScript Version 3 verwendet, die in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

```
const { S3Client, ListBucketsCommand } = require('@aws-sdk/client-s3');
const s3 = new S3Client({ region: 'us-east-1' });

exports.handler = async (event) => {
  const data = await s3.send(new ListBucketsCommand({}));
  return data.Buckets;
};
```

Callbacks verwenden

Wir empfehlen, dass Sie Async/Await verwenden, um den Funktionshandler zu deklarieren, anstatt Callbacks zu verwenden. Async/Await ist aus mehreren Gründen eine bessere Wahl:

- Lesbarkeit: Async/Await-Code ist einfacher zu lesen und zu verstehen als Callback-Code, der schnell schwer zu verstehen sein kann und in die Callback-Hölle führen kann.
- Debugging und Fehlerbehandlung: Das Debuggen von Callback-basiertem Code kann schwierig sein. Der Aufrufliste kann schwer zu folgen sein und Fehler können leicht verschluckt werden. Mit Async/Await können Sie Try/Catch-Blöcke verwenden, um Fehler zu behandeln.
- Effizienz: Callbacks erfordern oft das Umschalten zwischen verschiedenen Teilen des Codes. Async/Await kann die Anzahl der Kontextwechsel reduzieren, was zu effizienterem Code führt.

Wenn Sie in Ihrem Handler verwenden, wird die Funktion so lange ausgeführt, bis die Ereignisschleife leer ist oder eine Zeitüberschreitung auftritt. Die Antwort wird erst an den Aufrufer gesendet, wenn alle Ereignisschleifenaufgaben abgeschlossen sind. Wenn eine Zeitüberschreitung der Funktion auftritt, wird stattdessen ein Fehler zurückgegeben. Sie können die Laufzeit so

konfigurieren, dass die Antwort sofort gesendet wird, indem Sie context.callback WaitsFor EmptyEvent Loop auf false setzen.

Die Callback-Funktion verwendet zwei Argumente, einen `Error` und eine Antwort. Das Response-Objekt muss mit kompatibel sei `JSON.stringify`.

Die folgende Beispielfunktion prüft eine URL und gibt den Statuscode an den Aufrufer zurück.

ES module handler

Example – HTTP-Anforderung mit callback

```
import https from "https";
let url = "https://aws.amazon.com/";

export function handler(event, context, callback) {
  https.get(url, (res) => {
      callback(null, res.statusCode);
    }).on("error", (e) => {
      callback(Error(e));
    });
}
```

CommonJS module handler

Example – HTTP-Anforderung mit callback

```
const https = require("https");
let url = "https://aws.amazon.com/";

exports.handler = function (event, context, callback) {
  https.get(url, (res) => {
      callback(null, res.statusCode);
    }).on("error", (e) => {
      callback(Error(e));
    });
};
```

Im folgenden Beispiel wird die Antwort von Amazon S3 an den Aufrufer zurückgegeben, sobald sie verfügbar ist. Die Zeitüberschreitung für die Ereignisschleife wird eingefroren und die Ausführung wird fortgesetzt, wenn die Funktion das nächste Mal aufgerufen wird.

> **Note**
>
> Bevor Sie dieses Beispiel verwenden, stellen Sie sicher, dass die Ausführungsrolle Ihrer Funktion über Amazon-S3-Leseberechtigungen verfügt.

ES module handler

Example — SDK v3 AWS mit Loop callbackWaitsFor EmptyEvent

In diesem Beispiel wird AWS SDK for JavaScript Version 3 verwendet, die in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

```
import AWS from "@aws-sdk/client-s3";
const s3 = new AWS.S3({});

export const handler = function (event, context, callback) {
  context.callbackWaitsForEmptyEventLoop = false;
  s3.listBuckets({}, callback);
  setTimeout(function () {
    console.log("Timeout complete.");
  }, 5000);
};
```

CommonJS module handler

Example — AWS SDK v3 mit Loop callbackWaitsFor EmptyEvent

In diesem Beispiel wird AWS SDK for JavaScript Version 3 verwendet, die in `nodejs18.x` und späteren Laufzeiten verfügbar ist.

```
const AWS = require("@aws-sdk/client-s3");
const s3 = new AWS.S3({});

exports.handler = function (event, context, callback) {
  context.callbackWaitsForEmptyEventLoop = false;
  s3.listBuckets({}, callback);
  setTimeout(function () {
    console.log("Timeout complete.");
  }, 5000);
};
```

Bereitstellen von Node.js Lambda-Funktionen mit ZIP-Dateiarchiven

Der Code Ihrer AWS Lambda Funktion besteht aus einer .js- oder .mjs-Datei, die den Handlercode Ihrer Funktion enthält, zusammen mit allen zusätzlichen Paketen und Modulen, von denen Ihr Code abhängt. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Dieses Paket kann entweder ein ZIP-Dateiarchiv oder ein Container-Image sein. Weitere Informationen zur Verwendung von Container-Images mit Node.js finden Sie unter Bereitstellen von Node.js-Lambda-Funktionen mit Container-Images.

Zum Erstellen des Bereitstellungspakets für ein ZIP-Dateiarchiv können Sie ein integriertes Dienstprogramm für ZIP-Dateien Ihres Befehlszeilen-Tools oder ein anderes Dienstprogramm für ZIP-Dateien verwenden, wie 7zip. In den Beispiele in den folgenden Abschnitten wird davon ausgegangen, dass Sie ein `zip`-Befehlszeilen-Tool in einer Linux- oder MacOS-Umgebung verwenden. Unter Windows können Sie das Windows-Subsystem für Linux installieren, um eine Windows-Version von Ubuntu und Bash zu erhalten und dieselben Befehle zu verwenden.

Da Lambda POSIX-Dateiberechtigungen verwendet, müssen Sie möglicherweise Berechtigungen für den Bereitstellungspaketordner festlegen, bevor Sie das ZIP-Dateiarchiv erstellen.

Themen

Laufzeitabhängigkeiten in Node.js

Für Lambda-Funktionen, die die Node.js-Laufzeit verwenden, kann eine Abhängigkeit ein beliebiges Node.js-Modul sein. Die Laufzeitumgebung von Node.js enthält eine Reihe gängiger Bibliotheken sowie eine Version des AWS SDK for JavaScript. Die `nodejs16.x`-Lambda-Laufzeitversion enthält Version 2.x des SDK. Laufzeitversionen `nodejs18.x` und höher beinhalten Version 3 des SDK. Um Version 2 des SDK mit den Laufzeitversionen `nodejs18.x` und höher zu verwenden, fügen Sie das SDK Ihrem Bereitstellungspaket für die ZIP-Datei hinzu. Wenn die von Ihnen gewählte Laufzeit die

Version des von Ihnen verwendeten SDK enthält, müssen Sie die SDK-Bibliothek nicht in Ihre ZIP-Datei aufnehmen. Informationen darüber, welche Version des SDK in der von Ihnen verwendeten Runtime enthalten ist, finden Sie unter. the section called “SDK-Versionen, die Runtime enthalten”

Lambda aktualisiert die SDK-Bibliotheken in der Node.js-Laufzeit regelmäßig, um die aktuellen Features und Sicherheitsupgrades aufzunehmen. Lambda wendet auch Sicherheitspatches und Updates auf die anderen in der Laufzeit enthaltenen Bibliotheken an. Um die volle Kontrolle über die Abhängigkeiten in Ihrem Paket zu haben, können Sie Ihrem Bereitstellungspaket Ihre bevorzugte Version einer beliebigen in die Laufzeit eingeschlossenen Abhängigkeit hinzufügen. Wenn Sie beispielsweise eine bestimmte Version des SDK verwenden möchten JavaScript, können Sie sie als Abhängigkeit in Ihre ZIP-Datei aufnehmen. Weitere Informationen zum Hinzufügen von in die Laufzeit eingeschlossene Abhängigkeiten zu Ihrer ZIP-Datei finden Sie unter Suchpfad für Abhängigkeiten und integrierte Laufzeit-Bibliotheken.

Im Rahmen des AWS -Modells der geteilten Verantwortung sind Sie für die Verwaltung aller Abhängigkeiten in den Bereitstellungspaketen Ihrer Funktionen verantwortlich. Dies beinhaltet das Durchführen von Updates und Sicherheitspatches. Zum Aktualisieren von Abhängigkeiten im Bereitstellungspaket Ihrer Funktion erstellen Sie zunächst eine neue ZIP-Datei und laden Sie diese dann in Lambda hoch. Weitere Informationen finden Sie unter ZIP-Bereitstellungspakets mit Abhängigkeiten erstellen und Erstellen und Aktualisieren von Node.js-Lambda-Funktionen mithilfe von ZIP-Dateien.

ZIP-Bereitstellungspakets ohne Abhängigkeiten erstellen

Wenn Ihr Funktionscode neben den in der Lambda-Laufzeit eingeschlossenen Bibliotheken keine Abhängigkeiten hat, enthält Ihre ZIP-Datei nur die `index.js`- oder `index.mjs`-Datei mit dem Handler-Code Ihrer Funktion. Erstellen Sie mit Ihrem bevorzugten ZIP-Programm eine ZIP-Datei mit Ihrer `index.js`- oder `index.mjs`-Datei im Stammverzeichnis. Wenn sich die Datei mit Ihrem Handler-Code nicht im Stammverzeichnis Ihrer ZIP-Datei, kann Lambda Ihren Code nicht ausführen.

Informationen zum Bereitstellen Ihrer ZIP-Datei zum Erstellen einer neuen Lambda-Funktion oder Aktualisieren einer vorhandenen Funktion, finden Sie unter Erstellen und Aktualisieren von Node.js-Lambda-Funktionen mithilfe von ZIP-Dateien.

ZIP-Bereitstellungspakets mit Abhängigkeiten erstellen

Wenn Ihr Funktionscode von Paketen oder Modulen abhängt, die nicht in der Lambda-Node.js-Laufzeit enthalten sind, können Sie diese Abhängigkeiten entweder mit Ihrem Funktionscode zu Ihrer ZIP-Datei hinzufügen oder eine Lambda-Ebene verwenden. Die Anweisungen in diesem Abschnitt

zeigen Ihnen, wie Sie Ihre Abhängigkeiten in Ihr ZIP-Bereitstellungspaket aufnehmen. Anweisungen zum Einschließen Ihrer Abhängigkeiten in eine Ebene finden Sie unter the section called “Erstellen einer Node.js-Ebene für Ihre Abhängigkeiten”.

Die folgenden CLI-Befehle erstellen Sie eine ZIP-Datei mit dem Namen `my_deployment_package.zip`, welche die `index.js`- oder `index.mjs`-Datei mit dem Handler-Code Ihrer Funktion und die zugehörigen Abhängigkeiten enthält. Im Beispiel installieren Sie Abhängigkeiten mit dem npm-Paketmanager.

Erstellen des Bereitstellungspakets

1. Navigieren Sie zum Projektverzeichnis, das Ihre Quellcodedatei `index.js` oder `index.mjs` enthält. In diesem Beispiel trägt das Verzeichnis den Namen `my_function`.

   ```
   cd my_function
   ```

2. Installieren Sie die erforderlichen Bibliotheken Ihrer Funktion im Verzeichnis `node_modules` mit dem Befehl `npm install`. In diesem Beispiel installieren Sie das AWS X-Ray-SDK for Node.js.

   ```
   npm install aws-xray-sdk
   ```

   Dabei wird eine Ordnerstruktur erstellt, die etwa wie folgt aussieht:

   ```
   ~/my_function
   ### index.mjs
   ### node_modules
       ### async
       ### async-listener
       ### atomic-batcher
       ### aws-sdk
       ### aws-xray-sdk
       ### aws-xray-sdk-core
   ```

   Sie können Ihrem Bereitstellungspaket auch benutzerdefinierte Module hinzufügen, die Sie selbst erstellen. Erstellen Sie ein Verzeichnis unter `node_modules` mit dem Namen Ihres Moduls und speichern Sie Ihre benutzerdefinierten geschriebenen Pakete dort.

3. Erstellen Sie im Stammverzeichnis eine ZIP-Datei mit den Inhalten Ihres Projektordners. Benutzen Sie die `r` (rekursive) Option, um sicherzustellen, dass der zip-Befehl die Unterordner komprimiert.

```
zip -r my_deployment_package.zip .
```

Erstellen einer Node.js-Ebene für Ihre Abhängigkeiten

Die Anweisungen in diesem Abschnitt zeigen Ihnen, wie Sie Ihre Abhängigkeiten in eine Ebene einschließen. Anweisungen zum Einschließen Ihrer Abhängigkeiten in Ihr Bereitstellungspaket finden Sie unter the section called “ZIP-Bereitstellungspakets mit Abhängigkeiten erstellen”.

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Ebeneninhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

- `nodejs/node_modules`
- `nodejs/node16/node_modules (NODE_PATH)`
- `nodejs/node18/node_modules (NODE_PATH)`
- `nodejs/node20/node_modules (NODE_PATH)`

Die Struktur Ihrer Ebene-ZIP-Datei könnte beispielsweise wie folgt aussehen:

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

Darüber hinaus erkennt Lambda automatisch alle Bibliotheken im `/opt/lib`-Verzeichnis und alle Binärdateien im `/opt/bin`-Verzeichnis. Um sicherzustellen, dass Lambda Ihren Ebeneninhalt korrekt findet, können Sie auch eine Ebene mit der folgenden Struktur erstellen:

```
custom-layer.zip
# lib
    | lib_1
    | lib_2
# bin
    | bin_1
    | bin_2
```

Nachdem Sie Ihre Ebene gebündelt haben, sehen Sie sich the section called “Erstellen und Löschen von Ebenen” und the section called “Hinzufügen von Ebenen” an, um die Einrichtung Ihrer Ebene abzuschließen.

Suchpfad für Abhängigkeiten und integrierte Laufzeit-Bibliotheken

Die Laufzeitumgebung von Node.js enthält eine Reihe gängiger Bibliotheken sowie eine Version des AWS SDK for JavaScript. Wenn Sie eine andere Version einer in die Laufzeit eingeschlossenen Bibliothek verwenden möchten, können Sie sie mit Ihrer Funktion bündeln oder sie als Abhängigkeit zu Ihrem Bereitstellungspaket hinzufügen. Sie können beispielsweise eine andere Version des SDK verwenden, indem Sie es Ihrem ZIP-Bereitstellungspaket hinzufügen. Sie können sie auch in eine Lambda-Ebene für Ihre Funktion aufnehmen.

Wenn Sie in Ihrem Code eine `import`- oder `require`-Anweisung verwenden, durchsucht die Node.js-Laufzeit die Verzeichnisse im `NODE_PATH`-Pfad, bis das Modul gefunden wird. Standardmäßig ist der erste Speicherort, den die Laufzeit durchsucht, das Verzeichnis, in das Ihr ZIP-Bereitstellungspaket entpackt und bereitgestellt wird (`/var/task`). Nehmen Sie eine Version einer in der Laufzeit integrierten Bibliothek in Ihr Bereitstellungspaket auf, hat diese Version Vorrang vor der in der Laufzeit enthaltenen. Abhängigkeiten in Ihrem Bereitstellungspaket haben ebenfalls Vorrang vor Abhängigkeiten in Ebenen.

Wenn Sie einer Ebene eine Abhängigkeit hinzufügen, extrahiert Lambda diese in `/opt/nodejs/nodexx/node_modules`, wobei `nodexx` die von Ihnen verwendete Version der Laufzeitumgebung ist. Im Suchpfad hat dieses Verzeichnis Vorrang vor dem Verzeichnis mit den zur Laufzeit enthaltenen Bibliotheken (`/var/lang/lib/node_modules`). Bibliotheken in Funktionsebenen haben daher Vorrang vor Versionen, die in der Laufzeit enthalten sind.

Sie können den vollständigen Suchpfad für Ihre Lambda-Funktion sehen, indem Sie die folgende Codezeile hinzufügen:

```
console.log(process.env.NODE_PATH)
```

Fügen Sie Abhängigkeiten alternativ auch in einem separaten Ordner in Ihrem ZIP-Paket hinzu. Fügen Sie beispielsweise eine benutzerdefinierte Version zu einem Ordner in Ihrem ZIP-Paket mit dem Namen `common` hinzu. Wird Ihr ZIP-Paket entpackt und bereitgestellt, wird dieser Ordner im Verzeichnis „`/var/task`“ abgelegt. Um eine Abhängigkeit von einem Ordner in Ihrem ZIP-Bereitstellungspaket in Ihrem Code zu verwenden, verwenden Sie eine `import { } from`- oder `const { } = require()`-Anweisung, je nachdem, ob Sie die CJS- oder die ESM-Modulauflösung verwenden. Beispielsweise:

```
import { myModule } from './common'
```

Wenn Sie Ihren Code mit `esbuild`, `rollup` oder ähnlichem bündeln, werden die von Ihrer Funktion verwendeten Abhängigkeiten in einer oder mehreren Dateien gebündelt. Wir empfehlen, diese Methode zu verwenden, um Abhängigkeiten wann immer möglich zu vergeben. Im Vergleich zum Hinzufügen von Abhängigkeiten zu Ihrem Bereitstellungspaket führt die Bündelung Ihres Codes zu einer verbesserten Leistung, da weniger E/A-Vorgänge erforderlich sind.

Erstellen und Aktualisieren von Node.js-Lambda-Funktionen mithilfe von ZIP-Dateien

Nach der Erstellung Ihres ZIP-Bereitstellungspakets können Sie es verwenden, um eine neue Lambda-Funktion zu erstellen oder eine vorhandene zu aktualisieren. Sie können Ihr .zip-Paket mithilfe der Lambda-Konsole, der und der AWS Command Line Interface Lambda-API bereitstellen. Sie können Lambda-Funktionen auch mit AWS Serverless Application Model (AWS SAM) und AWS CloudFormation erstellen und aktualisieren.

Die maximale Größe eines ZIP-Bereitstellungspakets für Lambda beträgt 250 MB (entpackt). Beachten Sie, dass dieser Grenzwert für die kombinierte Größe aller hochgeladenen Dateien gilt, einschließlich aller Lambda-Ebenen.

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Schreibweise von Linux-Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen () für Verzeichnisse und ausführbare Dateien. rwxr-xr-x

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Konsole

Eine neue Funktion müssen Sie zuerst in der Konsole erstellen und dann Ihr ZIP-Archiv hochladen. Zum Aktualisieren einer bestehenden Funktion öffnen Sie die Seite für Ihre Funktion und gehen dann genauso vor, um Ihre aktualisierte ZIP-Datei hinzuzufügen.

Bei einer ZIP-Datei mit unter 50 MB können Sie eine Funktion erstellen oder aktualisieren, indem Sie die Datei direkt von Ihrem lokalen Computer hochladen. Bei ZIP-Dateien mit einer Größe von mehr als 50 MB müssen Sie Ihr Paket zuerst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3-Bucket mithilfe von finden Sie unter Erste Schritte mit Amazon S3. AWS Management Console Informationen zum Hochladen von Dateien mit dem AWS CLI finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch.

> **Note**
>
> Sie können den Bereitstellungspakettyp (.zip oder Container-Image) für eine bestehende Funktion nicht ändern. Sie können beispielsweise eine Container-Image-Funktion nicht so konvertieren, dass sie ein ZIP-Dateiarchiv verwendet. Sie müssen eine neue Funktion erstellen.

So erstellen Sie eine neue Funktion (Konsole)

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Funktion erstellen aus.
2. Wählen Sie Author from scratch aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie als Funktionsname den Namen Ihrer Funktion ein.
   b. Wählen Sie für Laufzeit die Laufzeit aus, die Sie verwenden möchten.
   c. (Optional) Für Architektur wählen Sie die Befehlssatz-Architektur für Ihre Funktion aus. Die Standardarchitektur ist x86_64. Stellen Sie sicher, dass das ZIP-Bereitstellungspaket für Ihre Funktion mit der von Ihnen gewählten Befehlssatzarchitektur kompatibel ist.
4. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
5. Wählen Sie Funktion erstellen. Lambda erstellt eine grundlegende „Hello World“-Funktion mit der von Ihnen gewählten Laufzeit.

So laden Sie ein ZIP-Archiv von Ihrem lokalen Computer hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie die ZIP-Datei aus.
5. Laden Sie die ZIP-Datei wie folgt hoch:
   a. Wählen Sie Hochladen und dann Ihre ZIP-Datei in der Dateiauswahl aus.
   b. Klicken Sie auf Open.
   c. Wählen Sie Speichern.

So laden Sie ein ZIP-Archiv aus einem Amazon-S3-Bucket hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie eine neue ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie den Amazon-S3-Speicherort aus.
5. Fügen Sie die Amazon-S3-Link-URL Ihrer ZIP-Datei ein und wählen Sie Speichern aus.

ZIP-Dateifunktionen mithilfe des Konsolencode-Editors aktualisieren

Für einige Funktionen mit ZIP-Bereitstellungspaketen können Sie Ihren Funktionscode direkt mit dem in der Lambda-Konsole integrierten Code-Editor aktualisieren. Zur Verwendung dieses Features muss Ihre Funktion folgende Kriterien erfüllen:

- Ihre Funktion muss eine der interpretierten Sprache der Laufzeit verwenden (Python, Node.js oder Ruby).
- Das Bereitstellungspaket Ihrer Funktion muss kleiner als 3 MB sein.

Funktionscode für Funktionen mit Container-Image-Bereitstellungspaketen kann nicht direkt in der Konsole bearbeitet werden.

So aktualisieren Sie Ihren Funktionscode mit dem Code-Editor

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle Ihre Quellcodedatei aus und bearbeiten Sie sie im integrierten Code-Editor.
4. Nach der Bearbeitung Ihres Codes wählen Sie Bereitstellen aus, um Ihre Änderungen zu speichern und Ihre Funktion zu aktualisieren.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe der AWS CLI

Sie können die AWS CLI verwenden, um eine neue Funktion zu erstellen oder eine vorhandene unter Verwendung einer ZIP-Datei zu aktualisieren. Verwenden Sie die Erstellungsfunktion und die update-function-codeBefehle, um Ihr .zip-Paket bereitzustellen. Wenn Ihre ZIP-Datei kleiner als 50 MB ist, können Sie das ZIP-Paket von einem Dateispeicherort auf Ihrem lokalen Build-Computer hochladen. Bei größeren Dateien müssen Sie Ihr ZIP-Paket aus einem Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

> **Note**
>
> Wenn Sie Ihre ZIP-Datei mithilfe von aus einem Amazon S3 S3-Bucket hochladen AWS CLI, muss sich der Bucket im selben Verzeichnis befinden AWS-Region wie Ihre Funktion.

Um eine neue Funktion mithilfe einer .zip-Datei mit dem zu erstellen AWS CLI, müssen Sie Folgendes angeben:

- Den Namen Ihrer Funktion (`--function-name`)
- Die Laufzeit Ihrer Funktion (`--runtime`)
- Den Amazon-Ressourcennamen (ARN) der Ausführungsrolle der Funktion (`--role`).
- Den Namen der Handler-Methode in Ihrem Funktionscode (`--handler`)

Sie müssen auch den Speicherort Ihrer ZIP-Datei angeben. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda create-function --function-name myFunction \
--runtime nodejs20.x --handler index.handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigte `--code`-Option. Sie müssen den `S3ObjectVersion`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda create-function --function-name myFunction \
--runtime nodejs20.x --handler index.handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=DOC-EXAMPLE-BUCKET,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Um eine vorhandene Funktion mit der CLI zu aktualisieren, geben Sie den Namen Ihrer Funktion unter Verwendung des `--function-name`-Parameters an. Sie müssen auch den Speicherort der ZIP-Datei angeben, die Sie zum Aktualisieren Ihres Funktionscodes verwenden möchten. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigten `--s3-bucket`- und `--s3-key`-Optionen. Sie müssen den `--s3-object-version`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket DOC-EXAMPLE-BUCKET --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Lambda-API

Um Funktionen zu erstellen und zu konfigurieren, die ein ZIP-Dateiarchiv verwenden, verwenden Sie die folgenden API-Operationen:

- CreateFunction
- UpdateFunctionCode

Funktionen mit ZIP-Dateien erstellen und aktualisieren mit AWS SAM

Das AWS Serverless Application Model (AWS SAM) ist ein Toolkit, das dabei hilft, den Prozess der Erstellung und Ausführung serverloser Anwendungen zu optimieren. AWS Sie definieren die Ressourcen für Ihre Anwendung in einer YAML- oder JSON-Vorlage und verwenden die AWS SAM Befehlszeilenschnittstelle (AWS SAM CLI), um Ihre Anwendungen zu erstellen, zu verpacken und bereitzustellen. Wenn Sie eine Lambda-Funktion aus einer AWS SAM Vorlage erstellen, AWS SAM wird automatisch ein ZIP-Bereitstellungspaket oder ein Container-Image mit Ihrem Funktionscode und allen von Ihnen angegebenen Abhängigkeiten erstellt. Weitere Informationen zur Verwendung AWS SAM zum Erstellen und Bereitstellen von Lambda-Funktionen finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model Entwicklerhandbuch.

Sie können es auch verwenden AWS SAM , um eine Lambda-Funktion mithilfe eines vorhandenen ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion zu erstellen AWS SAM, können Sie Ihre ZIP-Datei in einem Amazon S3 S3-Bucket oder in einem lokalen Ordner auf Ihrem Build-Computer speichern. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS SAM Vorlage spezifiziert die `AWS::Serverless::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `CodeUri`- auf die Amazon S3 S3-URI, den Pfad zum lokalen Ordner oder FunctionCodeObjekt des Funktionscodes gesetzt
- `Runtime` – festlegen auf die gewünschte Laufzeit

Wenn Ihre ZIP-Datei größer als 50 MB ist, müssen Sie sie nicht zuerst in einen Amazon S3 S3-Bucket hochladen. AWS SAM AWS SAM kann .zip-Pakete bis zur maximal zulässigen Größe von 250 MB (entpackt) von einem Speicherort auf Ihrem lokalen Build-Computer hochladen.

Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei in finden Sie AWS::Serverless::Functionim AWS SAM Entwicklerhandbuch.AWS SAM

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe von AWS CloudFormation

Sie können verwenden AWS CloudFormation , um eine Lambda-Funktion mithilfe eines ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion aus einer ZIP-Datei zu erstellen, müssen Sie

Ihre Datei zunächst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS CloudFormation Vorlage spezifiziert die `AWS::Lambda::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `Code` – Geben Sie den Namen des Amazon-S3-Buckets und den ZIP-Dateinamen in die Felder `S3Bucket` und `S3Key` ein
- `Runtime` – festlegen auf die gewünschte Laufzeit

Die AWS CloudFormation generierte ZIP-Datei darf 4 MB nicht überschreiten. Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei finden Sie AWS::Lambda::Functionim AWS CloudFormation Benutzerhandbuch. AWS CloudFormation

Bereitstellen von Node.js-Lambda-Funktionen mit Container-Images

Es gibt drei Möglichkeiten, ein Container-Image für eine Node.js-Lambda-Funktion zu erstellen:

- Verwenden Sie ein Basis-Image für Node.js AWS

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.
- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Node.js in das Image aufnehmen.
- Verwenden Sie ein Nicht-Basis-Image AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Node.js in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

Themen

- AWS Basis-Images für Node.js
- Verwenden Sie ein Basis-Image für Node.js AWS
- Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

AWS Basis-Images für Node.js

AWS stellt die folgenden Basis-Images für Node.js bereit:

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
20	Node.js 20	Amazon Linux 2023	Dockerfile für Node.js 20 auf GitHub	
18	Node.js 18	Amazon Linux 2	Dockerfile für Node.js 18 auf GitHub	
16	Node.js 16	Amazon Linux 2	Dockerfile für Node.js 16 auf GitHub	12. Juni 2024

Amazon-ECR-Repository: gallery.ecr.aws/lambda/nodejs

Die Basis-Images von Node.js 20 und höher basieren auf dem minimalen Container-Image von Amazon Linux 2023. Frühere Basis-Images verwenden Amazon Linux 2. AL2023 bietet mehrere Vorteile gegenüber Amazon Linux 2, darunter einen geringeren Bereitstellungsaufwand und aktualisierte Versionen von Bibliotheken wie `glibc`.

AL2023-basierte Images verwenden `microdnf` (symbolisiert als`dnf`) als Paketmanager anstelle von`yum`, dem Standard-Paketmanager in Amazon Linux 2. `microdnf`ist eine eigenständige Implementierung von. `dnf` Eine Liste der Pakete, die in AL2023-basierten Images enthalten sind, finden Sie in den Spalten Minimal Container unter Comparing packages installed on Amazon Linux 2023 Container Images. Weitere Informationen zu den Unterschieden zwischen AL2023 und Amazon Linux 2 finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.

> **Note**
>
> Um AL2023-basierte Images lokal auszuführen, auch mit AWS Serverless Application Model (AWS SAM), müssen Sie Docker-Version 20.10.10 oder höher verwenden.

Verwenden Sie ein Basis-Image für Node.js AWS

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker (Mindestversion 20.10.10 für Node.js 20 und spätere Basis-Images)
- Node.js

Erstellen eines Images aus einem Base Image

Um ein Container-Image aus einem AWS Basis-Image für Node.js zu erstellen

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

   ```
   mkdir example
   cd example
   ```

2. Erstellen Sie ein neues Node.js-Projekt mit `npm`. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

   ```
   npm init
   ```

3. Erstellen Sie eine neue Datei mit dem Namen `index.js`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example CommonJS-Handler

   ```
   exports.handler = async (event) => {
       const response = {
           statusCode: 200,
           body: JSON.stringify('Hello from Lambda!'),
   ```

```
    };
    return response;
};
```

4. Wenn Ihre Funktion von anderen Bibliotheken als den abhängt AWS SDK for JavaScript, verwenden Sie npm, um sie Ihrem Paket hinzuzufügen.
5. Erstellen Sie eine neue Docker-Datei mit der folgenden Konfiguration:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.
   - Verwenden Sie den Befehl COPY, um den Funktionscode und die Laufzeitabhängigkeiten in eine von Lambda definierte Umgebungsvariable zu `{LAMBDA_TASK_ROOT}` kopieren.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

   Example Dockerfile

```
FROM public.ecr.aws/lambda/nodejs:20

# Copy function code
COPY index.js ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "index.handler" ]
```

6. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. In diesem Beispiel ist `docker-image` der Image-Name und `test` der Tag.

   ```
   docker run --platform linux/amd64 -p 9000:8080 docker-image:test
   ```

   Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis an den lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden Befehl aus: `Invoke-WebRequest`

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

Wenn Sie ein OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Laufzeitschnittstellen-Client erweitert die Lambda-Laufzeiten-API, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet.

Installieren Sie den Laufzeitschnittstellen-Client für Node.js mit dem npm-Paketmanager:

```
npm install aws-lambda-ric
```

Sie können den Runtime Interface-Client von Node.js auch herunterladen GitHub. Der Laufzeitschnittstellen-Client unterstützt die folgenden Node.js-Versionen:

- 14.x
- 16.x
- 18.x
- 20.x

Das folgende Beispiel zeigt, wie ein Container-Image für Node.js mithilfe eines AWS Nicht-Basis-Images erstellt wird. Das Beispiel-Dockerfile verwendet ein `buster`-Basis-Image. Das Docker-File enthält den Laufzeitschnittstellen-Client.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2

- Docker
- Node.js

Erstellen eines Images aus einem alternativen Basis-Image

Um ein Container-Image aus einem AWS Nicht-Basis-Image zu erstellen

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir example
cd example
```

2. Erstellen Sie ein neues Node.js-Projekt mit `npm`. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

```
npm init
```

3. Erstellen Sie eine neue Datei mit dem Namen `index.js`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example CommonJS-Handler

```
exports.handler = async (event) => {
    const response = {
        statusCode: 200,
        body: JSON.stringify('Hello from Lambda!'),
    };
    return response;
};
```

4. Erstellen Sie eine neue Docker-Datei. Das folgende Dockerfile verwendet ein `buster`-Basis-Image anstelle eines AWS -Basis-Images. Das Dockerfile enthält den Laufzeitschnittstellen-Client, der das Image mit Lambda kompatibel macht. Das folgende Dockerfile verwendet einen Build mit mehreren Phasen. In der ersten Phase wird ein Build-Image erstellt, bei dem es sich um eine Standardumgebung von Node.js handelt, in der die Abhängigkeiten der Funktion installiert werden. In der zweiten Phase wird ein schlankeres Image erstellt, das den Funktionscode und seine Abhängigkeiten enthält. Dadurch wird die endgültige Image-Größe reduziert.

   - Legen Sie `FROM`-Eigenschaft auf die Kennung des Basis-Images fest.

- Verwenden Sie den Befehl `COPY`, um den Funktionscode und die Laufzeitabhängigkeiten zu kopieren.
- Legen Sie `ENTRYPOINT` auf das Modul fest, das der Docker-Container beim Start ausführen soll. In diesem Fall ist das Modul der Laufzeitschnittstellen-Client.
- Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

Example Dockerfile

```
# Define custom function directory
ARG FUNCTION_DIR="/function"

FROM node:20-buster as build-image

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Install build dependencies
RUN apt-get update && \
    apt-get install -y \
    g++ \
    make \
    cmake \
    unzip \
    libcurl4-openssl-dev

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

WORKDIR ${FUNCTION_DIR}

# Install Node.js dependencies
RUN npm install

# Install the runtime interface client
RUN npm install aws-lambda-ric

# Grab a fresh slim copy of the image to reduce the final size
FROM node:20-buster-slim

# Required for Node runtimes which use npm@8.6.0+ because
```

```
# by default npm writes logs under /home/.npm and Lambda fs is read-only
ENV NPM_CONFIG_CACHE=/tmp/.npm

# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT ["/usr/local/bin/npx", "aws-lambda-ric"]
# Pass the name of the function handler as an argument to the runtime
CMD ["index.handler"]
```

5. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um das Image lokal zu testen. Sie können den Emulator in Ihr Image einbauen oder ihn mit dem folgenden Verfahren auf Ihrem lokalen Computer installieren.

Installieren des Laufzeitschnittstellen-Emulators auf Ihrem lokalen Computer

1. Führen Sie in Ihrem Projektverzeichnis den folgenden Befehl aus, um den Runtime-Interface-Emulator (x86-64-Architektur) herunterzuladen GitHub und auf Ihrem lokalen Computer zu installieren.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie die GitHub Repository-URL im vorherigen Befehl durch Folgendes:

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie das `$downloadLink` durch Folgendes:

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

2. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.

- `/usr/local/bin/npx aws-lambda-ric index.handler` ist der `ENTRYPOINT` gefolgt von dem `CMD` aus Ihrem Dockerfile.

Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /usr/local/bin/npx aws-lambda-ric index.handler
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/local/bin/npx aws-lambda-ric index.handler
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

3. Veröffentlichen Sie ein Ereignis auf dem lokalen Endpunkt.

Linux/macOS

Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Die Container-ID erhalten.

```
docker ps
```

5. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

- Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
- Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:
   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Beispiel:

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

   ```
   aws lambda create-function \
     --function-name hello-world \
     --package-type Image \
     --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
     --role arn:aws:iam::111122223333:role/lambda-ex
   ```

   > **Note**
   >
   > Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

AWS Lambda-Context-Objekt in Node.js

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Methoden

- `getRemainingTimeInMillis()` – Gibt die Anzahl der verbleibenden Millisekunden zurück, bevor die Ausführung das Zeitlimit überschreitet.

Context-Eigenschaften

- `functionName` – Der Name der Lambda-Funktion.
- `functionVersion` – Die Version der Funktion.
- `invokedFunctionArn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `memoryLimitInMB` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `awsRequestId` – Der Bezeichner der Aufrufanforderung.
- `logGroupName` – Protokollgruppe für die Funktion.
- `logStreamName` – Der Protokollstream für die Funktions-Instance.
- `identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
  - `cognitoIdentityId`— Die authentifizierte Amazon-Cognito-Identität.
  - `cognitoIdentityPoolId` – Der Amazon-Cognito-Identitätspool, der den Aufruf autorisiert hat.
- `clientContext` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`
  - `client.app_package_name`
  - `env.platform_version`
  - `env.platform`

  - `env.make`
  - `env.model`
  - `env.locale`
  - `Custom` – Benutzerdefinierte Werte, die durch die mobilen Anwendung festgelegt werden.
- `callbackWaitsForEmptyEventLoop` – Legen Sie den Wert auf „false“ fest, um die Antwort direkt zu senden, wenn der Rückruf ausgeführt wird, anstatt zu warten, bis die Node.js-Ereignisschleife leer ist. Bei „false“ werden alle ausstehenden Ereignisse während des nächsten Aufrufs weiter ausgeführt.

Die folgende Beispielfunktion protokolliert Kontextinformationen und gibt den Speicherort der Protokolle zurück.

Example Datei index.js

```
exports.handler = async function(event, context) {
  console.log('Remaining time: ', context.getRemainingTimeInMillis())
  console.log('Function name: ', context.functionName)
  return context.logStreamName
}
```

AWS Lambda Funktionsprotokollierung in Node.js

AWS Lambda überwacht automatisch Lambda-Funktionen in Ihrem Namen und sendet Protokolle an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Auf dieser Seite wird beschrieben, wie Sie eine Protokollausgabe aus dem Code Ihrer Lambda-Funktion erstellen oder mit der AWS Command Line Interface Lambda-Konsole oder der CloudWatch Konsole auf Logs zugreifen.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus dem Code Ihrer Funktion auszugeben, können Sie Methoden auf dem Konsolenobjekt oder eine Protokollierungsbibliothek verwenden, die zu `stdout` oder `stderr` schreibt. Das folgende Beispiel protokolliert die Werte der Umgebungsvariablen und des Ereignisobjekts.

Example Datei index.js – Protokollierung

```
exports.handler = async function(event, context) {
  console.log("ENVIRONMENT VARIABLES\n" + JSON.stringify(process.env, null, 2))
  console.info("EVENT\n" + JSON.stringify(event, null, 2))
  console.warn("Event not processed.")
  return context.logStreamName
}
```

Example Protokollformat

```
START RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Version: $LATEST
2019-06-07T19:11:20.562Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO ENVIRONMENT
 VARIABLES
{
  "AWS_LAMBDA_FUNCTION_VERSION": "$LATEST",
  "AWS_LAMBDA_LOG_GROUP_NAME": "/aws/lambda/my-function",
  "AWS_LAMBDA_LOG_STREAM_NAME": "2019/06/07/[$LATEST]e6f4a0c4241adcd70c262d34c0bbc85c",
  "AWS_EXECUTION_ENV": "AWS_Lambda_nodejs12.x",
  "AWS_LAMBDA_FUNCTION_NAME": "my-function",
  "PATH": "/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin",
  "NODE_PATH": "/opt/nodejs/node10/node_modules:/opt/nodejs/node_modules:/var/runtime/
node_modules",
  ...
}
2019-06-07T19:11:20.563Z c793869b-ee49-115b-a5b6-4fd21e8dedac INFO EVENT
{
  "key": "value"
}
2019-06-07T19:11:20.564Z c793869b-ee49-115b-a5b6-4fd21e8dedac WARN Event not processed.
END RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac
REPORT RequestId: c793869b-ee49-115b-a5b6-4fd21e8dedac Duration: 128.83 ms Billed
 Duration: 200 ms Memory Size: 128 MB Max Memory Used: 74 MB Init Duration: 166.62 ms
 XRAY TraceId: 1-5d9d007f-0a8c7fd02xmpl480aed55ef0 SegmentId: 3d752xmpl1bbe37e Sampled:
 true
```

Die Node.js-Laufzeit protokolliert die Zeilen `START`, `END`, und `REPORT` für jeden Aufruf. Sie fügt jedem von der Funktion protokollierten Eintrag einen Zeitstempel, eine Anforderungs-ID und eine Protokollebene hinzu. Die Berichtszeile enthält die folgenden Details.

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.

- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Sie können Protokolle in der Lambda-Konsole, in der CloudWatch Logs-Konsole oder über die Befehlszeile anzeigen.

Verwenden von Lambda-Optionen für die erweiterte Protokollierung mit Node.js

Um Ihnen mehr Kontrolle darüber zu geben, wie die Protokolle Ihrer Funktionen erfasst, verarbeitet und verwendet werden, können Sie die folgenden Protokollierungsoptionen für unterstützte Node.js-Laufzeiten konfigurieren:

- Protokollformat – Wählen Sie zwischen Klartext und einem strukturierten JSON-Format für die Protokolle Ihrer Funktion aus.
- Protokollebene — für Logs im JSON-Format wählen Sie die Detailebene der Logs, die Lambda an Amazon sendet CloudWatch, wie ERROR, DEBUG oder INFO
- Protokollgruppe — wählen Sie die CloudWatch Protokollgruppe aus, an die Ihre Funktion Protokolle sendet

Weitere Informationen zu diesen Protokollierungsoptionen und Anweisungen zur Konfiguration Ihrer Funktion für deren Verwendung finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.

Informationen zur Verwendung der Optionen für das Protokollformat und die Protokollebene mit Ihren Node.js-Lambda-Funktionen finden Sie in den folgenden Abschnitten.

Verwenden strukturierter JSON-Protokolle mit Node.js

Wenn Sie JSON für das Protokollformat Ihrer Funktion auswählen, sendet Lambda die Protokollausgabe mit den Konsolenmethoden`console.trace`,,`console.debug`, `console.log` `console.infoconsole.error`, und `console.warn` an CloudWatch als strukturiertes JSON. Jedes JSON-Protokollobjekt enthält mindestens vier Schlüssel-Wert-Paare mit den folgenden Schlüsseln:

- `"timestamp"` – die Uhrzeit, zu der die Protokollmeldung generiert wurde
- `"level"` – die der Meldung zugewiesene Protokollebene
- `"message"` – der Inhalt der Protokollmeldung
- `"requestId"` – die eindeutige Anforderungs-ID für den Funktionsaufruf

Abhängig von der Protokollierungsmethode, die Ihre Funktion verwendet, kann dieses JSON-Objekt auch zusätzliche Schlüsselpaare enthalten. Wenn Ihre Funktion beispielsweise `console`-Methoden verwendet, um Fehlerobjekte mit mehreren Argumenten zu protokollieren, enthält das JSON-Objekt zusätzliche Schlüssel-Wert-Paare mit den Schlüsseln `errorMessage`, `errorType` und `stackTrace`.

Wenn Ihr Code bereits eine andere Logging-Bibliothek wie Powertools for verwendet AWS Lambda, um strukturierte JSON-Logs zu erstellen, müssen Sie keine Änderungen vornehmen. Lambda codiert Protokolle, die bereits JSON-codiert sind, nicht doppelt, sodass die Anwendungsprotokolle Ihrer Funktion weiterhin wie zuvor erfasst werden.

Weitere Informationen zur Verwendung des Pakets Powertools for AWS Lambda Logging zur Erstellung strukturierter JSON-Logs in der Laufzeit von Node.js finden Sie unter. the section called “Protokollierung”

Beispiel für Protokollausgaben im JSON-Format

Die folgenden Beispiele zeigen, wie verschiedene Protokollausgaben, die mithilfe der `console` Methoden mit einzelnen und mehreren Argumenten generiert wurden, in CloudWatch Logs erfasst werden, wenn Sie das Protokollformat Ihrer Funktion auf JSON setzen.

Im ersten Beispiel wird die `console.error`-Methode verwendet, um eine einfache Zeichenfolge auszugeben.

Example Protokollcode für Node.js

```
export const handler = async (event) => {
  console.error("This is a warning message");
  ...
}
```

Example JSON-Protokolldatensatz

```
{
```

```
    "timestamp":"2023-11-01T00:21:51.358Z",
    "level":"ERROR",
    "message":"This is a warning message",
    "requestId":"93f25699-2cbf-4976-8f94-336a0aa98c6f"
}
```

Sie können mit den `console`-Methoden auch komplexere strukturierte Protokollnachrichten ausgeben, indem Sie entweder einzelne oder mehrere Argumente verwenden. Im nächsten Beispiel verwenden Sie `console.log`, um zwei Schlüssel-Wert-Paare mit einem einzigen Argument auszugeben. Beachten Sie, dass das `"message"` Feld im JSON-Objekt, das Lambda an CloudWatch Logs sendet, nicht stringifiziert ist.

Example Protokollcode für Node.js

```
export const handler = async (event) => {
  console.log({data: 12.3, flag: false});
  ...
}
```

Example JSON-Protokolldatensatz

```
{
    "timestamp": "2023-12-08T23:21:04.664Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": {
        "data": 12.3,
        "flag": false
    }
}
```

Im nächsten Beispiel verwenden Sie erneut die `console.log`-Methode, um eine Protokollausgabe zu erstellen. Diesmal verwendet die Methode zwei Argumente, eine Map mit zwei Schlüssel-Wert-Paaren und eine identifizierende Zeichenfolge. Beachten Sie, dass Lambda in diesem Fall das Feld `"message"` in eine Zeichenfolge umwandelt, da Sie zwei Argumente angegeben haben.

Example Protokollcode für Node.js

```
export const handler = async (event) => {
  console.log('Some object - ', {data: 12.3, flag: false});
  ...
```

```
}
```

Example JSON-Protokolldatensatz

```
{
    "timestamp": "2023-12-08T23:21:04.664Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": "Some object -  { data: 12.3, flag: false }"
}
```

Lambda weist Ausgaben, die mit `console.log` generiert wurden, der Protokollebene INFO zu.

Das letzte Beispiel zeigt, wie Fehlerobjekte mithilfe der Methoden in CloudWatch Logs ausgegeben werden können. `console` Beachten Sie, dass Lambda die Felder `errorMessage`, `errorType` und `stackTrace` zur Protokollausgabe hinzufügt, wenn Sie Fehlerobjekte mit mehreren Argumenten protokollieren.

Example Protokollcode für Node.js

```
export const handler = async (event) => {
  let e1 = new ReferenceError("some reference error");
  let e2 = new SyntaxError("some syntax error");
  console.log(e1);
  console.log("errors logged - ", e1, e2);
};
```

Example JSON-Protokolldatensatz

```
{
    "timestamp": "2023-12-08T23:21:04.632Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": {
        "errorType": "ReferenceError",
        "errorMessage": "some reference error",
        "stackTrace": [
            "ReferenceError: some reference error",
            "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
            "    at Runtime.handleOnceNonStreaming (file:///var/runtime/
index.mjs:1173:29)"
```

```
        ]
    }
}

{
    "timestamp": "2023-12-08T23:21:04.646Z",
    "level": "INFO",
    "requestId": "405a4537-9226-4216-ac59-64381ec8654a",
    "message": "errors logged -  ReferenceError: some reference error
\n    at Runtime.handler (file:///var/task/index.mjs:3:12)\n    at
 Runtime.handleOnceNonStreaming
    (file:///var/runtime/index.mjs:1173:29) SyntaxError: some syntax
 error\n    at Runtime.handler (file:///var/task/index.mjs:4:12)\n    at
 Runtime.handleOnceNonStreaming
    (file:///var/runtime/index.mjs:1173:29)",
    "errorType": "ReferenceError",
    "errorMessage": "some reference error",
    "stackTrace": [
        "ReferenceError: some reference error",
        "    at Runtime.handler (file:///var/task/index.mjs:3:12)",
        "    at Runtime.handleOnceNonStreaming (file:///var/runtime/index.mjs:1173:29)"
    ]
}
```

Bei der Protokollierung mehrerer Fehlertypen werden die zusätzlichen Felder `errorMessage`, `errorType` und `stackTrace` aus dem ersten Fehlertyp extrahiert, der an die `console`-Methode übergeben wurde.

Verwenden von Clientbibliotheken im Embedded Metric Format (EMF) mit strukturierten JSON-Protokollen

AWS stellt Open-Source-Clientbibliotheken für Node.js bereit, mit denen Sie Logs im Embedded Metric Format (EMF) erstellen können. Wenn Sie bereits über Funktionen verfügen, die diese Bibliotheken verwenden, und Sie das Protokollformat Ihrer Funktion in JSON ändern, werden die von Ihrem Code ausgegebenen Metriken CloudWatch möglicherweise nicht mehr erkannt.

Wenn Ihr Code derzeit EMF-Protokolle direkt mit `console.log` oder mithilfe von Powertools for AWS Lambda (TypeScript) ausgibt, können CloudWatch Sie diese auch nicht analysieren, wenn Sie das Protokollformat Ihrer Funktion in JSON ändern.

> **Important**
>
> Um sicherzustellen, dass die EMF-Protokolle Ihrer Funktionen weiterhin ordnungsgemäß analysiert werden, aktualisieren Sie Ihre EMF- und Powertools for CloudWatch -Bibliotheken auf die neuesten Versionen. AWS Lambda Wenn Sie zum JSON-Protokollformat wechseln, empfehlen wir Ihnen zudem, Tests durchzuführen, um die Kompatibilität mit den eingebetteten Metriken Ihrer Funktion sicherzustellen. Wenn Ihr Code EMF-Protokolle direkt mit `console.log` ausgibt, ändern Sie Ihren Code so, dass diese Metriken direkt in `stdout` ausgegeben werden, wie im folgenden Codebeispiel gezeigt.

Example Code, der eingebettete Metriken in **`stdout`** ausgibt

```
process.stdout.write(JSON.stringify(
    {
        "_aws": {
            "Timestamp": Date.now(),
            "CloudWatchMetrics": [{
                "Namespace": "lambda-function-metrics",
                "Dimensions": [["functionVersion"]],
                "Metrics": [{
                    "Name": "time",
                    "Unit": "Milliseconds",
                    "StorageResolution": 60
                }]
            }]
        },
        "functionVersion": "$LATEST",
        "time": 100,
        "requestId": context.awsRequestId
    }
) + "\n")
```

Verwenden der Filterung auf Protokollebene mit Node.js

AWS Lambda Um Ihre Anwendungsprotokolle nach ihrer Protokollebene zu filtern, muss Ihre Funktion Protokolle im JSON-Format verwenden. Sie können dies auf zwei Arten erreichen:

- Erstellen Sie Protokollausgaben mit den Standardmethoden der Konsole und konfigurieren Sie Ihre Funktion so, dass sie die JSON-Protokollformatierung verwendet. AWS Lambda filtert

dann Ihre Protokollausgaben mithilfe des Schlüsselwertpaars „Level“ im JSON-Objekt, wie unter beschriebenthe section called “Verwenden strukturierter JSON-Protokolle mit Node.js”. Informationen zur Konfiguration des Protokollformats Ihrer Funktion finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.

- Verwenden Sie eine andere Protokollierungsbibliothek oder Methode, um strukturierte JSON-Protokolle in Ihrem Code zu erstellen, die ein „level“-Schlüssel-Wert-Paar enthalten, das die Ebene der Protokollausgabe definiert. Sie können Powertools zum Beispiel verwenden, AWS Lambda um strukturierte JSON-Protokollausgaben aus Ihrem Code zu generieren. Weitere Informationen zur Verwendung von Powertools mit der Laufzeit Node.js finden Sie unter the section called “Protokollierung”.

  Damit Lambda die Protokolle Ihrer Funktion filtern kann, müssen Sie auch ein `"timestamp"`-Schlüssel-Wert-Paar in Ihre JSON-Protokollausgabe aufnehmen. Die Uhrzeit muss im gültigen RFC 3339-Zeitstempelformat angegeben werden. Wenn Sie keinen gültigen Zeitstempel angeben, weist Lambda dem Protokoll die Stufe INFO zu und fügt einen Zeitstempel für Sie hinzu.

Wenn Sie Ihre Funktion für die Filterung auf Protokollebene konfigurieren, wählen Sie aus den folgenden Optionen die Ebene der CloudWatch Protokolle aus AWS Lambda , die Sie an Logs senden möchten:

Protokollebene	Standardnutzung
TRACE (am detailliertesten)	Die detailliertesten Informationen, die verwendet werden, um den Ausführungspfad Ihres Codes nachzuverfolgen
DEBUG	Detaillierte Informationen für das System-De bugging
INFO	Meldungen, die den normalen Betrieb Ihrer Funktion erfassen
WARN	Meldungen über mögliche Fehler, die zu unerwartetem Verhalten führen können, wenn sie nicht behoben werden

Protokollebene	Standardnutzung
ERROR	Meldungen über Probleme, die verhindern, dass der Code wie erwartet funktioniert
FATAL (am wenigsten Details)	Meldungen über schwerwiegende Fehler, die dazu führen, dass die Anwendung nicht mehr funktioniert

Lambda sendet Protokolle der ausgewählten Stufe und niedriger bis CloudWatch. Wenn Sie beispielsweise die Protokollebene WARN konfigurieren, sendet Lambda Protokolle, die den Stufen WARN, ERROR und FATAL entsprechen.

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der Konsole CloudWatch

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Protokolle für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
```

```
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Instrumentierung von Node.js Code in AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS -Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von zwei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) — Eine sichere, produktionsbereite und AWS unterstützte Distribution des (OTel) SDK. OpenTelemetry
- AWS X-Ray-SDK for Node.js – Ein SDK zum Generieren und Senden von Nachverfolgungsdaten an X-Ray.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda SDKs sind Teil einer eng integrierten Instrumentierungslösung von. AWS Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Ablaufverfolgung in X-Ray mit beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS -Distro für Open Telemetry und X-Ray-SDKs.

Sections

- Interpretieren einer X-Ray-Nachverfolgung
- Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)

Verwenden von ADOT zur Instrumentierung Ihrer Node.js-Funktionen

ADOT bietet vollständig verwaltete Lambda-Ebenen, die alles packen, was Sie zum Sammeln von Telemetriedaten mit dem OTel-SDK benötigen. Indem Sie diese Ebene verwenden, können Sie Ihre Lambda-Funktionen instrumentieren, ohne einen Funktionscode ändern zu müssen. Sie können Ihren Ebenen auch für die benutzerdefinierte Initialisierung von OTel konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Konfiguration für den ADOT Collector auf Lambda in der ADOT-Dokumentation.

Für Node.js-Laufzeiten können Sie den AWS -verwalteten Lambda-Ebene für ADOT Javascript hinzufügen, um Ihre Funktionen automatisch zu instrumentieren. Eine ausführliche Anleitung zum Hinzufügen dieser Ebene finden Sie unter AWS Distro for OpenTelemetry Lambda Support for JavaScript in der ADOT-Dokumentation.

Verwenden des X-Ray-SDK zum Instrumentieren Ihrer Node.js-Funktionen

Um Details zu Aufrufen aufzuzeichnen, die Ihre Lambda-Funktion an andere Ressourcen in Ihrer Anwendung vornimmt, können Sie auch AWS X-Ray-SDK for Node.js verwenden. Um das SDK zu erhalten, fügen Sie das `aws-xray-sdk-core`-Paket den Abhängigkeiten Ihrer Anwendung hinzu.

Example blank-nodejs/package.json

```
{
  "name": "blank-nodejs",
  "version": "1.0.0",
  "private": true,
  "devDependencies": {
    "jest": "29.7.0"
  },
  "dependencies": {
    "@aws-sdk/client-lambda": "3.345.0",
    "aws-xray-sdk-core": "3.5.3"
  },
  "scripts": {
    "test": "jest"
  }
}
```

Um AWS SDK-Clients in Version 3 zu instrumentieren AWS SDK for JavaScript , schließen Sie die Client-Instanz mit der Methode ein. `captureAWSv3Client`

Example blank-nodejs/function/index.js — Einen AWS SDK-Client verfolgen

```
const AWSXRay = require('aws-xray-sdk-core');
const { LambdaClient, GetAccountSettingsCommand } = require('@aws-sdk/client-lambda');

// Create client outside of handler to reuse
const lambda = AWSXRay.captureAWSv3Client(new LambdaClient());

// Handler
exports.handler = async function(event, context) {
    event.Records.forEach(record => {
  ...
```

Die Lambda-Laufzeit legt zur Konfiguration des X-Ray-SDK einige Umgebungsvariablen fest. Beispielsweise setzt Lambda `AWS_XRAY_CONTEXT_MISSING` auf `LOG_ERROR`, um Laufzeitfehler aus dem X-Ray-SDK zu vermeiden. Um eine benutzerdefinierte Strategie für fehlenden Kontext festzulegen, überschreiben Sie die Umgebungsvariable in der Funktionskonfiguration so, dass sie keinen Wert aufweist. Dann können Sie die Strategie für fehlenden Kontext programmgesteuert festlegen.

Example Beispiel-Initialisierungscode

```
const AWSXRay = require('aws-xray-sdk-core');

// Configure the context missing strategy to do nothing
AWSXRay.setContextMissingStrategy(() => {});
```

Weitere Informationen finden Sie unter the section called “Konfigurieren von Umgebungsvariablen”.

Aktivieren Sie nach Hinzufügen der richtigen Abhängigkeiten die Nachverfolgung in der Konfiguration Ihrer Funktion über die Lambda-Konsole oder die API.

Aktivieren der Nachverfolgung mit der Lambda-Konsole

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

Aktivieren der Nachverfolgung mit der Lambda-API

Konfigurieren Sie die Ablaufverfolgung für Ihre Lambda-Funktion mit dem AWS CLI oder AWS SDK und verwenden Sie die folgenden API-Operationen:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Interpretieren einer X-Ray-Nachverfolgung

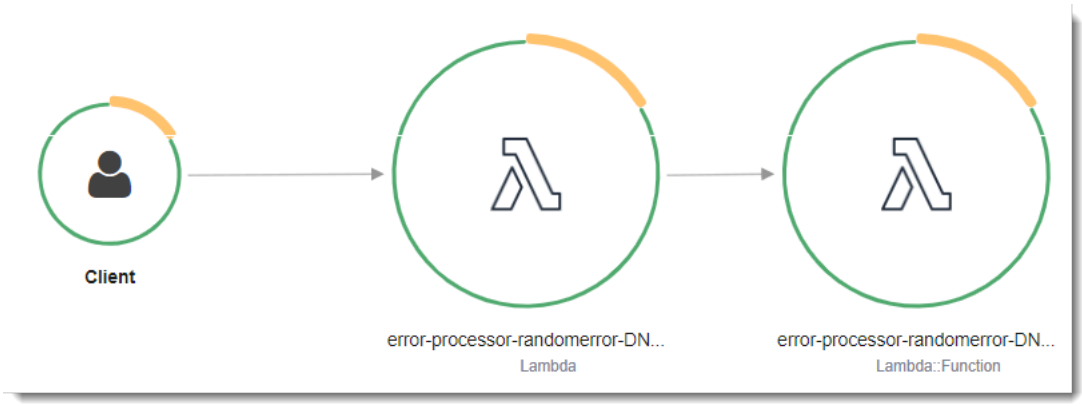
Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray.
Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

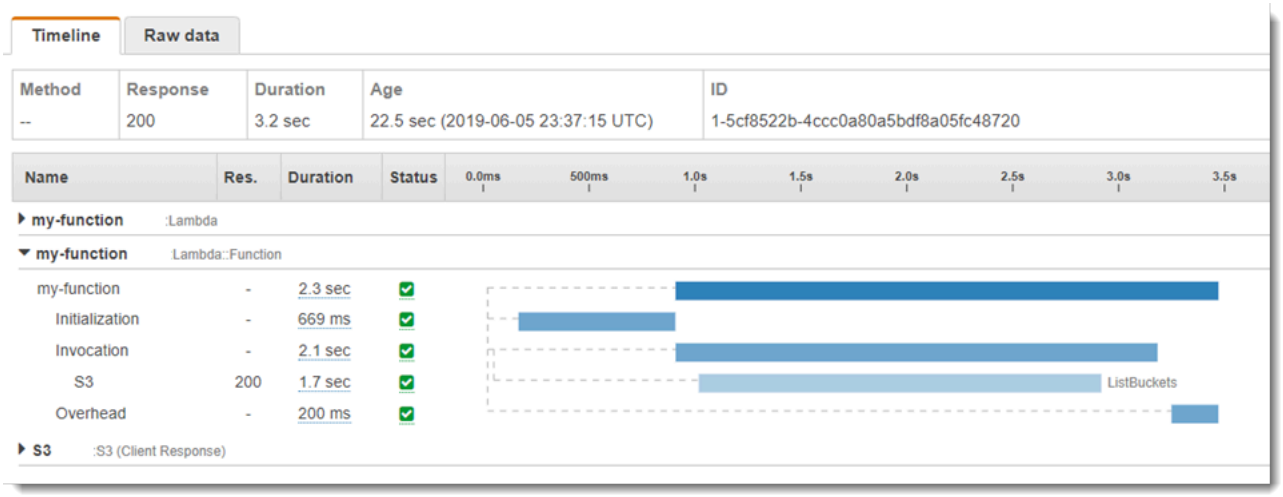
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.
- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter AWS X-Ray-SDK for Node.js im AWS X-Ray -Entwicklerhandbuch.

> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-

Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)

Wenn Sie das X-Ray-SDK verwenden, um AWS SDK-Clients Ihren Funktionscode zu instrumentieren, kann Ihr Bereitstellungspaket ziemlich umfangreich werden. Um Laufzeitabhängigkeiten bei jeder Aktualisierung des Funktionscodes zu vermeiden, verpacken Sie das X-Ray-SDK in einer Lambda-Ebene.

Das folgende Beispiel zeigt eine `AWS::Serverless::LayerVersion`-Ressource, die das AWS X-Ray-SDK for Node.js speichert.

Example template.yml – Abhängigkeitenebene

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-nodejs-lib
      Description: Dependencies for the blank sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - nodejs16.x
```

Bei dieser Konfiguration aktualisieren Sie die Bibliotheksebene nur, wenn Sie Ihre Laufzeitabhängigkeiten ändern. Da das Funktionsbereitstellungspaket nur Ihren Code enthält, kann dies dazu beitragen, die Upload-Zeiten zu reduzieren.

Das Erstellen einer Ebene für Abhängigkeiten erfordert Build-Konfigurationsänderungen, um das Ebenen-Archiv vor der Bereitstellung zu generieren. Ein funktionierendes Beispiel finden Sie in der Beispielanwendung blank-nodejs .

Aufbau von Lambda-Funktionen mit TypeScript

Sie können die Laufzeit von Node.js verwenden, um TypeScript Code darin AWS Lambda auszuführen. Da Node.js TypeScript Code nicht nativ ausführt, müssen Sie Ihren TypeScript Code zuerst in das Format transpilieren. JavaScript Verwenden Sie dann die JavaScript Dateien, um Ihren Funktionscode für Lambda bereitzustellen. Ihr Code wird in einer Umgebung ausgeführt, die das AWS SDK für enthält JavaScript, mit Anmeldeinformationen aus einer AWS Identity and Access Management (IAM-) Rolle, die Sie verwalten. Weitere Informationen zu den SDK-Versionen, die in den Laufzeiten von Node.js enthalten sind, finden Sie unter. the section called “SDK-Versionen, die Runtime enthalten”

Lambda unterstützt die folgenden Node.js-Laufzeiten.

Node.js

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Node.js 20	`nodejs20.x`	Amazon Linux 2023			
Node.js 18	`nodejs18.x`	Amazon Linux 2			
Node.js 16	`nodejs16.x`	Amazon Linux 2	12. Juni 2024	28. Februar 2025	31. März 2025

Themen

Einrichtung einer TypeScript Entwicklungsumgebung

Verwenden Sie eine lokale integrierte Entwicklungsumgebung (IDE), einen Texteditor oder AWS Cloud9um Ihren TypeScript Funktionscode zu schreiben. Sie können auf der Lambda-Konsole keinen TypeScript Code erstellen.

Um Ihren TypeScript Code zu transpilieren, richten Sie einen Compiler wie esbuild oder Microsofts TypeScript Compiler (`tsc`) ein, der im Lieferumfang der Distribution enthalten ist. TypeScript Sie können das AWS Serverless Application Model (AWS SAM) oder das verwenden, um das Erstellen und Bereitstellen von Code AWS Cloud Development Kit (AWS CDK)zu vereinfachen. TypeScript Beide Tools verwenden Esbuild, um TypeScript Code zu transpilieren. JavaScript

Wenn Sie esbuild verwenden, beachten Sie Folgendes:

- Es gibt mehrere VorbehalteTypeScript .
- Sie müssen Ihre TypeScript Transpilationseinstellungen so konfigurieren, dass sie der Laufzeit von Node.js entsprechen, die Sie verwenden möchten. Weitere Informationen finden Sie unter Ziel in der esbuild-Dokumentation. Ein Beispiel für eine tsconfig.json-Datei, die zeigt, wie Sie auf eine bestimmte, von Lambda unterstützte Version von Node.js abzielen, finden Sie im Repository. TypeScript GitHub
- esbuild führt keine Typ-Überprüfungen durch. Um Typen zu überprüfen, verwenden Sie den `tsc`-Compiler. Führen Sie `tsc -noEmit` aus oder fügen Sie einen `"noEmit"`-Parameter zu Ihrer tsconfig.json-Datei hinzu, wie im folgenden Beispiel gezeigt. Dies ist so konfiguriert`tsc`, dass keine Dateien ausgegeben werden. JavaScript Verwenden Sie nach der Überprüfung der Typen Esbuild, um die TypeScript Dateien in zu konvertieren. JavaScript

Example tsconfig.json

```
{
 "compilerOptions": {
   "target": "es2020",
   "strict": true,
   "preserveConstEnums": true,
   "noEmit": true,
   "sourceMap": false,
   "module":"commonjs",
   "moduleResolution":"node",
   "esModuleInterop": true,
   "skipLibCheck": true,
```

```
    "forceConsistentCasingInFileNames": true,
    "isolatedModules": true,
  },
  "exclude": ["node_modules", "**/*.test.ts"]
}
```

Definieren Sie den Lambda-Funktionshandler in TypeScript

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Example TypeScript Handler

Diese Beispielfunktion protokolliert den Inhalt des Ereignisobjekts und gibt den Speicherort der Protokolle zurück. Beachten Sie Folgendes:

- Bevor Sie diesen Code in einer Lambda-Funktion verwenden, müssen Sie das Paket @types/aws-lambda als Entwicklungsabhängigkeit hinzufügen. Dieses Paket enthält die Typdefinitionen für Lambda. Bei der Installation von `@types/aws-lambda` importiert die `import`-Anweisung (`import ... from 'aws-lambda'`) die Typdefinitionen. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im Repository. DefinitelyTyped GitHub
- Der Handler in diesem Beispiel ist ein ES-Modul und muss in der Datei `package.json` oder mithilfe der Dateierweiterung `.mjs` entsprechend angegeben werden. Weitere Informationen hierzu finden Sie unter Designieren eines Funktionshandlers als ES-Modul.

```
import { Handler } from 'aws-lambda';

export const handler: Handler = async (event, context) => {
    console.log('EVENT: \n' + JSON.stringify(event, null, 2));
    return context.logStreamName;
};
```

Die Laufzeit übergibt Argumente an die Handler-Methode. Das erste Argument ist das Objekt `event`, das Informationen aus dem Aufrufer enthält. Der Aufrufer übergibt diese Informationen als Zeichenfolge im JSON-Format, wenn er Invoke, aufruft, und die Laufzeit konvertiert sie in ein Objekt. Wenn ein AWS Dienst Ihre Funktion aufruft, variiert die Ereignisstruktur je nach Dienst. Wir empfehlen TypeScript, Typanmerkungen für das Ereignisobjekt zu verwenden. Weitere Informationen finden Sie unter Typen für das Ereignisobjekt verwenden.

Das zweite Argument ist das Context-Objekt, das Informationen über den Aufruf, die Funktion und die Ausführungsumgebung enthält. Im vorherigen Beispiel ruft die Funktion den Namen des Protokollstreams aus dem Context-Objekt ab und gibt ihn an den Aufrufer zurück.

Sie können ein Callback-Argument verwenden, ist eine Funktion, die Sie in nicht-asynchronen Handlern aufrufen können, um eine Antwort zu senden. Wir empfehlen Ihnen, Async/Await anstelle von Callback zu verwenden. Async/Await bietet eine verbesserte Lesbarkeit, Fehlerbehandlung und Effizienz. Weitere Informationen zu den Unterschieden zwischen Async/Await und Callbacks finden Sie unter Callbacks verwenden.

Verwenden von async/await

Wenn Ihr Code eine asynchrone Aufgabe ausführt, verwenden Sie das Async-/Await, um sicherzustellen, dass die Ausführung des Handler beendet wird. Async/Await ist eine präzise und lesbare Methode, um asynchronen Code in Node.js zu schreiben, ohne dass verschachtelte Callbacks oder Verkettungsversprechen erforderlich sind. Mit Async/Await können Sie Code schreiben, der sich wie synchroner Code liest, aber dennoch asynchron und blockierungsfrei ist.

Das `async`-Schlüsselwort kennzeichnet eine Funktion als asynchron, und das `await`-Schlüsselwort unterbricht die Ausführung der Funktion, bis `Promise` aufgelöst ist.

Example TypeScript Funktion — asynchron

In diesem Beispiel wird `fetch` verwendet, das in der `nodejs18.x`-Laufzeit verfügbar ist. Beachten Sie Folgendes:

- Bevor Sie diesen Code in einer Lambda-Funktion verwenden, müssen Sie das Paket @types/aws-lambda als Entwicklungsabhängigkeit hinzufügen. Dieses Paket enthält die Typdefinitionen für Lambda. Bei der Installation von `@types/aws-lambda` importiert die `import`-Anweisung (`import ... from 'aws-lambda'`) die Typdefinitionen. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im Repository. DefinitelyTyped GitHub
- Der Handler in diesem Beispiel ist ein ES-Modul und muss in der Datei `package.json` oder mithilfe der Dateierweiterung `.mjs` entsprechend angegeben werden. Weitere Informationen hierzu finden Sie unter Designieren eines Funktionshandlers als ES-Modul.

```
import { APIGatewayProxyEvent, APIGatewayProxyResult } from 'aws-lambda';
const url = 'https://aws.amazon.com/';
export const lambdaHandler = async (event: APIGatewayProxyEvent):
 Promise<APIGatewayProxyResult> => {
    try {
        // fetch is available with Node.js 18
        const res = await fetch(url);
```

```
        return {
            statusCode: res.status,
            body: JSON.stringify({
                message: await res.text(),
            }),
        };
    } catch (err) {
        console.log(err);
        return {
            statusCode: 500,
            body: JSON.stringify({
                message: 'some error happened',
            }),
        };
    }
};
```

Callbacks verwenden

Wir empfehlen, dass Sie Async/Await verwenden, um den Funktionshandler zu deklarieren, anstatt Callbacks zu verwenden. Async/Await ist aus mehreren Gründen eine bessere Wahl:

- Lesbarkeit: Async/Await-Code ist einfacher zu lesen und zu verstehen als Callback-Code, der schnell schwer zu verstehen sein kann und in die Callback-Hölle führen kann.
- Debugging und Fehlerbehandlung: Das Debuggen von Callback-basiertem Code kann schwierig sein. Der Aufrufliste kann schwer zu folgen sein und Fehler können leicht verschluckt werden. Mit Async/Await können Sie Try/Catch-Blöcke verwenden, um Fehler zu behandeln.
- Effizienz: Callbacks erfordern oft das Umschalten zwischen verschiedenen Teilen des Codes. Async/Await kann die Anzahl der Kontextwechsel reduzieren, was zu effizienterem Code führt.

Wenn Sie in Ihrem Handler verwenden, wird die Funktion so lange ausgeführt, bis die Ereignisschleife leer ist oder eine Zeitüberschreitung auftritt. Die Antwort wird erst an den Aufrufer gesendet, wenn alle Ereignisschleifenaufgaben abgeschlossen sind. Wenn eine Zeitüberschreitung der Funktion auftritt, wird stattdessen ein Fehler zurückgegeben. Sie können die Laufzeit so konfigurieren, dass die Antwort sofort gesendet wird, indem Sie context.callback Loop auf false WaitsFor EmptyEvent setzen.

Die Callback-Funktion verwendet zwei Argumente, einen `Error` und eine Antwort. Das Response-Objekt muss mit kompatibel sei `JSON.stringify`.

Example TypeScript Funktion mit Callback

Diese Beispielfunktion empfängt ein Ereignis von Amazon API Gateway, protokolliert die Ereignis- und Kontextobjekte und gibt dann eine Antwort an API Gateway zurück. Beachten Sie Folgendes:

- Bevor Sie diesen Code in einer Lambda-Funktion verwenden, müssen Sie das Paket @types/aws-lambda als Entwicklungsabhängigkeit hinzufügen. Dieses Paket enthält die Typdefinitionen für Lambda. Bei der Installation von `@types/aws-lambda` importiert die `import`-Anweisung (`import ... from 'aws-lambda'`) die Typdefinitionen. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im Repository. DefinitelyTyped GitHub
- Der Handler in diesem Beispiel ist ein ES-Modul und muss in der Datei `package.json` oder mithilfe der Dateierweiterung `.mjs` entsprechend angegeben werden. Weitere Informationen hierzu finden Sie unter Designieren eines Funktionshandlers als ES-Modul.

```
import { Context, APIGatewayProxyCallback, APIGatewayEvent } from 'aws-lambda';

export const lambdaHandler = (event: APIGatewayEvent, context: Context, callback:
 APIGatewayProxyCallback): void => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    callback(null, {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
        }),
    });
};
```

Typen für das Ereignisobjekt verwenden

Wir empfehlen, dass Sie keinen Typ für die Handler-Argumente und den Rückgabetyp verwenden, da Sie die Möglichkeit verlieren, Typen zu überprüfen. Generieren Sie stattdessen ein Ereignis mit demselben lokalen AWS Serverless Application Model CLI-Befehl generate-event oder verwenden Sie eine Open-Source-Definition aus dem Paket @types /aws-lambda.

Generieren eines Ereignisses mit dem Befehl sam local generate-event

1. Generieren Sie ein Amazon Simple Storage Service (Amazon S3)-Proxy-Ereignis.

```
sam local generate-event s3 put >> S3PutEvent.json
```

2. Verwenden Sie das Quicktype-Hilfsprogramm, um Typdefinitionen aus der S3-.json-Datei zu generieren. PutEvent

```
npm install -g quicktype
quicktype S3PutEvent.json -o S3PutEvent.ts
```

3. Verwenden Sie die generierten Typen in Ihrem Code.

```
import { S3PutEvent } from './S3PutEvent';

export const lambdaHandler = async (event: S3PutEvent): Promise<void> => {
  event.Records.map((record) => console.log(record.s3.object.key));
};
```

Generieren eines Ereignisses mit einer Open-Source-Definition aus dem @types/aws-lambda-Paket

1. Fügen Sie das @types/aws-lambda-Paket als Entwicklungsabhängigkeit hinzu.

```
npm install -D @types/aws-lambda
```

2. Verwenden Sie die Typen in Ihrem Code.

```
import { S3Event } from "aws-lambda";

export const lambdaHandler = async (event: S3Event): Promise<void> => {
  event.Records.map((record) => console.log(record.s3.object.key));
};
```

Bereitstellen von transpiliertem TypeScript Code in Lambda mit ZIP-Dateiarchiven

Bevor Sie TypeScript Code in bereitstellen könnenAWS Lambda, müssen Sie ihn in transpilieren JavaScript. Auf dieser Seite werden drei Möglichkeiten zum Erstellen und Bereitstellen von TypeScript Code in Lambda mit ZIP-Dateiarchiven erläutert:

- Verwenden von AWS Serverless Application Model (AWS SAM)
- Verwendung von AWS Cloud Development Kit (AWS CDK)
- Verwendung der AWS Command Line Interface (AWS CLI) und esbuild

AWS SAM und AWS CDK vereinfachen das Erstellen und Bereitstellen von TypeScript Funktionen. Die AWS SAM-Vorlagenspezifikation bietet eine einfache und saubere Syntax zur Beschreibung der Lambda-Funktionen, APIs, Berechtigungen, Konfigurationen und Ereignisse, aus denen Ihre Serverless-Anwendung besteht. Über das AWS CDK Sie können zuverlässige, skalierbare und kostengünstige Anwendungen in der Cloud mit der beträchtlichen Ausdruckskraft einer Programmiersprache erstellen. Das AWS CDK ist für mäßig bis sehr erfahrene AWS-Benutzer geplant. Sowohl das als auch AWS CDK das AWS SAM verwenden esbuild, um TypeScript Code in zu transpilieren JavaScript.

Verwenden von AWS SAM zum Bereitstellen von TypeScript Code in Lambda

Führen Sie die folgenden Schritte aus, um eine Hello-World- TypeScript Beispielanwendung mit der herunterzuladen, zu erstellen und bereitzustellenAWS SAM. Diese Anwendung implementiert ein grundlegendes API-Backend. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anforderung an den API-Gateway-Endpunkt senden, wird die Lambda-Funktion aufgerufen. Die Funktion gibt eine `hello world`-Nachricht zurück.

> **Note**
>
> AWS SAM verwendet esbuild, um Node.js-Lambda-Funktionen aus dem TypeScript Code zu erstellen. Die esbuild-Unterstützung befindet sich derzeit in der öffentlichen Vorschau. Während der öffentlichen Vorschau kann der esbuild-Support Änderungen unterliegen, die nicht mehr rückwärtskompatibel sind.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS CLI Version 2
- AWS SAM-CLI-Version 1.75 oder höher
- Node.js 18.x

Bereitstellen einer AWS SAM-Beispielanwendung

1. Initialisieren Sie die Anwendung mit der Hello World- TypeScript Vorlage.

```
sam init --app-template hello-world-typescript --name sam-app --package-type Zip --runtime nodejs18.x
```

2. (Optional) Die Beispielanwendung enthält Konfigurationen für häufig verwendete Tools wie eslLint für Code-Linting und Jest für Einheitentests. So führen Sie Lint- und Testbefehle aus:

```
cd sam-app/hello-world
npm install
npm run lint
npm run test
```

3. Entwickeln Sie die App.

```
cd sam-app
sam build
```

4. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

5. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, antworten Sie mit `Enter`.
6. Die Ausgabe zeigt den Endpunkt für die REST-API. Öffnen Sie den Endpunkt in einem Browser, um die Funktion zu testen. Folgende Antwort sollte angezeigt werden:

```
{"message":"hello world"}
```

7. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwenden der AWS CDK zum Bereitstellen von TypeScript Code in Lambda

Führen Sie die folgenden Schritte aus, um eine TypeScript Beispielanwendung mithilfe der zu erstellen und bereitzustellenAWS CDK. Diese Anwendung implementiert ein grundlegendes API-Backend. Es besteht aus einem API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anforderung an den API-Gateway-Endpunkt senden, wird die Lambda-Funktion aufgerufen. Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS CLI Version 2
- AWS CDK Version 2
- Node.js 18.x
- Entweder Docker oder esbuild

Bereitstellen einer AWS CDK-Beispielanwendung

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie die App.

```
cdk init app --language typescript
```

3. Fügen Sie das @types/aws-lambda-Paket als Entwicklungsabhängigkeit hinzu. Dieses Paket enthält die Typdefinitionen für Lambda.

```
npm install -D @types/aws-lambda
```

4. Öffnen Sie das lib-Verzeichnis. Sie sollten eine Datei mit dem Namen hello-world-stack.ts sehen. Erstellen Sie neue zwei neue Dateien in diesem Verzeichnis: hello-world.function.ts und hello-world.ts.
5. Öffnen Sie hello-world.function.ts und fügen Sie den folgenden Code in die Datei ein. Dies ist der Code für die Lambda-Funktion.

> **Note**
>
> Die `import`-Anweisung importiert die Typdefinitionen aus @types/aws-lambda. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im DefinitelyTyped GitHub Repository.

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    return {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
        }),
    };
};
```

6. Öffnen Sie hello-world.ts und fügen Sie den folgenden Code in die Datei ein. Dies enthält das NodejsFunction Konstrukt , das die Lambda-Funktion erstellt, und das LambdaRestApi Konstrukt , das die REST-API erstellt.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';

export class HelloWorld extends Construct {
```

```
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function');
    new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
  }
}
```

Das `NodejsFunction`-Konstrukt geht standardmäßig von folgendem aus:

- Ihr Funktions-Handler heißt `handler`.
- Die .ts-Datei, die den Funktionscode enthält (hello-world.function.ts), befindet sich im selben Verzeichnis wie die .ts-Datei, die das Konstrukt (hello-world.ts) enthält. Das Konstrukt verwendet die ID des Konstrukts („hello-world“) und den Namen der Lambda-Handler-Datei („function“), um den Funktionscode zu finden. Wenn sich Ihr Funktionscode beispielsweise in einer Datei namens hello-world.my-function.ts befindet, muss die Datei hello-world.ts wie folgt auf den Funktionscode verweisen:

  ```
  const helloFunction = new NodejsFunction(this, 'my-function');
  ```

Sie können dieses Verhalten ändern und andere esbuild-Parameter konfigurieren. Weitere Informationen finden Sie unter esbuild konfigurieren in der AWS CDK-API-Referenz.

7. Öffnen Sie hello-world-stack.ts . Dies ist der Code, der Ihren AWS CDK-Stack definiert. Ersetzen Sie den Code mit Folgendem:

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

8. Stellen Sie Ihre Anwendung aus dem Verzeichnis `hello-world` bereit, das Ihre `cdk.json` Datei enthält.

```
cdk deploy
```

9. Das AWS CDK erstellt und packt die Lambda-Funktion mit esbuild und stellt die Funktion dann für die Lambda-Laufzeit bereit. Die Ausgabe zeigt den Endpunkt für die REST-API. Öffnen Sie den Endpunkt in einem Browser, um die Funktion zu testen. Folgende Antwort sollte angezeigt werden:

   ```
   {"message":"hello world"}
   ```

   Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

Verwenden von AWS CLI und esbuild zum Bereitstellen von TypeScript Code in Lambda

Das folgende Beispiel zeigt, wie Code mithilfe von esbuild und in TypeScript Lambda transpiliert und bereitgestellt wirdAWS CLI. esbuild erzeugt eine JavaScript Datei mit allen Abhängigkeiten. Dies ist die einzige Datei, die Sie dem ZIP-Archiv hinzufügen müssen.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS CLI Version 2
- Node.js 18.x
- Eine Ausführungsrolle für die Lambda-Funktion
- Für Windows-Benutzer ein ZIP-Datei-Hilfsprogramm wie 7zip.

Bereitstellen einer Beispielfunktion

1. Erstellen Sie auf Ihrem lokalen Computer ein Projektverzeichnis für Ihre neue Funktion.
2. Erstellen Sie ein neues Node.js Projekt mit npm oder einem Paketmanager Ihrer Wahl.

   ```
   npm init
   ```

3. Fügen Sie die Pakete @types /aws-lambda und esbuild als Entwicklungsabhängigkeiten hinzu. Das `@types/aws-lambda`-Paket enthält die Typdefinitionen für Lambda.

```
npm install -D @types/aws-lambda esbuild
```

4. Erstellen Sie eine neue Datei mit dem Namen index.ts. Fügen Sie den folgenden Code zur Datei hinzu. Dies ist der Code für die Lambda-Funktion. Die Funktion gibt eine `hello world`-Nachricht zurück. Die Funktion erstellt keine API-Gateway-Ressourcen.

> **Note**
>
> Die `import`-Anweisung importiert die Typdefinitionen aus @types/aws-lambda. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im DefinitelyTyped GitHub Repository.

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  console.log(`Event: ${JSON.stringify(event, null, 2)}`);
  console.log(`Context: ${JSON.stringify(context, null, 2)}`);
  return {
      statusCode: 200,
      body: JSON.stringify({
          message: 'hello world',
      }),
   };
};
```

5. Hinzufügen eines Entwicklungs-Skripts zur package.json-Datei. Dies konfiguriert esbuild so, dass das ZIP-Bereitstellungspaket automatisch erstellt wird. Weitere Informationen finden Sie unter Entwicklungs-Skripte in der esbuild-Dokumentation.

   Linux and MacOS

```
"scripts": {
  "prebuild": "rm -rf dist",
```

```
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
target=es2020 --outfile=dist/index.js",
  "postbuild": "cd dist && zip -r index.zip index.js*"
},
```

Windows

In diesem Beispiel verwendet der `"postbuild"` Befehl das 7zip-Hilfsprogramm, um Ihre ZIP-Datei zu erstellen. Verwenden Sie Ihr bevorzugtes Windows-ZIP-Hilfsprogramm und ändern Sie den Befehl nach Bedarf.

```
"scripts": {
  "prebuild": "del /q dist",
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
target=es2020 --outfile=dist/index.js",
  "postbuild": "cd dist && 7z a -tzip index.zip index.js*"
},
```

6. Erstellen Sie das Paket.

```
npm run build
```

7. Erstellen Sie eine Lambda-Funktion mit dem ZIP-Bereitstellungspaket. Ersetzen Sie den markierten Text durch den Amazon-Ressourcennamen (ARN) Ihrer Ausführungsrolle.

```
aws lambda create-function --function-name hello-world --runtime "nodejs18.x" --
role arn:aws:iam::123456789012:role/lambda-ex --zip-file "fileb://dist/index.zip"
 --handler index.handler
```

8. Führen Sie ein Testereignis aus, um zu bestätigen, dass die Funktion die folgende Antwort zurückgibt. Wenn Sie diese Funktion mit API Gateway aufrufen möchten, Erstellen und Konfigurieren Sie eine REST-API.

```
{
  "statusCode": 200,
  "body": "{\"message\":\"hello world\"}"
}
```

Stellen Sie transpilierten TypeScript Code in Lambda mit Container-Images bereit

Sie können Ihren TypeScript Code als Container-Image für Node.js in einer AWS Lambda Funktion bereitstellen. AWS stellt Basis-Images für Node.js bereit, um Ihnen bei der Erstellung des Container-Images zu helfen. Diese Basis-Images sind mit einer Sprachlaufzeit und anderen Komponenten, die für die Ausführung des Images auf Lambda erforderlich sind, vorinstalliert. AWS stellt für jedes der Basis-Images ein Dockerfile bereit, das Sie beim Erstellen Ihres Container-Images unterstützt.

Wenn Sie ein Community- oder Privatunternehmens-Basis-Image verwenden, müssen Sie den Node.js-Laufzeitschnittstellen-Client (RIC) zum Basis-Image hinzufügen, um es mit Lambda kompatibel zu machen.

Lambda bietet einen Emulator für die Laufzeitschnittstelle zum lokalen Testen. Die AWS Basis-Images für Node.js enthalten den Runtime-Interface-Emulator. Wenn Sie ein alternatives Basis-Image verwenden (beispielsweise ein Alpine Linux-Image oder ein Debian-Image), können Sie den Emulator in Ihr Image integrieren oder ihn auf Ihrem lokalen Computer installieren.

Verwenden eines Node.js -Basisimages zum Erstellen und Verpacken von TypeScript Funktionscode

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker
- Node.js 18.x

Erstellen eines Images aus einem Base Image

Um ein Image aus einem AWS Basis-Image für Lambda zu erstellen

1. Erstellen Sie auf Ihrem lokalen Computer ein Projektverzeichnis für Ihre neue Funktion.
2. Erstellen Sie ein neues Node.js-Projekt mit `npm` oder einem Paketmanager Ihrer Wahl.

```
npm init
```

3. Fügen Sie die Pakete @types/aws-lambda und esbuild als Entwicklungsabhängigkeiten hinzu. Das `@types/aws-lambda`-Paket enthält die Typdefinitionen für Lambda.

```
npm install -D @types/aws-lambda esbuild
```

4. Hinzufügen eines Entwicklungs-Skripts zur `package.json`-Datei.

```
  "scripts": {
  "build": "esbuild index.ts --bundle --minify --sourcemap --platform=node --
target=es2020 --outfile=dist/index.js"
}
```

5. Erstellen Sie eine neue Datei mit dem Namen `index.ts`. Fügen Sie den folgenden Beispiel-Code zur neuen Datei hinzu. Dies ist der Code für die Lambda-Funktion. Die Funktion gibt eine `hello world`-Nachricht zurück.

> **Note**
>
> Die `import`-Anweisung importiert die Typdefinitionen aus @types/aws-lambda. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im Repository. DefinitelyTyped GitHub

```
import { Context, APIGatewayProxyResult, APIGatewayEvent } from 'aws-lambda';

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
    console.log(`Event: ${JSON.stringify(event, null, 2)}`);
    console.log(`Context: ${JSON.stringify(context, null, 2)}`);
    return {
        statusCode: 200,
        body: JSON.stringify({
            message: 'hello world',
        }),
    };
};
```

6. Erstellen Sie eine neue Docker-Datei mit der folgenden Konfiguration:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.

- Legen Sie das `CMD`-Argument zur Angabe des Lambda-Funktionshandlers fest.

Example Dockerfile

Die folgende Docker-Datei verwendet eine mehrstufige Entwicklung. Der erste Schritt transpiliert den Code in. TypeScript JavaScript Im zweiten Schritt wird ein Container-Image erstellt, das nur JavaScript Dateien und Produktionsabhängigkeiten enthält.

```
FROM public.ecr.aws/lambda/nodejs:18 as builder
WORKDIR /usr/app
COPY package.json index.ts  ./
RUN npm install
RUN npm run build

FROM public.ecr.aws/lambda/nodejs:18
WORKDIR ${LAMBDA_TASK_ROOT}
COPY --from=builder /usr/app/dist/* ./
CMD ["index.handler"]
```

7. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. In diesem Beispiel ist `docker-image` der Image-Name und `test` der Tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis an den lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:
   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR

verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

AWS Lambda -Kontextobjekt in TypeScript

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Methoden

- `getRemainingTimeInMillis()` – Gibt die Anzahl der verbleibenden Millisekunden zurück, bevor die Ausführung das Zeitlimit überschreitet.

Context-Eigenschaften

- `functionName` – Der Name der Lambda-Funktion.
- `functionVersion` – Die Version der Funktion.
- `invokedFunctionArn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `memoryLimitInMB` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `awsRequestId` – Der Bezeichner der Aufrufanforderung.
- `logGroupName` – Protokollgruppe für die Funktion.
- `logStreamName` – Der Protokollstream für die Funktions-Instance.
- `identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
  - `cognitoIdentityId`— Die authentifizierte Amazon-Cognito-Identität.
  - `cognitoIdentityPoolId` – Der Amazon-Cognito-Identitätspool, der den Aufruf autorisiert hat.
- `clientContext` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`
  - `client.app_package_name`
  - `env.platform_version`
  - `env.platform`

  - `env.make`
  - `env.model`
  - `env.locale`
  - `Custom` – Benutzerdefinierte Werte, die durch die mobilen Anwendung festgelegt werden.
- `callbackWaitsForEmptyEventLoop` – Legen Sie den Wert auf „false“ fest, um die Antwort direkt zu senden, wenn der Rückruf ausgeführt wird, anstatt zu warten, bis die Node.js-Ereignisschleife leer ist. Bei „false“ werden alle ausstehenden Ereignisse während des nächsten Aufrufs weiter ausgeführt.

Sie können das @types/aws-lambda npm-Paket verwenden, um mit dem Kontextobjekt zu arbeiten.

Example Datei index.js

Die folgende Beispielfunktion protokolliert Kontextinformationen und gibt den Speicherort der Protokolle zurück.

> **Note**
>
> Bevor Sie diesen Code in einer Lambda-Funktion verwenden, müssen Sie das Paket @types/aws-lambda als Entwicklungsabhängigkeit hinzufügen. Dieses Paket enthält die Typdefinitionen für Lambda. Bei der Installation von `@types/aws-lambda` importiert die `import`-Anweisung (`import ... from 'aws-lambda'`) die Typdefinitionen. Das `aws-lambda`-NPM-Paket wird nicht importiert, da es sich um ein unabhängiges Tool eines Drittanbieters handelt. Weitere Informationen finden Sie unter aws-lambda im DefinitelyTyped GitHub Repository.

```
import { Context } from 'aws-lambda';
export const lambdaHandler = async (event: string, context: Context): Promise<string>
 => {
  console.log('Remaining time: ', context.getRemainingTimeInMillis());
  console.log('Function name: ', context.functionName);
  return context.logStreamName;
};
```

AWS Lambda Funktion einloggen TypeScript

AWS Lambda überwacht automatisch Lambda-Funktionen und sendet Protokolleinträge an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen zu CloudWatch Logs finden Sie unterVerwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Um Protokolle aus Ihrem Funktionscode auszugeben, können Sie Methoden auf dem Konsolenobjekt verwenden. Für eine detailliertere Protokollierung können Sie jede Protokollierungsbibliothek verwenden, die in `stdout` oder `stderr` schreibt.

Sections

- Tools und Bibliotheken
- Verwendung von Powertools für AWS Lambda (TypeScript) und für die strukturierte Protokollierung AWS SAM
- Verwenden Sie Powertools für AWS Lambda (TypeScript) und AWS CDK für die strukturierte Protokollierung
- Verwenden von Lambda-Konsole
- Verwenden der CloudWatch Konsole

Tools und Bibliotheken

Powertools for AWS Lambda (TypeScript) ist ein Entwickler-Toolkit zur Implementierung von Best Practices für Serverless und zur Steigerung der Entwicklergeschwindigkeit. Das Logger-Serviceprogramm bietet einen für Lambda optimierten Logger, der zusätzliche Informationen über den Funktionskontext all Ihrer Funktionen enthält, wobei die Ausgabe als JSON strukturiert ist. Mit diesem Serviceprogramm können Sie Folgendes tun:

- Erfassung von Schlüsselfeldern aus dem Lambda-Kontext, Kaltstart und Strukturen der Protokollierungsausgabe als JSON
- Protokollieren Sie Ereignisse von Lambda-Aufrufen, wenn Sie dazu aufgefordert werden (standardmäßig deaktiviert)
- Alle Protokolle nur für einen bestimmten Prozentsatz der Aufrufe über Protokollstichproben drucken (standardmäßig deaktiviert)

- Fügen Sie dem strukturierten Protokoll zu einem beliebigen Zeitpunkt zusätzliche Schlüssel hinzu
- Verwenden Sie einen benutzerdefinierten Protokollformatierer (Bring Your Own Formatter), um Protokolle in einer Struktur auszugeben, die mit dem Logging RFC Ihres Unternehmens kompatibel ist

Verwendung von Powertools für AWS Lambda (TypeScript) und für die strukturierte Protokollierung AWS SAM

Gehen Sie wie folgt vor, um mithilfe von eine Hello TypeScript World-Beispielanwendung mit integrierten Powertools for AWS Lambda (TypeScript) -Modulen herunterzuladen, zu erstellen und bereitzustellen. AWS SAM Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Node.js 18.x oder höher
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mithilfe der Hello TypeScript World-Vorlage.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs18.x
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name sam-app
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.552000
 START RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Version: $LATEST
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.594000
 2022-08-31T09:33:10.557Z 70693159-7e94-4102-a2af-98a6343fb8fb
 INFO {"_aws":{"Timestamp":1661938390556,"CloudWatchMetrics":
[{"Namespace":"sam-app","Dimensions":[["service"]],"Metrics":
[{"Name":"ColdStart","Unit":"Count"}]}]},"service":"helloWorld","ColdStart":1}
```

```
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.595000
 2022-08-31T09:33:10.595Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
 {"level":"INFO","message":"This is an INFO log - sending HTTP 200 - hello world
 response","service":"helloWorld","timestamp":"2022-08-31T09:33:10.594Z"}
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.655000
 2022-08-31T09:33:10.655Z 70693159-7e94-4102-a2af-98a6343fb8fb INFO
 {"_aws":{"Timestamp":1661938390655,"CloudWatchMetrics":[{"Namespace":"sam-
app","Dimensions":[["service"]],"Metrics":[]}]},"service":"helloWorld"}
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.754000 END
 RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb
2023/01/31/[$LATEST]4d53e8d279824834a1ccd35511a4949c 2022-08-31T09:33:10.754000
 REPORT RequestId: 70693159-7e94-4102-a2af-98a6343fb8fb Duration: 201.55 ms Billed
 Duration: 202 ms Memory Size: 128 MB Max Memory Used: 66 MB Init Duration: 252.42
 ms
XRAY TraceId: 1-630f2ad5-1de22b6d29a658a466e7ecf5 SegmentId: 567c116658fbf11a
 Sampled: true
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwalten der Protokollaufbewahrung

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um zu vermeiden, dass Protokolle auf unbestimmte Zeit gespeichert werden, löschen Sie die Protokollgruppe oder konfigurieren Sie einen Aufbewahrungszeitraum, nach dessen Ablauf die Protokolle CloudWatch automatisch gelöscht werden. Um die Aufbewahrung von Protokollen einzurichten, fügen Sie Ihrer AWS SAM Vorlage Folgendes hinzu:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
    # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Verwenden Sie Powertools für AWS Lambda (TypeScript) und AWS CDK für die strukturierte Protokollierung

Gehen Sie wie folgt vor, um mithilfe von eine Hello TypeScript World-Beispielanwendung mit integrierten Powertools for AWS Lambda (TypeScript) -Modulen herunterzuladen, zu erstellen und bereitzustellen. AWS CDK Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Node.js 18.x oder höher
- AWS CLI Version 2
- AWS CDK Ausführung 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS CDK Beispielanwendung bereit

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie die App.

```
cdk init app --language typescript
```

3. Fügen Sie das @types/aws-lambda-Paket als Entwicklungsabhängigkeit hinzu.

```
npm install -D @types/aws-lambda
```

4. Installieren Sie das Logger-Dienstprogramm von Powertools.

```
npm install @aws-lambda-powertools/logger
```

5. Öffnen Sie das lib-Verzeichnis. Sie sollten eine Datei mit dem Namen hello-world-stack.ts sehen. Erstellen Sie neue zwei neue Dateien in diesem Verzeichnis: hello-world.function.ts und hello-world.ts.
6. Öffnen Sie hello-world.function.ts und fügen Sie den folgenden Code in die Datei ein. Dies ist der Code für die Lambda-Funktion.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Logger } from '@aws-lambda-powertools/logger';
const logger = new Logger();

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  logger.info('This is an INFO log - sending HTTP 200 - hello world response');
  return {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
};
```

7. Öffnen Sie hello-world.ts und fügen Sie den folgenden Code in die Datei ein. Dies enthält das NodejsFunction Konstrukt, das die Lambda-Funktion erstellt, Umgebungsvariablen für Powertools konfiguriert und die Protokollspeicherung auf eine Woche festlegt. Es beinhaltet auch das LambdaRestApi Konstrukt, das die REST-API erstellt.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { RetentionDays } from 'aws-cdk-lib/aws-logs';
import { CfnOutput } from 'aws-cdk-lib';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        Powertools_SERVICE_NAME: 'helloWorld',
        LOG_LEVEL: 'INFO',
```

```
      },
      logRetention: RetentionDays.ONE_WEEK,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}
```

8. Öffnen Sie hello-world-stack.ts. Dies ist der Code, der Ihren AWS CDK -Stack definiert. Ersetzen Sie den Code mit Folgendem:

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

9. Kehren Sie zum Projektverzeichnis zurück.

```
cd hello-world
```

10. Stellen Sie die Anwendung bereit.

```
cdk deploy
```

11. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

12. Rufen Sie den API-Endpunkt auf:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

13. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name HelloWorldStack
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.047000
 START RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Version: $LATEST
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.050000 {
"level": "INFO",
"message": "This is an INFO log - sending HTTP 200 - hello world response",
"service": "helloWorld",
"timestamp": "2022-08-31T14:48:37.048Z",
"xray_trace_id": "1-630f74c4-2b080cf77680a04f2362bcf2"
}
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.082000 END
 RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c
2023/01/31/[$LATEST]2ca67f180dcd4d3e88b5d68576740c8e 2022-08-31T14:48:37.082000
 REPORT RequestId: 19ad1007-ff67-40ce-9afe-0af0a9eb512c Duration: 34.60 ms Billed
 Duration: 35 ms Memory Size: 128 MB Max Memory Used: 57 MB Init Duration: 173.48
 ms
```

14. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
cdk destroy
```

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der CloudWatch Konsole

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

TypeScript Ablaufverfolgungscode in AWS Lambda

Lambda ist mit AWS X-Ray integriert, um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS-Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von drei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) – Eine sichere, produktionsbereite, von AWSunterstützte Distribution des OpenTelemetry (OTel) SDK.
- AWS X-Ray SDK für Node.js – Ein SDK zum Generieren und Senden von Nachverfolgungsdaten an X-Ray.
- Powertools für AWS Lambda (TypeScript) – Ein Entwickler-Toolkit zur Implementierung bewährter Methoden für Serverless und zur Steigerung der Entwicklergeschwindigkeit.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda-SDKs sind Teil einer eng integrierten Instrumentierungslösung von AWS. Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Nachverfolgung in X-Ray mit einer der beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS-Distro für Open Telemetry und X-Ray-SDKs.

Sections

Verwenden von Powertools für AWS Lambda (TypeScript) und AWS SAM für die Nachverfolgung

Führen Sie die folgenden Schritte aus, um eine Hello-World- TypeScript Beispielanwendung mit integrierten Modulen von Powertools für AWS Lambda (TypeScript) mithilfe der herunterzuladen, zu erstellen und bereitzustellenAWS SAM. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anforderung an den API Gateway-Endpunkt senden, ruft die Lambda-Funktion auf, sendet Protokolle und Metriken im Embedded Metric Format an CloudWatchund sendet Ablaufverfolgungen an AWS X-Ray. Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Node.js 18.x oder höher
- AWS CLI Version 2
- AWS SAM-CLI-Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM-CLI haben, finden Sie weitere Informationen unter Aktualisieren der AWS SAM-CLI.

Bereitstellen einer AWS SAM-Beispielanwendung

1. Initialisieren Sie die Anwendung mit der Hello World- TypeScript Vorlage.

```
sam init --app-template hello-world-powertools-typescript --name sam-app --package-type Zip --runtime nodejs18.x --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für HelloWorldFunction ist möglicherweise keine Autorisierung definiert. Ist das in Ordnung?, stellen Sie sicher, dass Sie eingebeny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
XRay Event [revision 1] at (2023-01-31T11:29:40.527000) with id
 (1-11a2222-111a222222cb33de3b95daf9) and duration (0.483s)
  - 0.425s - sam-app/Prod [HTTP: 200]
    - 0.422s - Lambda [HTTP: 200]
  - 0.406s - sam-app-HelloWorldFunction-Xyzv11a1bcde [HTTP: 200]
  - 0.172s - sam-app-HelloWorldFunction-Xyzv11a1bcde
    - 0.179s - Initialization
    - 0.112s - Invocation
      - 0.052s - ## app.lambdaHandler
        - 0.001s - ### MySubSegment
    - 0.059s - Overhead
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

Verwenden von Powertools für AWS Lambda (TypeScript) und des AWS CDK für die Nachverfolgung

Führen Sie die folgenden Schritte aus, um eine Hello-World- TypeScript Beispielanwendung mit integrierten Modulen von Powertools für AWS Lambda (TypeScript) mithilfe der herunterzuladen, zu erstellen und bereitzustellenAWS CDK. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anforderung an den API Gateway-Endpunkt senden, ruft die Lambda-Funktion auf, sendet Protokolle und Metriken im Embedded Metric Format an CloudWatchund sendet Ablaufverfolgungen an AWS X-Ray. Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Node.js 18.x oder höher
- AWS CLI Version 2
- AWS CDK Version 2
- AWS SAM-CLI-Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM-CLI haben, finden Sie weitere Informationen unter Aktualisieren der AWS SAM-CLI.

Bereitstellen einer AWS Cloud Development Kit (AWS CDK)-Beispielanwendung

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie die App.

```
cdk init app --language typescript
```

3. Fügen Sie das @types/aws-lambda-Paket als Entwicklungsabhängigkeit hinzu.

```
npm install -D @types/aws-lambda
```

4. Installieren Sie das Tracer-Dienstprogramm von Powertools.

```
npm install @aws-lambda-powertools/tracer
```

5. Öffnen Sie das lib-Verzeichnis. Sie sollten eine Datei mit dem Namen hello-world-stack.ts sehen. Erstellen Sie neue zwei neue Dateien in diesem Verzeichnis: hello-world.function.ts und hello-world.ts.
6. Öffnen Sie hello-world.function.ts und fügen Sie den folgenden Code in die Datei ein. Dies ist der Code für die Lambda-Funktion.

```
import { APIGatewayEvent, APIGatewayProxyResult, Context } from 'aws-lambda';
import { Tracer } from '@aws-lambda-powertools/tracer';
const tracer = new Tracer();

export const handler = async (event: APIGatewayEvent, context: Context):
 Promise<APIGatewayProxyResult> => {
  // Get facade segment created by Lambda
  const segment = tracer.getSegment();

  // Create subsegment for the function and set it as active
  const handlerSegment = segment.addNewSubsegment(`## ${process.env._HANDLER}`);
  tracer.setSegment(handlerSegment);

  // Annotate the subsegment with the cold start and serviceName
  tracer.annotateColdStart();
  tracer.addServiceNameAnnotation();
```

```
  // Add annotation for the awsRequestId
  tracer.putAnnotation('awsRequestId', context.awsRequestId);
  // Create another subsegment and set it as active
  const subsegment = handlerSegment.addNewSubsegment('### MySubSegment');
  tracer.setSegment(subsegment);
  let response: APIGatewayProxyResult = {
    statusCode: 200,
    body: JSON.stringify({
      message: 'hello world',
    }),
  };
  // Close subsegments (the Lambda one is closed automatically)
  subsegment.close(); // (### MySubSegment)
  handlerSegment.close(); // (## index.handler)

  // Set the facade segment as active again (the one created by Lambda)
  tracer.setSegment(segment);
  return response;
};
```

7. Öffnen Sie hello-world.ts und fügen Sie den folgenden Code in die Datei ein. Dies enthält das NodejsFunction Konstrukt , das die Lambda-Funktion erstellt, Umgebungsvariablen für Powertools konfiguriert und die Protokollaufbewahrung auf eine Woche festlegt. Sie enthält auch das LambdaRestApi Konstrukt , das die REST-API erstellt.

```
import { Construct } from 'constructs';
import { NodejsFunction } from 'aws-cdk-lib/aws-lambda-nodejs';
import { LambdaRestApi } from 'aws-cdk-lib/aws-apigateway';
import { CfnOutput } from 'aws-cdk-lib';
import { Tracing } from 'aws-cdk-lib/aws-lambda';

export class HelloWorld extends Construct {
  constructor(scope: Construct, id: string) {
    super(scope, id);
    const helloFunction = new NodejsFunction(this, 'function', {
      environment: {
        POWERTOOLS_SERVICE_NAME: 'helloWorld',
      },
      tracing: Tracing.ACTIVE,
    });
    const api = new LambdaRestApi(this, 'apigw', {
      handler: helloFunction,
    });
```

```
    new CfnOutput(this, 'apiUrl', {
      exportName: 'apiUrl',
      value: api.url,
    });
  }
}
```

8. Öffnen Sie hello-world-stack.ts . Dies ist der Code, der Ihren AWS CDK-Stack definiert. Ersetzen Sie den Code mit Folgendem:

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import { HelloWorld } from './hello-world';

export class HelloWorldStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);
    new HelloWorld(this, 'hello-world');
  }
}
```

9. Stellen Sie die Anwendung bereit.

```
cd ..
cdk deploy
```

10. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?ExportName==`apiUrl`].OutputValue' --output text
```

11. Rufen Sie den API-Endpunkt auf:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

12. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

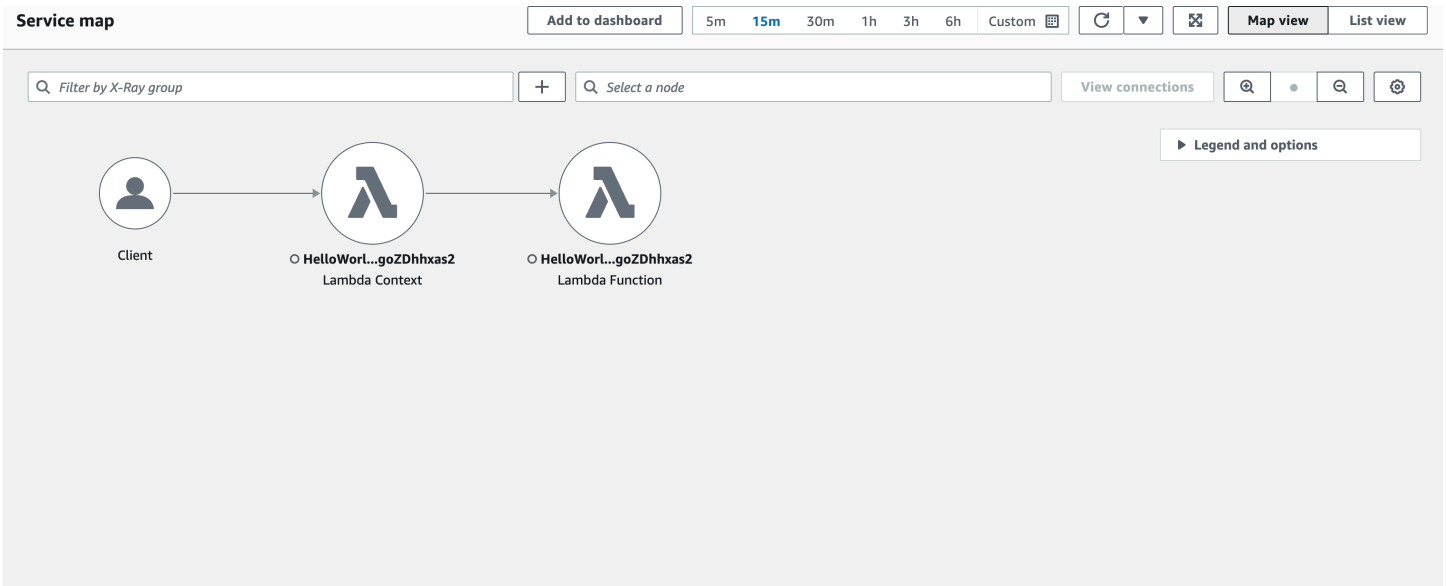
```
XRay Event [revision 1] at (2023-01-31T11:50:06.997000) with id
 (1-11a2222-111a222222cb33de3b95daf9) and duration (0.449s)
  - 0.350s - HelloWorldStack-helloworldfunction111A2BCD-Xyzv11a1bcde [HTTP: 200]
  - 0.157s - HelloWorldStack-helloworldfunction111A2BCD-Xyzv11a1bcde
    - 0.169s - Initialization
    - 0.058s - Invocation
      - 0.055s - ## index.handler
        - 0.000s - ### MySubSegment
    - 0.099s - Overhead
```

13. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
cdk destroy
```

Interpretieren einer X-Ray-Nachverfolgung

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Die X-Ray-Trace-Map liefert Informationen über Ihre Anwendung und alle ihre Komponenten. Das folgende Beispiel zeigt eine Nachverfolgung aus der Beispielanwendung:



Erstellen von Lambda-Funktionen mit Python

Sie können Python-Code in AWS Lambda ausführen. Lambda bietet Laufzeiten für Python, die Ihren Code ausführen, um Ereignisse zu verarbeiten. Ihr Code wird in einer Umgebung ausgeführt, die das SDK for Python (Boto3) enthält, mit Anmeldeinformationen von einer AWS Identity and Access Management (IAM-) Rolle, die Sie verwalten. Weitere Informationen zu den SDK-Versionen, die in den Python-Laufzeiten enthalten sind, finden Sie unterthe section called “SDK-Versionen, die Runtime enthalten”.

Lambda unterstützt die folgenden Python-Laufzeiten.

Python

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Python 3.12	`python3.12`	Amazon Linux 2023			
Python 3.11	`python3.11`	Amazon Linux 2			
Python 3.10	`python3.10`	Amazon Linux 2			
Python 3.9	`python3.9`	Amazon Linux 2			
Python 3.8	`python3.8`	Amazon Linux 2	14. Oktober 202	28. Februar 2025	31. März 2025

> **Note**
>
> Die Laufzeitinformationen in dieser Tabelle werden kontinuierlich aktualisiert. Weitere Informationen zur Verwendung von AWS SDKs in Lambda finden Sie unter Verwalten von AWS SDKs in Lambda-Funktionen in Serverless Land.

So erstellen Sie eine Python-Funktion

1. Öffnen Sie die Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Konfigurieren Sie die folgenden Einstellungen:
   - Funktionsname: Geben Sie einen Namen für die Funktion ein.
   - Laufzeit: Wählen Sie Python 3.12 aus.
4. Wählen Sie Funktion erstellen.
5. Um ein Testereignis zu konfigurieren, wählen Sie Test.
6. Geben Sie für Event name (Ereignisname) **`test`** ein.
7. Wählen Sie Änderungen speichern aus.
8. Wählen Sie Test, um die Funktion aufzurufen.

Die Konsole erstellt eine Lambda-Funktion mit einer einzigen Quelldatei mit dem Namen `lambda_function`. Mit dem integrierten Code-Editor können Sie diese Datei bearbeiten und weitere Dateien hinzufügen. Klicken Sie auf Save (Speichern), um die Änderungen zu speichern. Um Ihren Code auszuführen, wählen Sie Test.

> **Note**
>
> Die Lambda-Konsole dient AWS Cloud9 dazu, eine integrierte Entwicklungsumgebung im Browser bereitzustellen. Sie können es auch verwenden AWS Cloud9 , um Lambda-Funktionen in Ihrer eigenen Umgebung zu entwickeln. Weitere Informationen finden Sie AWS Toolkit im AWS Cloud9 Benutzerhandbuch unter Arbeiten mit AWS Lambda Funktionen unter Verwendung von.

> **Note**
>
> Um mit der Anwendungsentwicklung in Ihrer lokalen Umgebung zu beginnen, stellen Sie eine der Beispielanwendungen bereit, die im GitHub Repository dieses Handbuchs verfügbar sind.

Lambda-Beispielanwendungen in Python

- blank-python — Eine Python-Funktion, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK zeigt. AWS

Ihre Lambda-Funktion enthält eine CloudWatch Logs-Protokollgruppe. Die Funktionslaufzeit sendet Details zu jedem Aufruf an CloudWatch Logs. Es leitet alle Protokolle weiter, die Ihre Funktion während des Aufrufs ausgibt. Wenn Ihre Funktion einen Fehler zurückgibt, formatiert Lambda den Fehler und gibt ihn an den Aufrufer zurück.

Themen

SDK-Versionen, die Runtime enthalten

Die Version des AWS SDK, die in der Python-Laufzeit enthalten ist, hängt von der Laufzeitversion und Ihrer ab AWS-Region. Um die Version des SDK zu finden, die in der von Ihnen verwendeten Runtime enthalten ist, erstellen Sie eine Lambda-Funktion mit dem folgenden Code.

```
import boto3
import botocore

def lambda_handler(event, context):
   print(f'boto3 version: {boto3.__version__}')
```

```
    print(f'botocore version: {botocore.__version__}')
```

Reaktionsformat

In Python 3.12 und späteren Python-Laufzeiten geben Funktionen Unicode-Zeichen als Teil ihrer JSON-Antwort zurück. Frühere Python-Laufzeiten geben Escape-Sequenzen für Unicode-Zeichen in Antworten zurück. Wenn Sie beispielsweise in Python 3.11 eine Unicode-Zeichenfolge wie "こんにちは" zurückgeben, werden die Unicode-Zeichen mit Ecape-Zeichen versehen und es wird "\u3053\u3093\u306b\u3061\u306f" zurückgegeben. Die Python-3.12-Laufzeit gibt das Original "こんにちは" zurück.

Durch die Verwendung von Unicode-Antworten wird die Größe von Lambda-Antworten reduziert, sodass größere Antworten einfacher in die maximale Nutzlastgröße von 6 MB für synchrone Funktionen passen können. Im vorherigen Beispiel hat die Escaped-Version 32 Byte – die Unicode-Zeichenfolge hat 17 Byte.

Wenn Sie auf Python 3.12 aktualisieren, müssen Sie möglicherweise Ihren Code anpassen, um das neue Antwortformat zu berücksichtigen. Wenn der Aufrufer Unicode in Escape-Zeichen erwartet, müssen Sie entweder der zurückgebenden Funktion Code hinzufügen, um den Unicode manuell mit Escape-Zeichen zu versehen, oder den Aufrufer so anpassen, dass er die Unicode-Rückgabe verarbeitet.

Ordnungsgemäßes Herunterfahren von Erweiterungen

Python 3.12 und neuere Python-Laufzeiten bieten verbesserte Funktionen zum ordnungsgemäßen Herunterfahren von Funktionen mit externen Erweiterungen. Wenn Lambda eine Ausführungsumgebung beendet, sendet es ein `SIGTERM`-Signal an die Laufzeitumgebung und dann ein `SHUTDOWN`-Ereignis an jede registrierte externe Erweiterung. Sie können das `SIGTERM`-Signal in Ihrer Lambda-Funktion abfangen und Ressourcen wie Datenbankverbindungen, die von der Funktion erstellt wurden, bereinigen.

Weitere Informationen zum Lebenszyklus der Ausführungsumgebung finden Sie unter Lambda-Ausführungsumgebung. Beispiele für die Verwendung von Graceful Shutdown mit Erweiterungen finden Sie im AWS GitHub Samples-Repository.

Definieren Sie den Lambda-Funktionshandler in Python

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Sie können die folgende allgemeine Syntax verwenden, wenn Sie einen Funktionshandler in Python erstellen:

```
def handler_name(event, context):
    ...
    return some_value
```

Benennung

Der zum Zeitpunkt der Erstellung einer Lambda-Funktion angegebene Lambda-Funktionshandlername wird abgeleitet von:

- dem Namen der Datei, in der sich die Lambda-Handler-Funktion befindet.
- dem Namen der Python-Handler-Funktion.

Ein Funktionshandler kann ein beliebiger Name sein, der Standardname auf der Lambda-Konsole ist jedoch `lambda_function.lambda_handler`. Dieser Name des Funktionshandlers spiegelt den Funktionsnamen (`lambda_handler`) und die Datei, in der der Handler-Code gespeichert ist, (`lambda_function.py`) wider.

Wenn Sie eine Funktion in der Konsole mit einem anderen Dateinamen oder Funktionshandlernamen erstellen, müssen Sie den Standardhandlernamen bearbeiten.

So ändern Sie den Funktionshandlernamen (Konsole)

1. Öffnen Sie die Seite Functions (Funktionen) der Lambda-Konsole und wählen Sie eine Funktion aus.
2. Wählen Sie die Registerkarte Code (Code).
3. Scrollen Sie nach unten zum Bereich Laufzeiteinstellungen und wählen Sie Bearbeiten.
4. Geben Sie unter Handler den neuen Namen für Ihren Funktionshandler ein.
5. Wählen Sie Speichern.

Funktionsweise

Wenn Lambda Ihren Funktionshandler aufruft, übergibt die Lambda-Laufzeit zwei Argumente an den Funktionshandler:

- Das erste Argument ist das Ereignisobjekt. Ein Ereignis ist ein JSON-formatiertes Dokument, das Daten für eine Lambda-Funktion enthält, die verarbeitet werden soll. Die Lambda-Laufzeit konvertiert das Ereignis zu einem Objekt und übergibt es an Ihren Funktionscode. Es ist normalerweise vom Python-`dict`-Typ. Es kann sich aber auch um den Typ `list`, `str`, `int`, `float` oder `NoneType` handeln.

  Das Ereignisobjekt enthält Informationen vom aufrufenden Dienst. Wenn Sie eine Funktion aufrufen, bestimmen Sie die Struktur und den Inhalt des Ereignisses. Wenn ein AWS Dienst Ihre Funktion aufruft, definiert der Dienst die Ereignisstruktur. Weitere Hinweise zu Ereignissen von AWS Diensten finden Sie unterLambda mit Ereignissen aus anderen Diensten aufrufen AWS.
- Das zweite Argument ist das Context-Objekt. Zur Laufzeit wird ein Kontextobjekt von Lambda an Ihre Funktion übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Laufzeitumgebung bereit.

Rückgabe eines Wertes

Optional kann ein Handler einen Wert zurückgeben. Was mit dem zurückgegebenen Wert passiert, hängt von der Aufrufart und dem Service ab, der die Funktion aufgerufen hat. Beispielsweise:

- Wenn Sie den `RequestResponse` Aufruftyp verwenden, z. B.Synchroner Aufruf, wird das Ergebnis des Python-Funktionsaufrufs an den Client AWS Lambda zurückgegeben, der die Lambda-Funktion aufruft (in der HTTP-Antwort auf die Aufrufanforderung, serialisiert in JSON). Wenn eine AWS Lambda -Konsole zum Beispiel den Aufruftyp `RequestResponse` verwendet, zeigt die Konsole den zurückgegebenen Wert an, nachdem die Funktion auf der Konsole abgerufen wurde.
- Wenn der Handler Objekte zurückgibt, die nicht von `json.dumps` serialisiert werden können, gibt die Laufzeit einen Fehler zurück.
- Wenn der Handler `None` zurückgibt, wie es Python-Funktionen ohne eine `return`-Anweisung implizit tun, gibt die Laufzeit `null` zurück.
- Wenn Sie den Aufruftyp `Event` (asynchroner Aufruf) verwenden, wird der Wert verworfen.

> **Note**
>
> In Python 3.9 und späteren Versionen schließt Lambda die requestId des Aufrufs in die Fehlerantwort ein.

Beispiele

Der folgende Abschnitt zeigt Beispiele für Python-Funktionen, die Sie mit Lambda verwenden können. Wenn Sie die Lambda-Konsole zum Erstellen Ihrer Funktion verwenden, müssen Sie keine ZIP-Archivdatei anhängen, um die Funktionen in diesem Abschnitt auszuführen. Diese Funktionen verwenden Standard-Python-Bibliotheken, die in der von Ihnen ausgewählten Lambda-Laufzeit enthalten sind. Weitere Informationen finden Sie unter Lambda-Bereitstellungspakete.

Rückgabe einer Nachricht

Das folgende Codebeispiel zeigt eine Funktion namens `lambda_handler`. Die Funktion akzeptiert Benutzereingaben eines Vor- und Nachnamens und gibt eine Meldung zurück, die Daten aus dem Ereignis enthält, das sie als Eingabe erhalten hat.

```
def lambda_handler(event, context):
    message = 'Hello {} {}!'.format(event['first_name'], event['last_name'])
    return {
        'message' : message
    }
```

Sie können die folgenden Ereignisdaten verwenden, um die Funktion aufzurufen:

```
{
    "first_name": "John",
    "last_name": "Smith"
}
```

Die Antwort zeigt die als Eingabe übergebenen Ereignisdaten an:

```
{
    "message": "Hello John Smith!"
}
```

Parsen einer Antwort

Das folgende Codebeispiel zeigt eine Funktion namens `lambda_handler`. Die Funktion verwendet zur Lambda-Laufzeit übergebene Ereignisdaten. Es analysiert die Umgebungsvariable in `AWS_REGION`, die in der JSON-Antwort zurückgegeben wird.

```
import os
import json

def lambda_handler(event, context):
    json_region = os.environ['AWS_REGION']
    return {
        "statusCode": 200,
        "headers": {
            "Content-Type": "application/json"
        },
        "body": json.dumps({
            "Region ": json_region
        })
    }
```

Sie können beliebige Ereignisdaten verwenden, um die Funktion aufzurufen:

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```

Lambda Laufzeiten setzen mehrere Umgebungsvariablen während der Initialisierung. Weitere Hinweise zu den Umgebungsvariablen, die zur Laufzeit in der Antwort zurückgegeben werden, finden Sie unter Verwenden Sie Lambda-Umgebungsvariablen, um Werte im Code zu konfigurieren.

Die Funktion in diesem Beispiel hängt von einer erfolgreichen Antwort (in `200`) der Invoke API ab. Weitere Informationen zum API-Aufruf-Status finden Sie unter Antwortsyntax aufrufen.

Rückgabe einer Berechnung

Das folgende Codebeispiel zeigt eine Funktion namens `lambda_handler`. Die Funktion akzeptiert Benutzereingaben und gibt eine Berechnung an den Benutzer zurück. Weitere Informationen zu diesem Beispiel finden Sie im Repository. aws-doc-sdk-examples GitHub

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)

def lambda_handler(event, context):
    ...
    result = None
    action = event.get('action')
    if action == 'increment':
        result = event.get('number', 0) + 1
        logger.info('Calculated result of %s', result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {'result': result}
    return response
```

Sie können die folgenden Ereignisdaten verwenden, um die Funktion aufzurufen:

```
{
    "action": "increment",
    "number": 3
}
```

Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen

Der Code Ihrer AWS Lambda Funktion besteht aus einer .py-Datei, die den Handlercode Ihrer Funktion enthält, zusammen mit allen zusätzlichen Paketen und Modulen, von denen Ihr Code abhängt. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Dieses Paket kann entweder ein ZIP-Dateiarchiv oder ein Container-Image sein. Weitere Informationen zur Verwendung von Container-Images mit Python finden Sie unter Bereitstellen von Python-Lambda-Funktionen mit Container-Images.

Zum Erstellen des Bereitstellungspakets für ein ZIP-Dateiarchiv können Sie ein integriertes Dienstprogramm für ZIP-Dateien Ihres Befehlzeilen-Tools oder ein anderes Dienstprogramm für ZIP-Dateien verwenden, wie 7zip. In den Beispiele in den folgenden Abschnitten wird davon ausgegangen, dass Sie ein `zip`-Befehlszeilen-Tool in einer Linux- oder MacOS-Umgebung verwenden. Unter Windows können Sie das Windows-Subsystem für Linux installieren, um eine Windows-Version von Ubuntu und Bash zu erhalten und dieselben Befehle zu verwenden.

Da Lambda POSIX-Dateiberechtigungen verwendet, müssen Sie möglicherweise Berechtigungen für den Bereitstellungspaketordner festlegen, bevor Sie das ZIP-Dateiarchiv erstellen.

Themen

Laufzeitabhängigkeiten in Python

Für Lambda-Funktionen, die die Python-Laufzeit verwenden, kann eine Abhängigkeit ein beliebiges Python-Paket oder -Modul sein. Wenn Sie Ihre Funktion mithilfe eines ZIP-Archivs bereitstellen, können Sie diese Abhängigkeiten entweder mit Ihrem Funktionscode zu Ihrer .zip-Datei hinzufügen oder eine Lambda-Schicht verwenden. Eine Ebene ist ein separates ZIP-Dateiarchiv, das zusätzlichen Code und andere Daten enthalten kann. Weitere Informationen zur Verwendung von Lambda-Layern in Python finden Sie unterthe section called “Ebenen”.

Die Lambda-Python-Laufzeiten beinhalten die AWS SDK for Python (Boto3) und ihre Abhängigkeiten. Lambda stellt das SDK in der Laufzeit für Bereitstellungsszenarien bereit, in denen Sie keine eigenen Abhängigkeiten hinzufügen können. Zu diesen Szenarien gehören die Erstellung von Funktionen in der Konsole mithilfe des integrierten Code-Editors oder die Verwendung von Inline-Funktionen in AWS Serverless Application Model (AWS SAM) oder AWS CloudFormation Vorlagen.

Lambda aktualisiert die Bibliotheken in der Python-Laufzeit regelmäßig, um die neuesten Updates und Sicherheitspatches aufzunehmen. Wenn Ihre Funktion die in der Runtime enthaltene Version des Boto3-SDK verwendet, Ihr Bereitstellungspaket jedoch SDK-Abhängigkeiten enthält, kann dies zu Versionsproblemen führen. Ihr Bereitstellungspaket enthält beispielsweise die SDK-Abhängigkeit urllib3. Aktualisiert Lambda das SDK während der Laufzeit, können Kompatibilitätsprobleme zwischen der neuen Version der Laufzeit und der Version von urllib3 in Ihrem Bereitstellungspaket dazu führen, dass Ihre Funktion fehlschlägt.

> **Important**
>
> Um die volle Kontrolle über Ihre Abhängigkeiten zu behalten und mögliche Versionsprobleme zu vermeiden, empfehlen wir Ihnen, alle Abhängigkeiten Ihrer Funktion zu Ihrem Bereitstellungspaket hinzuzufügen, auch wenn Versionen davon in der Lambda-Laufzeit enthalten sind. Dazu gehört das Boto3-SDK.

Informationen darüber, welche Version des SDK for Python (Boto3) in der von Ihnen verwendeten Runtime enthalten ist, finden Sie unter. the section called “SDK-Versionen, die Runtime enthalten”

Im Rahmen des AWS -Modells der geteilten Verantwortung sind Sie für die Verwaltung aller Abhängigkeiten in den Bereitstellungspaketen Ihrer Funktionen verantwortlich. Dies beinhaltet das Durchführen von Updates und Sicherheitspatches. Zum Aktualisieren von Abhängigkeiten im Bereitstellungspaket Ihrer Funktion erstellen Sie zunächst eine neue ZIP-Datei und laden Sie diese dann in Lambda hoch. Weitere Informationen finden Sie unter ZIP-Bereitstellungspakets mit Abhängigkeiten erstellen und Python-Lambda-Funktionen mithilfe von ZIP-Dateien erstellen und aktualisieren.

ZIP-Bereitstellungspakets ohne Abhängigkeiten erstellen

Hat Ihr Funktionscode keine Abhängigkeiten, enthält Ihre ZIP-Datei nur die PY-Datei mit dem Handler-Code Ihrer Funktion. Erstellen Sie mit Ihrem bevorzugten ZIP-Programm eine ZIP-Datei mit Ihrer PY-Datei im Stammverzeichnis. Befindet sich die PY-Datei nicht im Stammverzeichnis Ihrer ZIP-Datei, kann Lambda Ihren Code nicht ausführen.

Informationen zum Bereitstellen Ihrer ZIP-Datei zum Erstellen einer neuen Lambda-Funktion oder Aktualisieren einer vorhandenen Funktion, finden Sie unter Python-Lambda-Funktionen mithilfe von ZIP-Dateien erstellen und aktualisieren.

ZIP-Bereitstellungspakets mit Abhängigkeiten erstellen

Wenn Ihr Funktionscode von zusätzlichen Paketen oder Modulen abhängt, können Sie diese Abhängigkeiten entweder mit Ihrem Funktionscode zu Ihrer .zip-Datei hinzufügen oder eine Lambda-Schicht verwenden. Die Anweisungen in diesem Abschnitt zeigen Ihnen, wie Sie Ihre Abhängigkeiten in Ihr ZIP-Bereitstellungspaket aufnehmen. Damit Lambda Ihren Code ausführen kann, muss die PY-Datei, die Ihren Handler-Code und alle Abhängigkeiten Ihrer Funktion enthält, im Stammverzeichnis der ZIP-Datei installiert werden.

Angenommen, Ihr Funktionscode ist in einer Datei mit dem Namen „`lambda_function.py`“ gespeichert. Die folgenden CLI-Befehle erstellen Sie eine ZIP-Datei mit dem Namen „`my_deployment_package.zip`“, die Ihren Funktionscode und seine Abhängigkeiten enthält. Sie können Ihre Abhängigkeiten entweder direkt in einem Ordner in Ihrem Projektverzeichnis installieren oder eine virtuelle Python-Umgebung verwenden.

So erstellen Sie das Bereitstellungspaket (Projektverzeichnis)

1. Navigieren Sie zum Projektverzeichnis, das Ihre `lambda_function.py`-Quellcodedatei enthält. In diesem Beispiel trägt das Verzeichnis den Namen `my_function`.

   ```
   cd my_function
   ```

2. Erstellen Sie ein neues Verzeichnis mit dem Namen „package“, in das Sie Ihre Abhängigkeiten installieren.

   ```
   mkdir package
   ```

   Beachten Sie, dass Lambda bei einem ZIP-Bereitstellungspaket erwartet, dass sich Ihr Quellcode und seine Abhängigkeiten im Stammverzeichnis der ZIP-Datei befinden. Installieren Sie jedoch Abhängigkeiten direkt in Ihrem Projektverzeichnis, kann dies zu einer großen Anzahl neuer Dateien und Ordner führen und das Navigieren in Ihrer IDE erschweren. Sie erstellen hier ein separates `package`-Verzeichnis, um Ihre Abhängigkeiten von Ihrem Quellcode zu trennen.

3. Installieren Sie Ihre Abhängigkeiten im `package`-Verzeichnis. Im folgenden Beispiel wird das Boto3-SDK aus dem Python-Paketindex mithilfe von pip installiert. Verwendet Ihr Funktionscode selbst erstellte Python-Pakete, speichern Sie diese im `package`-Verzeichnis.

   ```
   pip install --target ./package boto3
   ```

4. Erstellen Sie eine ZIP-Datei mit den installierten Bibliotheken im Stammverzeichnis.

   ```
   cd package
   zip -r ../my_deployment_package.zip .
   ```

   Dadurch wird eine `my_deployment_package.zip`-Datei in Ihrem Projektverzeichnis generiert.

5. Fügen Sie die Datei „lambda_function.py“ dem Stammverzeichnis der ZIP-Datei hinzu.

   ```
   cd ..
   zip my_deployment_package.zip lambda_function.py
   ```

   Ihre ZIP-Datei sollte eine flache Verzeichnisstruktur haben, wobei der Handler-Code Ihrer Funktion und alle Ihre Abhängigkeitsordner wie folgt im Stammverzeichnis installiert sind.

   ```
   my_deployment_package.zip
   |- bin
   |  |-jp.py
   |- boto3
   |  |-compat.py
   |  |-data
   |  |-docs
   ...
   |- lambda_function.py
   ```

   Befindet sich die PY-Datei mit dem Handler-Code Ihrer Funktion nicht im Stammverzeichnis Ihrer ZIP-Datei, kann Lambda Ihren Code nicht ausführen.

So erstellen Sie das Bereitstellungspaket (virtuelle Umgebung)

1. Erstellen und aktivieren Sie eine virtuelle Umgebung in Ihrem Projektverzeichnis. In diesem Beispiel trägt das Projektverzeichnis den Namen „`my_function`“.

   ```
   ~$ cd my_function
   ```

```
~/my_function$ python3.12 -m venv my_virtual_env
~/my_function$ source ./my_virtual_env/bin/activate
```

2. Installieren Sie Ihre erforderlichen Bibliotheken mithilfe von pip. Im folgenden Beispiel wird das Boto3-SDK installiert.

```
(my_virtual_env) ~/my_function$ pip install boto3
```

3. Verwenden Sie `pip show`, um den Ort in Ihrer virtuellen Umgebung zu finden, an dem pip Ihre Abhängigkeiten installiert hat.

```
(my_virtual_env) ~/my_function$ pip show <package_name>
```

   Der Ordner, in dem pip Ihre Bibliotheken installiert, heißt entweder „`site-packages`“ oder „`dist-packages`“. Dieser Ordner befindet sich entweder im Verzeichnis „`lib/python3.x`“ oder „`lib64/python3.x`“ (wobei „python3.x“ die verwendete Python-Version ist).

4. Deaktivieren Sie die virtuelle Umgebung.

```
(my_virtual_env) ~/my_function$ deactivate
```

5. Navigieren Sie in das Verzeichnis mit den Abhängigkeiten, die Sie mit pip installiert haben, und erstellen Sie eine ZIP-Datei in Ihrem Projektverzeichnis mit den installierten Abhängigkeiten im Stammverzeichnis. In diesem Beispiel hat pip Ihre Abhängigkeiten im Verzeichnis „`my_virtual_env/lib/python3.12/site-packages`“ installiert.

```
~/my_function$ cd my_virtual_env/lib/python3.12/site-packages
~/my_function/my_virtual_env/lib/python3.12/site-packages$ zip -r ../../../../
my_deployment_package.zip .
```

6. Navigieren Sie zum Stammverzeichnis Ihres Projektverzeichnisses, in dem sich die PY-Datei mit Ihrem Handler-Code befindet, und fügen Sie diese Datei dem Stammverzeichnis Ihres ZIP-Pakets hinzu. In diesem Beispiel heißt Ihre Funktionscodedatei „`lambda_function.py`“.

```
~/my_function/my_virtual_env/lib/python3.12/site-packages$ cd ../../../../
~/my_function$ zip my_deployment_package.zip lambda_function.py
```

Suchpfad für Abhängigkeiten und integrierte Laufzeit-Bibliotheken

Wenn Sie in Ihrem Code eine `import`-Anweisung verwenden, durchsucht die Python-Laufzeit die Verzeichnisse in ihrem Suchpfad, bis sie das Modul oder Paket findet. Standardmäßig ist der erste Speicherort, den die Laufzeit durchsucht, das Verzeichnis, in das Ihr ZIP-Bereitstellungspaket entpackt und bereitgestellt wird (`/var/task`). Wenn Sie eine Version einer in der Laufzeit enthaltenen Bibliothek in Ihr Bereitstellungspaket einfügen, hat Ihre Version Vorrang vor der Version, die in der Laufzeit enthalten ist. Abhängigkeiten in Ihrem Bereitstellungspaket haben ebenfalls Vorrang vor Abhängigkeiten in Ebenen.

Wenn Sie einer Ebene eine Abhängigkeit hinzufügen, extrahiert Lambda diese in `/opt/python/lib/python3.x/site-packages` (wobei `python3.x` die von Ihnen verwendete Version der Laufzeit ist) oder in `/opt/python`. Im Suchpfad haben diese Verzeichnisse Vorrang vor den Verzeichnissen, die die in der Laufzeit enthaltenen Bibliotheken und die über pip installierten Bibliotheken enthalten (`/var/runtime` und `/var/lang/lib/python3.x/site-packages`). Bibliotheken in Funktionsebenen haben daher Vorrang vor Versionen, die in der Laufzeit enthalten sind.

> **Note**
>
> Im verwalteten Runtime- und Basis-Image von Python 3.11 sind das AWS SDK und seine Abhängigkeiten im `/var/lang/lib/python3.11/site-packages` Verzeichnis installiert.

Sie können den vollständigen Suchpfad für Ihre Lambda-Funktion sehen, indem Sie den folgenden Codeausschnitt hinzufügen.

```
import sys

search_path = sys.path
print(search_path)
```

> **Note**
>
> Da Abhängigkeiten in Ihrem Bereitstellungspaket oder Ihren Ebenen Vorrang vor Bibliotheken haben, die zur Laufzeit gehören, kann es zu Versionsproblemen kommen, wenn Sie eine SDK-Abhängigkeit wie urllib3 in Ihr Paket aufnehmen, ohne das SDK ebenfalls einzubetten. Stellen Sie Ihre eigene Version einer Boto3-Abhängigkeit bereit, müssen Sie Boto3 auch als

Abhängigkeit in Ihrem Bereitstellungspaket bereitstellen. Wir empfehlen, alle Abhängigkeiten Ihrer Funktion in ein Paket aufzunehmen, auch wenn Versionen davon in der Laufzeit enthalten sind.

Fügen Sie Abhängigkeiten alternativ auch in einem separaten Ordner in Ihrem ZIP-Paket hinzu. Fügen Sie beispielsweise eine Version des Boto3-SDK zu einem Ordner in Ihrem ZIP-Paket mit dem Namen „`common`“ hinzu. Wird Ihr ZIP-Paket entpackt und bereitgestellt, wird dieser Ordner im Verzeichnis „`/var/task`“ abgelegt. Mit einer `import from`-Anweisung verwenden Sie eine Abhängigkeit aus einem Ordner Ihres ZIP-Bereitstellungspakets in Ihrem Code. Verwenden Sie mithilfe folgender Anweisung beispielsweise eine Version von Boto3 aus einem Ordner, der in Ihrem ZIP-Paket „`common`“ heißt.

```
from common import boto3
```

__pycache__-Ordner verwenden

Es wird empfohlen, keine `__pycache__`-Ordner in das Bereitstellungspaket Ihrer Funktion aufzunehmen. Python-Bytecode, der auf einem Build-Computer mit einer anderen Architektur oder in einem anderen Betriebssystem kompiliert wurde, ist möglicherweise nicht mit der Lambda-Ausführungsumgebung kompatibel.

ZIP-Bereitstellungspakete mit nativen Bibliotheken erstellen

Verwendet Ihre Funktion nur reine Python-Pakete und -Module, können Sie mit dem `pip install`-Befehl Ihre Abhängigkeiten auf einem beliebigen lokalen Build-Computer installieren und Ihre ZIP-Datei erstellen. Viele beliebte Python-Bibliotheken, darunter NumPy Pandas, sind kein reines Python und enthalten Code, der in C oder C++ geschrieben ist. Fügen Sie Ihrem Bereitstellungspaket Bibliotheken hinzu, die C-/C++-Code enthalten, müssen Sie Ihr Paket korrekt erstellen, damit es mit der Lambda-Ausführungsumgebung kompatibel ist.

Die meisten Pakete im Python-Paketindex (PyPI) sind als „Wheels“ (WHL-Dateien) verfügbar. Eine WHL-Datei ist eine Art von ZIP-Datei, die eine erstellte Distribution mit vorkompilierten Binärdateien für ein bestimmtes Betriebssystem und eine bestimmte Befehlssatzarchitektur enthält. Für die Kompatibilität Ihres Bereitstellungspakets mit Lambda installieren Sie das Wheel für Linux-Betriebssysteme und die Befehlssatzarchitektur Ihrer Funktion.

Einige Pakete sind möglicherweise nur als Quelldistributionen verfügbar. Für diese Pakete müssen Sie die C-/C++-Komponenten selbst kompilieren und erstellen.

Gehen Sie wie folgt vor, um anzuzeigen, welche Distributionen für Ihr erforderliches Paket verfügbar sind:

1. Suchen Sie auf der Hauptseite des Python-Paketindex nach dem Namen des Pakets.
2. Wählen Sie die Paketversion aus, die Sie verwenden möchten.
3. Wählen Sie Dateien zum Herunterladen aus.

Mit erstellten Distributionen (Wheels) arbeiten

Zum Herunterladen eines Wheels, das mit Lambda kompatibel ist, verwenden Sie die pip-Option „`--platform`“.

Verwendet Ihre Lambda-Funktion die x86_64-Befehlssatzarchitektur, führen Sie den folgenden `pip install`-Befehl aus, um ein kompatibles Wheel in Ihrem `package`-Verzeichnis zu installieren. Ersetzen Sie „`--python 3.x`“ durch die Version der verwendeten Python-Laufzeit.

```
pip install \
--platform manylinux2014_x86_64 \
--target=package \
--implementation cp \
--python-version 3.x \
--only-binary=:all: --upgrade \
<package_name>
```

Verwendet Ihre Funktion die arm64-Befehlssatzarchitektur, führen Sie den folgenden Befehl aus. Ersetzen Sie „`--python 3.x`“ durch die Version der verwendeten Python-Laufzeit.

```
pip install \
--platform manylinux2014_aarch64 \
--target=package \
--implementation cp \
--python-version 3.x \
--only-binary=:all: --upgrade \
<package_name>
```

Mit Quelldistributionen arbeiten

Ist Ihr Paket nur als Quelldistribution verfügbar, müssen Sie die C-/C++-Bibliotheken selbst erstellen. Für die Kompatibilität Ihres Pakets mit der Lambda-Ausführungsumgebung müssen Sie es in einer Umgebung erstellen, die dasselbe Amazon-Linux-2-Betriebssystem verwendet. Erstellen Sie dafür Ihr Paket in einer Amazon-EC2-Linux-Instance.

Weitere Informationen zum Starten und Herstellen einer Verbindung mit einer Amazon-EC2-Linux-Instance finden Sie unter Tutorial: Erste Schritte mit Amazon-EC2-Instances für Linux im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

Python-Lambda-Funktionen mithilfe von ZIP-Dateien erstellen und aktualisieren

Nach der Erstellung Ihres ZIP-Bereitstellungspakets können Sie es verwenden, um eine neue Lambda-Funktion zu erstellen oder eine vorhandene zu aktualisieren. Sie können Ihr .zip-Paket mithilfe der Lambda-Konsole, der und der AWS Command Line Interface Lambda-API bereitstellen. Sie können Lambda-Funktionen auch mit AWS Serverless Application Model (AWS SAM) und AWS CloudFormation erstellen und aktualisieren.

Die maximale Größe eines ZIP-Bereitstellungspakets für Lambda beträgt 250 MB (entpackt). Beachten Sie, dass dieser Grenzwert für die kombinierte Größe aller hochgeladenen Dateien gilt, einschließlich aller Lambda-Ebenen.

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Linux-Notation der Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen (rwxr-xr-x) für Verzeichnisse und ausführbare Dateien.

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Konsole

Eine neue Funktion müssen Sie zuerst in der Konsole erstellen und dann Ihr ZIP-Archiv hochladen. Zum Aktualisieren einer bestehenden Funktion öffnen Sie die Seite für Ihre Funktion und gehen dann genauso vor, um Ihre aktualisierte ZIP-Datei hinzuzufügen.

Bei einer ZIP-Datei mit unter 50 MB können Sie eine Funktion erstellen oder aktualisieren, indem Sie die Datei direkt von Ihrem lokalen Computer hochladen. Bei ZIP-Dateien mit einer Größe von mehr als 50 MB müssen Sie Ihr Paket zuerst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3-Bucket mithilfe von finden Sie unter Erste Schritte mit Amazon S3. AWS Management Console Informationen zum Hochladen von Dateien mit dem AWS CLI finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch.

> **Note**
>
> Sie können den Bereitstellungspakettyp (.zip oder Container-Image) für eine bestehende Funktion nicht ändern. Sie können beispielsweise eine Container-Image-Funktion nicht so konvertieren, dass sie ein ZIP-Dateiarchiv verwendet. Sie müssen eine neue Funktion erstellen.

So erstellen Sie eine neue Funktion (Konsole)

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Funktion erstellen aus.
2. Wählen Sie Author from scratch aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie als Funktionsname den Namen Ihrer Funktion ein.
   b. Wählen Sie für Laufzeit die Laufzeit aus, die Sie verwenden möchten.
   c. (Optional) Für Architektur wählen Sie die Befehlssatz-Architektur für Ihre Funktion aus. Die Standardarchitektur ist x86_64. Stellen Sie sicher, dass das ZIP-Bereitstellungspaket für Ihre Funktion mit der von Ihnen gewählten Befehlssatzarchitektur kompatibel ist.
4. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
5. Wählen Sie Funktion erstellen. Lambda erstellt eine grundlegende „Hello World“-Funktion mit der von Ihnen gewählten Laufzeit.

So laden Sie ein ZIP-Archiv von Ihrem lokalen Computer hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie die ZIP-Datei aus.
5. Laden Sie die ZIP-Datei wie folgt hoch:
   a. Wählen Sie Hochladen und dann Ihre ZIP-Datei in der Dateiauswahl aus.
   b. Klicken Sie auf Open.
   c. Wählen Sie Speichern.

So laden Sie ein ZIP-Archiv aus einem Amazon-S3-Bucket hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie eine neue ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie den Amazon-S3-Speicherort aus.
5. Fügen Sie die Amazon-S3-Link-URL Ihrer ZIP-Datei ein und wählen Sie Speichern aus.

ZIP-Dateifunktionen mithilfe des Konsolencode-Editors aktualisieren

Für einige Funktionen mit ZIP-Bereitstellungspaketen können Sie Ihren Funktionscode direkt mit dem in der Lambda-Konsole integrierten Code-Editor aktualisieren. Zur Verwendung dieses Features muss Ihre Funktion folgende Kriterien erfüllen:

- Ihre Funktion muss eine der interpretierten Sprache der Laufzeit verwenden (Python, Node.js oder Ruby).
- Das Bereitstellungspaket Ihrer Funktion muss kleiner als 3 MB sein.

Funktionscode für Funktionen mit Container-Image-Bereitstellungspaketen kann nicht direkt in der Konsole bearbeitet werden.

So aktualisieren Sie Ihren Funktionscode mit dem Code-Editor

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle Ihre Quellcodedatei aus und bearbeiten Sie sie im integrierten Code-Editor.
4. Nach der Bearbeitung Ihres Codes wählen Sie Bereitstellen aus, um Ihre Änderungen zu speichern und Ihre Funktion zu aktualisieren.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe der AWS CLI

Sie können die AWS CLI verwenden, um eine neue Funktion zu erstellen oder eine vorhandene unter Verwendung einer ZIP-Datei zu aktualisieren. Verwenden Sie die Befehle Funktion erstellen und Funktionscode aktualisieren, um Ihr ZIP-Paket bereitzustellen. Wenn Ihre ZIP-Datei kleiner als 50 MB ist, können Sie das ZIP-Paket von einem Dateispeicherort auf Ihrem lokalen Build-Computer hochladen. Bei größeren Dateien müssen Sie Ihr ZIP-Paket aus einem Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

> **Note**
>
> Wenn Sie Ihre ZIP-Datei mithilfe von aus einem Amazon S3 S3-Bucket hochladen AWS CLI, muss sich der Bucket im selben Verzeichnis befinden AWS-Region wie Ihre Funktion.

Um eine neue Funktion mithilfe einer .zip-Datei mit dem zu erstellen AWS CLI, müssen Sie Folgendes angeben:

- Den Namen Ihrer Funktion (`--function-name`)
- Die Laufzeit Ihrer Funktion (`--runtime`)
- Den Amazon-Ressourcennamen (ARN) der Ausführungsrolle der Funktion (`--role`).
- Den Namen der Handler-Methode in Ihrem Funktionscode (`--handler`)

Sie müssen auch den Speicherort Ihrer ZIP-Datei angeben. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda create-function --function-name myFunction \
--runtime python3.12 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigte `--code`-Option. Sie müssen den `S3ObjectVersion`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda create-function --function-name myFunction \
--runtime python3.12 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=DOC-EXAMPLE-BUCKET,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Um eine vorhandene Funktion mit der CLI zu aktualisieren, geben Sie den Namen Ihrer Funktion unter Verwendung des `--function-name`-Parameters an. Sie müssen auch den Speicherort der ZIP-Datei angeben, die Sie zum Aktualisieren Ihres Funktionscodes verwenden möchten. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigten `--s3-bucket`- und `--s3-key`-Optionen. Sie müssen den `--s3-object-version`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket DOC-EXAMPLE-BUCKET --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Lambda-API

Um Funktionen zu erstellen und zu konfigurieren, die ein ZIP-Dateiarchiv verwenden, verwenden Sie die folgenden API-Operationen:

- CreateFunction
- UpdateFunctionCode

Funktionen mit ZIP-Dateien erstellen und aktualisieren mithilfe von AWS SAM

Das AWS Serverless Application Model (AWS SAM) ist ein Toolkit, das dabei hilft, den Prozess der Erstellung und Ausführung serverloser Anwendungen zu optimieren. AWS Sie definieren die Ressourcen für Ihre Anwendung in einer YAML- oder JSON-Vorlage und verwenden die AWS SAM Befehlszeilenschnittstelle (AWS SAM CLI), um Ihre Anwendungen zu erstellen, zu verpacken und bereitzustellen. Wenn Sie eine Lambda-Funktion aus einer AWS SAM Vorlage erstellen, AWS SAM wird automatisch ein ZIP-Bereitstellungspaket oder ein Container-Image mit Ihrem Funktionscode und allen von Ihnen angegebenen Abhängigkeiten erstellt. Weitere Informationen zur Verwendung AWS SAM zum Erstellen und Bereitstellen von Lambda-Funktionen finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model Entwicklerhandbuch.

Sie können es auch verwenden AWS SAM , um eine Lambda-Funktion mithilfe eines vorhandenen ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion zu erstellen AWS SAM, können Sie Ihre ZIP-Datei in einem Amazon S3 S3-Bucket oder in einem lokalen Ordner auf Ihrem Build-Computer speichern. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS SAM Vorlage spezifiziert die `AWS::Serverless::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `CodeUri`- auf die Amazon S3 S3-URI, den Pfad zum lokalen Ordner oder FunctionCodeObjekt des Funktionscodes gesetzt
- `Runtime` – festlegen auf die gewünschte Laufzeit

Wenn Ihre ZIP-Datei größer als 50 MB ist, müssen Sie sie nicht zuerst in einen Amazon S3 S3-Bucket hochladen. AWS SAM AWS SAM kann .zip-Pakete bis zur maximal zulässigen Größe von 250 MB (entpackt) von einem Speicherort auf Ihrem lokalen Build-Computer hochladen.

Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei in finden Sie AWS::Serverless::Functionim AWS SAM Entwicklerhandbuch.AWS SAM

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe von AWS CloudFormation

Sie können verwenden AWS CloudFormation , um eine Lambda-Funktion mithilfe eines ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion aus einer ZIP-Datei zu erstellen, müssen Sie

Ihre Datei zunächst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

Für Node.js- und Python-Laufzeiten können Sie auch Inline-Quellcode in Ihrer AWS CloudFormation Vorlage bereitstellen. AWS CloudFormation erstellt dann eine ZIP-Datei, die Ihren Code enthält, wenn Sie Ihre Funktion erstellen.

Eine vorhandene ZIP-Datei verwenden

In Ihrer AWS CloudFormation Vorlage spezifiziert die `AWS::Lambda::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `Code` – Geben Sie den Namen des Amazon-S3-Buckets und den ZIP-Dateinamen in die Felder `S3Bucket` und `S3Key` ein
- `Runtime` – festlegen auf die gewünschte Laufzeit

Eine ZIP-Datei aus dem Inline-Code erstellen

Sie können einfache Funktionen, die in Python oder Node.js geschrieben wurden, inline in einer AWS CloudFormation Vorlage deklarieren. Da der Code in YAML oder JSON eingebettet ist, können Sie Ihrem Bereitstellungspaket keine externen Abhängigkeiten hinzufügen. Das bedeutet, dass Ihre Funktion die Version des AWS SDK verwenden muss, die in der Laufzeit enthalten ist. Die Anforderungen der Vorlage, wie die Notwendigkeit von Escapezeichen für bestimmte Zeichen, erschweren ebenfalls die Verwendung von IDE-Features zur Syntaxprüfung und Codevervollständigung. Ihre Vorlage erfordert deshalb möglicherweise zusätzliche Tests. Aufgrund dieser Einschränkungen eignet sich das Inline-Deklarieren von Funktionen am besten für sehr einfachen Code, der sich nicht häufig ändert.

Zum Erstellen einer ZIP-Datei aus Inline-Code für Node.js- und Python-Laufzeiten legen Sie die folgenden Eigenschaften in der Ressource Ihrer `AWS::Lambda::Function`-Vorlage fest:

- `PackageType` – festlegen auf `Zip`
- `Code` – Funktionscode in das `ZipFile`-Feld eingeben
- `Runtime` – festlegen auf die gewünschte Laufzeit

Die AWS CloudFormation generierte ZIP-Datei darf 4 MB nicht überschreiten. Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei finden Sie AWS::Lambda::Functionim AWS CloudFormation Benutzerhandbuch. AWS CloudFormation

Bereitstellen von Python-Lambda-Funktionen mit Container-Images

Es gibt drei Möglichkeiten, ein Container-Image für eine Python-Lambda-Funktion zu erstellen:

- Verwenden eines AWS Basis-Images für Python

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.

- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Python in das Image aufnehmen.

- Verwenden Sie ein Nicht-Basis-Image AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Python in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

Themen

- AWS Basisbilder für Python

- Verwenden eines AWS Basis-Images für Python
- Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

AWS Basisbilder für Python

AWS stellt die folgenden Basis-Images für Python bereit:

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
3.12	Python 3.12	Amazon Linux 2023	Dockerfile für Python 3.12 auf GitHub	
3.11	Python 3.11	Amazon Linux 2	Dockerfile für Python 3.11 auf GitHub	
3.10	Python 3.10	Amazon Linux 2	Dockerfile für Python 3.10 auf GitHub	
3.9	Python 3.9	Amazon Linux 2	Dockerfile für Python 3.9 auf GitHub	
3.8	Python 3.8	Amazon Linux 2	Dockerfile für Python 3.8 auf GitHub	14. Oktober 2024

Amazon-ECR-Repository: gallery.ecr.aws/lambda/python

Die Basis-Images von Python 3.12 und höher basieren auf dem minimalen Container-Image von Amazon Linux 2023. Die Python 3.8-3.11-Basis-Images basieren auf dem Amazon Linux 2-Image. AL2023-basierte Images bieten mehrere Vorteile gegenüber Amazon Linux 2, darunter einen geringeren Bereitstellungsaufwand und aktualisierte Versionen von Bibliotheken wie. `glibc`

AL2023-basierte Images verwenden `microdnf` (symbolisiert als`dnf`) als Paketmanager anstelle von`yum`, dem Standard-Paketmanager in Amazon Linux 2. `microdnf`ist eine eigenständige Implementierung von. `dnf` Eine Liste der Pakete, die in AL2023-basierten Images enthalten sind, finden Sie in den Spalten Minimal Container unter Comparing packages installed on Amazon Linux 2023 Container Images. Weitere Informationen zu den Unterschieden zwischen AL2023 und Amazon

Linux 2 finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.

> **Note**
>
> Um AL2023-basierte Images lokal auszuführen, auch mit AWS Serverless Application Model (AWS SAM), müssen Sie Docker-Version 20.10.10 oder höher verwenden.

Suchpfad für Abhängigkeiten in den Basis-Images

Wenn Sie in Ihrem Code eine `import`-Anweisung verwenden, durchsucht die Python-Laufzeit die Verzeichnisse in ihrem Suchpfad, bis sie das Modul oder Paket findet. Standardmäßig durchsucht die Laufzeit zuerst das Verzeichnis `{LAMBDA_TASK_ROOT}`. Wenn Sie eine Version einer in der Laufzeit enthaltenen Bibliothek in Ihr Image einfügen, hat Ihre Version Vorrang vor der Version, die in der Laufzeit enthalten ist.

Andere Schritte im Suchpfad hängen davon ab, welche Version des Lambda-Basis-Images für Python Sie verwenden:

- Python 3.11 und neuer: In der Laufzeit enthaltene Bibliotheken und über pip installierte Bibliotheken werden im Verzeichnis `/var/lang/lib/python3.11/site-packages` installiert. Dieses Verzeichnis hat im Suchpfad Vorrang vor `/var/runtime`. Sie können das SDK außer Kraft setzen, indem Sie pip verwenden, um eine neuere Version zu installieren. Sie können mithilfe von pip überprüfen, ob das in der Laufzeit enthaltene SDK und seine Abhängigkeiten mit allen Paketen kompatibel sind, die Sie installieren.
- Python 3.8-3.10: In der Laufzeit enthaltene Bibliotheken werden im Verzeichnis `/var/runtime` installiert. Über pip installierte Bibliotheken werden im Verzeichnis `/var/lang/lib/python3.x/site-packages` installiert. Das Verzeichnis `/var/runtime` hat im Suchpfad Vorrang vor `/var/lang/lib/python3.x/site-packages`.

Sie können den vollständigen Suchpfad für Ihre Lambda-Funktion sehen, indem Sie den folgenden Codeausschnitt hinzufügen.

```
import sys

search_path = sys.path
print(search_path)
```

Verwenden eines AWS Basis-Images für Python

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker (Mindestversion 20.10.10 für Python 3.12 und spätere Basis-Images)
- Python

Erstellen eines Images aus einem Base Image

So erstellen Sie ein Container-Image aus einem AWS Basis-Image für Python

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

   ```
   mkdir example
   cd example
   ```

2. Erstellen Sie eine neue Datei mit dem Namen `lambda_function.py`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example Python-Funktion

   ```
   import sys
   def handler(event, context):
       return 'Hello from AWS Lambda using Python' + sys.version + '!'
   ```

3. Erstellen Sie eine neue Datei mit dem Namen `requirements.txt`. Wenn Sie den Beispielfunktionscode aus dem vorherigen Schritt verwenden, können Sie die Datei leer lassen, da es keine Abhängigkeiten gibt. Andernfalls listen Sie jede benötigte Bibliothek auf. So sollte beispielsweise Ihre `requirements.txt` aussehen, wenn Ihre Funktion AWS SDK for Python (Boto3) verwendet:

   Example requirements.txt

   ```
   boto3
   ```

4. Erstellen Sie eine neue Docker-Datei mit der folgenden Konfiguration:

- Setzen Sie die FROM-Eigenschaft auf den URI des Basis-Images.
- Verwenden Sie den Befehl COPY, um den Funktionscode und die Laufzeitabhängigkeiten in eine von Lambda definierte Umgebungsvariable zu {LAMBDA_TASK_ROOT} kopieren.
- Legen Sie das CMD-Argument auf den Lambda-Funktionshandler fest.

Example Dockerfile

```
FROM public.ecr.aws/lambda/python:3.12

# Copy requirements.txt
COPY requirements.txt ${LAMBDA_TASK_ROOT}

# Install the specified packages
RUN pip install -r requirements.txt

# Copy function code
COPY lambda_function.py ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.handler" ]
```

5. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. In diesem Beispiel ist `docker-image` der Image-Name und `test` der Tag.

   ```
   docker run --platform linux/amd64 -p 9000:8080 docker-image:test
   ```

   Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis an den lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden Befehl aus: `Invoke-WebRequest`

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

Wenn Sie ein OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Laufzeitschnittstellen-Client erweitert die Lambda-Laufzeiten-API, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet.

Installieren Sie den Laufzeitschnittstellen-Client für Python mit dem pip-Paketmanager:

```
pip install awslambdaric
```

Sie können den Python-Runtime-Interface-Client auch von herunterladen GitHub.

Das folgende Beispiel zeigt, wie ein Container-Image für Python mit einem AWS Nicht-Base-Image erstellt wird. Das Beispiel-Dockerfile verwendet ein offizielles Python-Basis-Image. Das Dockerfile enthält den Laufzeitschnittstellen-Client für Python.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker
- Python

Erstellen eines Images aus einem alternativen Basis-Image

Um ein Container-Image aus einem AWS Nicht-Basis-Image zu erstellen

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir example
cd example
```

2. Erstellen Sie eine neue Datei mit dem Namen `lambda_function.py`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example Python-Funktion

   ```
   import sys
   def handler(event, context):
       return 'Hello from AWS Lambda using Python' + sys.version + '!'
   ```

3. Erstellen Sie eine neue Datei mit dem Namen `requirements.txt`. Wenn Sie den Beispielfunktionscode aus dem vorherigen Schritt verwenden, können Sie die Datei leer lassen, da es keine Abhängigkeiten gibt. Andernfalls listen Sie jede benötigte Bibliothek auf. So sollte beispielsweise Ihre `requirements.txt` aussehen, wenn Ihre Funktion AWS SDK for Python (Boto3) verwendet:

   Example requirements.txt

   ```
   boto3
   ```

4. Erstellen Sie eine neue Docker-Datei. Das folgende Dockerfile verwendet ein offizielles Python-Basis-Image anstelle eines AWS -Basis-Images. Das Dockerfile enthält den Laufzeitschnittstellen-Client, der das Image mit Lambda kompatibel macht. Die folgende Beispiel-Docker-Datei verwendet eine mehrstufige Entwicklung.

   - Legen Sie die `FROM`-Eigenschaft auf das Basis-Image fest.
   - Legen Sie `ENTRYPOINT` auf das Modul fest, das der Docker-Container beim Start ausführen soll. In diesem Fall ist das Modul der Laufzeitschnittstellen-Client.
   - Legen Sie `CMD` auf den Lambda-Funktionshandler fest.

   Example Dockerfile

   ```
   # Define custom function directory
   ARG FUNCTION_DIR="/function"

   FROM python:3.12 as build-image
   ```

```
# Include global arg in this stage of the build
ARG FUNCTION_DIR

# Copy function code
RUN mkdir -p ${FUNCTION_DIR}
COPY . ${FUNCTION_DIR}

# Install the function's dependencies
RUN pip install \
    --target ${FUNCTION_DIR} \
        awslambdaric

# Use a slim version of the base Python image to reduce the final image size
FROM python:3.12-slim

# Include global arg in this stage of the build
ARG FUNCTION_DIR
# Set working directory to function root directory
WORKDIR ${FUNCTION_DIR}

# Copy in the built dependencies
COPY --from=build-image ${FUNCTION_DIR} ${FUNCTION_DIR}

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/local/bin/python", "-m", "awslambdaric" ]
# Pass the name of the function handler as an argument to the runtime
CMD [ "lambda_function.handler" ]
```

5. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den

Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um das Image lokal zu testen. Sie können den Emulator in Ihr Image einbauen oder ihn mit dem folgenden Verfahren auf Ihrem lokalen Computer installieren.

Installieren des Laufzeitschnittstellen-Emulators auf Ihrem lokalen Computer

1. Führen Sie in Ihrem Projektverzeichnis den folgenden Befehl aus, um den Runtime-Interface-Emulator (x86-64-Architektur) herunterzuladen GitHub und auf Ihrem lokalen Computer zu installieren.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie die GitHub Repository-URL im vorherigen Befehl durch Folgendes:

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

Um den arm64-Emulator zu installieren, ersetzen Sie das `$downloadLink` durch Folgendes:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.
   - `/usr/local/bin/python -m awslambdaric lambda_function.handler` ist der `ENTRYPOINT` gefolgt von dem `CMD` aus Ihrem Dockerfile.

   Linux/macOS

   ```
   docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
    9000:8080 \
       --entrypoint /aws-lambda/aws-lambda-rie \
       docker-image:test \
           /usr/local/bin/python -m awslambdaric lambda_function.handler
   ```

   PowerShell

   ```
   docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
    9000:8080 `
   --entrypoint /aws-lambda/aws-lambda-rie `
   docker-image:test `
       /usr/local/bin/python -m awslambdaric lambda_function.handler
   ```

   Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

3. Veröffentlichen Sie ein Ereignis auf dem lokalen Endpunkt.

Linux/macOS

Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Die Container-ID erhalten.

```
docker ps
```

5. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --
   password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
   ```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

   ```
   aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
   scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
   ```

   > **Note**
   >
   > Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

   Wenn erfolgreich, sehen Sie eine Antwort wie diese:

   ```
   {
       "repository": {
           "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
   world",
           "registryId": "111122223333",
           "repositoryName": "hello-world",
           "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world",
           "createdAt": "2023-03-09T10:39:01+00:00",
           "imageTagMutability": "MUTABLE",
           "imageScanningConfiguration": {
               "scanOnPush": true
   ```

```
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:
   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

   Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Ein Beispiel für das Erstellen eines Python-Images aus einem Alpine-Basis-Image finden Sie unter Unterstützung für Container-Images für Lambda im AWS Blog.

Arbeiten mit Ebenen für Python-Lambda-Funktionen

Eine Lambda-Schicht ist ein ZIP-Dateiarchiv, das zusätzlichen Code oder Daten enthält. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien. Das Erstellen einer Ebene umfasst drei allgemeine Schritte:

1. Package Sie Ihren Layer-Inhalt. Das bedeutet, dass Sie ein ZIP-Dateiarchiv erstellen müssen, das die Abhängigkeiten enthält, die Sie in Ihren Funktionen verwenden möchten.
2. Erstellen Sie die Ebene in Lambda.
3. Fügen Sie die Ebene zu Ihren Funktionen hinzu.

Dieses Thema enthält Schritte und Anleitungen zum ordnungsgemäßen Verpacken und Erstellen einer Python-Lambda-Schicht mit externen Bibliotheksabhängigkeiten.

Themen

Voraussetzungen

Um die Schritte in diesem Abschnitt ausführen zu können, benötigen Sie Folgendes:

- Python 3.11 und das Pip-Paketinstallationsprogramm
- AWS Command Line Interface (AWS CLI) Version 2

In diesem Thema verweisen wir auf die `layer-python`Beispielanwendung im awsdocs-Repository GitHub . Diese Anwendung enthält Skripte, die die Abhängigkeiten herunterladen und die Ebenen generieren. Die Anwendung enthält auch entsprechende Funktionen, die Abhängigkeiten von den Ebenen nutzen. Nachdem Sie eine Ebene erstellt haben, können Sie die entsprechende Funktion

bereitstellen und aufrufen, um zu überprüfen, ob alles ordnungsgemäß funktioniert. Da Sie die Python 3.11-Laufzeit für die Funktionen verwenden, müssen die Layer auch mit Python 3.11 kompatibel sein.

In der `layer-python` Beispielanwendung gibt es zwei Beispiele:

- Das erste Beispiel beinhaltet das Verpacken der `requests`Bibliothek in eine Lambda-Schicht. Das `layer/` Verzeichnis enthält die Skripte zum Generieren der Ebene. Das `function/` Verzeichnis enthält eine Beispielfunktion, mit deren Hilfe getestet werden kann, ob der Layer funktioniert. Der Großteil dieses Tutorials erklärt, wie dieser Layer erstellt und verpackt wird.
- Das zweite Beispiel beinhaltet das Verpacken der numpyBibliothek in eine Lambda-Schicht. Das `layer-numpy/` Verzeichnis enthält die Skripte zum Generieren der Ebene. Das `function-numpy/` Verzeichnis enthält eine Beispielfunktion, mit deren Hilfe getestet werden kann, ob der Layer funktioniert. Ein Beispiel für das Erstellen und Verpacken dieses Layers finden Sie unterthe section called “Mit `manylinux` Radverteilungen arbeiten”.

Python-Layer-Kompatibilität mit Amazon Linux

Der erste Schritt beim Erstellen einer Ebene besteht darin, den gesamten Ebeneninhalt in einem ZIP-Dateiarchiv zu bündeln. Da Lambda-Funktionen unter Amazon Linux ausgeführt werden, muss Ihr Ebeneninhalt in einer Linux-Umgebung kompiliert und erstellt werden können.

In Python sind die meisten Pakete zusätzlich zur Quelldistribution als Räder (`.whl`Dateien) verfügbar. Jedes Rad ist eine Art von gebauter Distribution, die eine bestimmte Kombination von Python-Versionen, Betriebssystemen und Maschinenbefehlssätzen unterstützt.

Räder sind nützlich, um sicherzustellen, dass Ihr Layer mit Amazon Linux kompatibel ist. Wenn Sie Ihre Abhängigkeiten herunterladen, laden Sie nach Möglichkeit das Universal Wheel herunter. (Standardmäßig `pip` wird das Universalrad installiert, sofern eines verfügbar ist.) Das Universalrad enthält `any` als Plattform-Tag, was darauf hinweist, dass es mit allen Plattformen, einschließlich Amazon Linux, kompatibel ist.

Im folgenden Beispiel packen Sie die `requests` Bibliothek in eine Lambda-Schicht. Die `requests` Bibliothek ist ein Beispiel für ein Paket, das als Universalrad verfügbar ist.

Nicht alle Python-Pakete werden als Universalräder vertrieben. numpyHat beispielsweise mehrere Radverteilungen, von denen jede eine andere Gruppe von Plattformen unterstützt. Laden Sie für solche Pakete die `manylinux` Distribution herunter, um die Kompatibilität mit Amazon Linux sicherzustellen. Eine ausführliche Anleitung zum Verpacken solcher Ebenen finden Sie unterthe section called “Mit `manylinux` Radverteilungen arbeiten”.

In seltenen Fällen ist ein Python-Paket möglicherweise nicht als Rad verfügbar. Wenn nur die Quelldistribution (sdist) existiert, empfehlen wir, Ihre Abhängigkeiten in einer Docker-Umgebung zu installieren und zu verpacken, die auf dem Amazon Linux 2023-Basiscontainer-Image basiert. Wir empfehlen diesen Ansatz auch, wenn Sie Ihre eigenen benutzerdefinierten Bibliotheken einbeziehen möchten, die in anderen Sprachen wie C/C++ geschrieben sind. Dieser Ansatz ahmt die Lambda-Ausführungsumgebung in Docker nach und stellt sicher, dass Ihre Nicht-Python-Paketabhängigkeiten mit Amazon Linux kompatibel sind.

Layer-Pfade für Python-Laufzeiten

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Layer-Inhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

- `python`
- `python/lib/python3.x/site-packages`

Die resultierende Layer-ZIP-Datei, die Sie in diesem Tutorial erstellen, hat beispielsweise die folgende Verzeichnisstruktur:

```
layer_content.zip
# python
    # lib
        # python3.11
            # site-packages
                # requests
                # <other_dependencies> (i.e. dependencies of the requests package)
                # ...
```

Die `requests`Bibliothek befindet sich korrekt im `python/lib/python3.11/site-packages` Verzeichnis. Dadurch wird sichergestellt, dass Lambda die Bibliothek bei Funktionsaufrufen finden kann.

Verpacken des Layer-Inhalts

In diesem Beispiel packen Sie die `requests` Python-Bibliothek in eine Layer-.zip-Datei. Führen Sie die folgenden Schritte aus, um den Layer-Inhalt zu installieren und zu verpacken.

So installieren und verpacken Sie Ihre Layer-Inhalte

1. Klonen Sie das aws-lambda-developer-guide GitHub Repo, das den Beispielcode enthält, den Sie im `sample-apps/layer-python` Verzeichnis benötigen.

   ```
   git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
   ```

2. Navigieren Sie zum `layer` Verzeichnis der `layer-python` Beispiel-App. Dieses Verzeichnis enthält die Skripts, die Sie verwenden, um den Layer ordnungsgemäß zu erstellen und zu verpacken.

   ```
   cd aws-lambda-developer-guide/sample-apps/layer-python/layer
   ```

3. Untersuchen Sie die `requirements.txt`Datei. Diese Datei definiert die Abhängigkeiten, die Sie in die Ebene aufnehmen möchten, nämlich die `requests` Bibliothek. Sie können diese Datei so aktualisieren, dass sie alle Abhängigkeiten enthält, die Sie in Ihre eigene Ebene aufnehmen möchten.

   Example requirements.txt

   ```
   requests==2.31.0
   ```

4. Stellen Sie sicher, dass Sie berechtigt sind, beide Skripts auszuführen.

   ```
   chmod 744 1-install.sh && chmod 744 2-package.sh
   ```

5. Führen Sie das `1-install.sh`Skript mit dem folgenden Befehl aus:

   ```
   ./1-install.sh
   ```

   Dieses Skript verwendet`venv`, um eine virtuelle Python-Umgebung mit dem Namen zu erstellen`create_layer`. Anschließend werden alle erforderlichen Abhängigkeiten im `create_layer/lib/python3.11/site-packages` Verzeichnis installiert.

   Example 1-install.sh

   ```
   python3.11 -m venv create_layer
   source create_layer/bin/activate
   pip install -r requirements.txt
   ```

6. Führen Sie das `2-package.sh`Skript mit dem folgenden Befehl aus:

```
./2-package.sh
```

Dieses Skript kopiert den Inhalt aus dem `create_layer/lib` Verzeichnis in ein neues Verzeichnis mit dem Namen`python`. Anschließend komprimiert es den Inhalt des `python` Verzeichnisses in eine Datei mit dem Namen`layer_content.zip`. Dies ist die ZIP-Datei für Ihren Layer. Sie können die Datei entpacken und überprüfen, ob sie die richtige Dateistruktur enthält, wie im the section called “Layer-Pfade für Python-Laufzeiten” Abschnitt gezeigt.

Example 2-package.sh

```
mkdir python
cp -r create_layer/lib python/
zip -r layer_content.zip python
```

Die Ebene erstellen

In diesem Abschnitt nehmen Sie die `layer_content.zip` Datei, die Sie im vorherigen Abschnitt generiert haben, und laden sie als Lambda-Schicht hoch. Sie können eine Ebene mit der AWS Management Console oder der Lambda-API über die AWS Command Line Interface (AWS CLI) hochladen. Wenn Sie Ihre Layer-.zip-Datei hochladen, geben Sie `python3.11` im folgenden PublishLayerVersion AWS CLI Befehl die kompatible Laufzeit und die kompatible `arm64` Architektur an.

```
aws lambda publish-layer-version --layer-name python-requests-layer \
    --zip-file fileb://layer_content.zip \
    --compatible-runtimes python3.11 \
    --compatible-architectures "arm64"
```

Notieren Sie sich aus der Antwort den`LayerVersionArn`, der wie `arn:aws:lambda:us-east-1:`*`123456789012`*`:layer:python-requests-layer:1` aussieht. Sie benötigen diesen Amazon-Ressourcennamen (ARN) im nächsten Schritt dieses Tutorials, wenn Sie den Layer zu Ihrer Funktion hinzufügen.

Hinzufügen der Ebene zu Ihrer Funktion

In diesem Abschnitt stellen Sie eine Lambda-Beispielfunktion bereit, die die `requests` Bibliothek in ihrem Funktionscode verwendet, und fügen dann den Layer hinzu. Um die Funktion bereitzustellen, benötigen Sie einethe section called “Ausführungsrolle (Berechtigungen für Funktionen zum Zugriff auf andere Ressourcen)”. Wenn Sie noch keine Ausführungsrolle haben, folgen Sie den Schritten im Abschnitt „Zusammenklappbar“. Fahren Sie andernfalls mit dem nächsten Abschnitt fort, um die Funktion bereitzustellen.

(Optional) Erstellen Sie eine Ausführungsrolle

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.
   - Trusted entity (Vertrauenswürdige Entität) – Lambda.
   - Berechtigungen — AWSLambdaBasicExecutionRole.
   - Role name (Name der Rolle – **`lambda-role`**.

   Die AWSLambdaBasicExecutionRoleRichtlinie verfügt über die Berechtigungen, die die Funktion benötigt, um Protokolle in Logs zu CloudWatch schreiben.

So stellen Sie die Lambda-Funktion bereit

1. Navigieren Sie zum `function/` Verzeichnis . Wenn Sie sich derzeit in dem `layer/` Verzeichnis befinden, führen Sie den folgenden Befehl aus:

   ```
   cd ../function
   ```

2. Überprüfen Sie den Funktionscode. Die Funktion importiert die `requests` Bibliothek, stellt eine einfache HTTP-GET-Anfrage und gibt dann den Statuscode und den Hauptteil zurück.

   ```
   import requests

   def lambda_handler(event, context):
       print(f"Version of requests library: {requests.__version__}")
   ```

```
    request = requests.get('https://api.github.com/')
    return {
        'statusCode': request.status_code,
        'body': request.text
    }
```

3. Erstellen Sie mit dem folgenden Befehl ein Bereitstellungspaket für eine ZIP-Datei:

```
zip my_deployment_package.zip lambda_function.py
```

4. Stellen Sie die Funktion bereit. Ersetzen Sie im folgenden AWS CLI Befehl den `--role` Parameter durch den ARN Ihrer Ausführungsrolle:

```
aws lambda create-function --function-name python_function_with_layer \
    --runtime python3.11 \
    --architectures "arm64" \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::123456789012:role/lambda-role \
    --zip-file fileb://my_deployment_package.zip
```

(Optional) Rufen Sie Ihre Funktion auf, ohne eine Ebene anzuhängen

An dieser Stelle können Sie optional versuchen, Ihre Funktion aufzurufen, bevor Sie den Layer anhängen. Wenn Sie dies versuchen, sollten Sie einen Importfehler erhalten, da Ihre Funktion nicht auf das `requests` Paket verweisen kann. Verwenden Sie den folgenden AWS CLI Befehl, um Ihre Funktion aufzurufen:

```
aws lambda invoke --function-name python_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "key": "value" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "StatusCode": 200,
    "FunctionError": "Unhandled",
    "ExecutedVersion": "$LATEST"
}
```

Um den spezifischen Fehler anzuzeigen, öffnen Sie die `response.json` Ausgabedatei. Sie sollten eine `ImportModuleError` mit der folgenden Fehlermeldung sehen:

```
"errorMessage": "Unable to import module 'lambda_function': No module named 'requests'"
```

Als Nächstes fügen Sie die Ebene Ihrer Funktion hinzu. Ersetzen Sie im folgenden AWS CLI Befehl den `--layers` Parameter durch den ARN der Layer-Version, den Sie zuvor notiert haben:

```
aws lambda update-function-configuration --function-name python_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --layers "arn:aws:lambda:us-east-1:123456789012:layer:python-requests-layer:1"
```

Versuchen Sie abschließend, Ihre Funktion mit dem folgenden AWS CLI Befehl aufzurufen:

```
aws lambda invoke --function-name python_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "key": "value" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

Die `response.json` Ausgabedatei enthält Details zur Antwort.

(Optional) Bereinigen Sie Ihre Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

Um die Lambda-Ebene zu löschen

1. Öffnen Sie die Seite Ebenen der Lambda-Konsole.
2. Wählen Sie die Ebene aus, die Sie erstellt haben.
3. Wählen Sie „Löschen“ und anschließend erneut „Löschen“.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

Mit **`manylinux`** Radverteilungen arbeiten

Manchmal hat ein Paket, das Sie als Abhängigkeit einschließen möchten, kein universelles Rad (insbesondere nicht `any` als Plattform-Tag). Laden Sie in diesem Fall `manylinux` stattdessen das Rad herunter, das unterstützt. Dadurch wird sichergestellt, dass Ihre Layer-Bibliotheken mit Amazon Linux kompatibel sind.

`numpy`ist ein Paket, das kein Universalrad hat. Wenn Sie das `numpy` Paket in Ihren Layer aufnehmen möchten, können Sie die folgenden Beispielschritte ausführen, um Ihren Layer ordnungsgemäß zu installieren und zu verpacken.

So installieren und verpacken Sie Ihren Layer-Inhalt

1. Klonen Sie das `aws-lambda-developer-guide` GitHub Repo, das den Beispielcode enthält, den Sie im `sample-apps/layer-python` Verzeichnis benötigen.

   ```
   git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
   ```

2. Navigieren Sie zum `layer-numpy` Verzeichnis der `layer-python` Beispiel-App. Dieses Verzeichnis enthält die Skripts, die Sie verwenden, um den Layer ordnungsgemäß zu erstellen und zu verpacken.

   ```
   cd aws-lambda-developer-guide/sample-apps/layer-python/layer-numpy
   ```

3. Untersuchen Sie die `requirements.txt`Datei. Diese Datei definiert die Abhängigkeiten, die Sie in Ihren Layer aufnehmen möchten, nämlich die `numpy` Bibliothek. Hier geben Sie die URL der `manylinux` Radverteilung an, die mit Python 3.11, Amazon Linux und dem `x86_64` Befehlssatz kompatibel ist:

Example requirements.txt

```
https://files.pythonhosted.org/packages/3a/d0/
edc009c27b406c4f9cbc79274d6e46d634d139075492ad055e3d68445925/numpy-1.26.4-cp311-
cp311-manylinux_2_17_x86_64.manylinux2014_x86_64.whl
```

4. Stellen Sie sicher, dass Sie berechtigt sind, beide Skripts auszuführen.

```
chmod 744 1-install.sh && chmod 744 2-package.sh
```

5. Führen Sie das `1-install.sh`Skript mit dem folgenden Befehl aus:

```
./1-install.sh
```

Dieses Skript verwendet`venv`, um eine virtuelle Python-Umgebung mit dem Namen zu erstellen`create_layer`. Anschließend werden alle erforderlichen Abhängigkeiten im `create_layer/lib/python3.11/site-packages` Verzeichnis installiert. Der `pip` Befehl ist in diesem Fall anders, da Sie das `--platform` Tag als angeben müssen`manylinux2014_x86_64`. Dies weist darauf `pip` hin, dass Sie das richtige `manylinux` Rad installieren müssen, auch wenn Ihr lokaler Computer macOS oder Windows verwendet.

Example 1-install.sh

```
python3.11 -m venv create_layer
source create_layer/bin/activate
pip install -r requirements.txt --platform=manylinux2014_x86_64 --only-binary=:all:
 --target ./create_layer/lib/python3.11/site-packages
```

6. Führen Sie das `2-package.sh`Skript mit dem folgenden Befehl aus:

```
./2-package.sh
```

Dieses Skript kopiert den Inhalt aus dem `create_layer/lib` Verzeichnis in ein neues Verzeichnis mit dem Namen`python`. Anschließend komprimiert es den Inhalt des `python` Verzeichnisses in eine Datei mit dem Namen`layer_content.zip`. Dies ist die ZIP-Datei für Ihren Layer. Sie können die Datei entpacken und überprüfen, ob sie die richtige Dateistruktur enthält, wie im the section called “Layer-Pfade für Python-Laufzeiten” Abschnitt gezeigt.

Example 2-package.sh

```
mkdir python
cp -r create_layer/lib python/
zip -r layer_content.zip python
```

Verwenden Sie den folgenden PublishLayerVersion AWS CLI Befehl, um diese Ebene auf Lambda hochzuladen:

```
aws lambda publish-layer-version --layer-name python-numpy-layer \
    --zip-file fileb://layer_content.zip \
    --compatible-runtimes python3.11 \
    --compatible-architectures "x86_64"
```

Notieren Sie sich aus der Antwort den`LayerVersionArn`, der wie `arn:aws:lambda:us-east-1:`*`123456789012`*`:layer:python-numpy-layer:1` aussieht. Um zu überprüfen, ob Ihr Layer wie erwartet funktioniert, stellen Sie die Lambda-Funktion im `function-numpy` Verzeichnis bereit.

So stellen Sie die Lambda-Funktion bereit

1. Navigieren Sie zum `function-numpy/` Verzeichnis . Wenn Sie sich derzeit in dem `layer-numpy/` Verzeichnis befinden, führen Sie den folgenden Befehl aus:

   ```
   cd ../function-numpy
   ```

2. Überprüfen Sie den Funktionscode. Die Funktion importiert die numpy Bibliothek, erstellt ein einfaches numpy Array und gibt dann einen Dummy-Statuscode und einen Hauptteil zurück.

   ```
   import json
   import numpy as np

   def lambda_handler(event, context):

       x = np.arange(15, dtype=np.int64).reshape(3, 5)
       print(x)

       return {
           'statusCode': 200,
   ```

```
        'body': json.dumps('Hello from Lambda!')
    }
```

3. Erstellen Sie mit dem folgenden Befehl ein Bereitstellungspaket für eine ZIP-Datei:

```
zip my_deployment_package.zip lambda_function.py
```

4. Stellen Sie die Funktion bereit. Ersetzen Sie im folgenden AWS CLI Befehl den `--role` Parameter durch den ARN Ihrer Ausführungsrolle:

```
aws lambda create-function --function-name python_function_with_numpy \
    --runtime python3.11 \
    --handler lambda_function.lambda_handler \
    --role arn:aws:iam::123456789012:role/lambda-role \
    --zip-file fileb://my_deployment_package.zip
```

(Optional) Rufen Sie Ihre Funktion auf, ohne eine Ebene anzuhängen

Optional können Sie versuchen, Ihre Funktion aufzurufen, bevor Sie den Layer anhängen. Wenn Sie dies versuchen, sollten Sie einen Importfehler erhalten, da Ihre Funktion nicht auf das numpy Paket verweisen kann. Verwenden Sie den folgenden AWS CLI Befehl, um Ihre Funktion aufzurufen:

```
aws lambda invoke --function-name python_function_with_numpy \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "key": "value" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "StatusCode": 200,
    "FunctionError": "Unhandled",
    "ExecutedVersion": "$LATEST"
}
```

Um den spezifischen Fehler anzuzeigen, öffnen Sie die `response.json` Ausgabedatei. Sie sollten eine `ImportModuleError` mit der folgenden Fehlermeldung sehen:

```
"errorMessage": "Unable to import module 'lambda_function': No module named 'numpy'"
```

Als Nächstes fügen Sie die Ebene Ihrer Funktion hinzu. Ersetzen Sie im folgenden AWS CLI Befehl den `--layers` Parameter durch den ARN Ihrer Layer-Version:

```
aws lambda update-function-configuration --function-name python_function_with_numpy \
    --cli-binary-format raw-in-base64-out \
    --layers "arn:aws:lambda:us-east-1:123456789012:layer:python-requests-layer:1"
```

Versuchen Sie abschließend, Ihre Funktion mit dem folgenden AWS CLI Befehl aufzurufen:

```
aws lambda invoke --function-name python_function_with_numpy \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "key": "value" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

Sie können anhand der Funktionsprotokolle überprüfen, ob der Code das numpy Array standardmäßig ausgibt.

AWS Lambda-Context-Objekt in Python

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit. Weitere Informationen darüber, wie das Kontextobjekt an den Funktions-Handler übergeben wird, finden Sie unter Definieren Sie den Lambda-Funktionshandler in Python.

Context-Methoden

- `get_remaining_time_in_millis` – Gibt die Anzahl der verbleibenden Millisekunden zurück, bevor die Ausführung das Zeitlimit überschreitet.

Context-Eigenschaften

- `function_name` – Der Name der Lambda-Funktion.
- `function_version` – Die Version der Funktion.
- `invoked_function_arn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `memory_limit_in_mb` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `aws_request_id` – Der Bezeichner der Aufrufanforderung.
- `log_group_name` – Protokollgruppe für die Funktion.
- `log_stream_name` – Der Protokollstream für die Funktions-Instance.
- `identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
  - `cognito_identity_id`— Die authentifizierte Amazon-Cognito-Identität.
  - `cognito_identity_pool_id` – Der Amazon-Cognito-Identitätspool, der den Aufruf autorisiert hat.
- `client_context` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.
  - `client.installation_id`
  - `client.app_title`
  - `client.app_version_name`
  - `client.app_version_code`
  - `client.app_package_name`

- `custom` – Ein `dict` mit benutzerdefinierten Werten, die von der mobilen Clientanwendung festgelegt wurden.
- `env` – Ein `dict` mit Umgebungsinformationen, die vom AWS SDK bereitgestellt wurden.

Das folgende Beispiel zeigt eine Handler-Funktion zur Protokollierung von Context-Informationen.

Example handler.py

```
import time

def lambda_handler(event, context):
    print("Lambda function ARN:", context.invoked_function_arn)
    print("CloudWatch log stream name:", context.log_stream_name)
    print("CloudWatch log group name:",  context.log_group_name)
    print("Lambda Request ID:", context.aws_request_id)
    print("Lambda function memory limits in MB:", context.memory_limit_in_mb)
    # We have added a 1 second delay so you can see the time remaining in
 get_remaining_time_in_millis.
    time.sleep(1)
    print("Lambda time remaining in MS:", context.get_remaining_time_in_millis())
```

Zusätzlich zu den oben aufgeführten Optionen können Sie das AWS X-Ray-SDK für Instrumentierung von Python-Code in AWS Lambda zudem verwenden, um kritische Code-Pfade zu identifizieren, deren Leistung nachzuverfolgen und die Daten für die Analyse zu erfassen.

AWS Lambda Funktionsprotokollierung in Python

AWS Lambda überwacht automatisch Lambda-Funktionen und sendet Protokolleinträge an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen zu CloudWatch Logs finden Sie unterVerwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Zur Ausgabe von Protokollen aus Ihrem Funktionscode können Sie das integrierte `logging`-Modul verwenden. Für detailliertere Einträge können Sie jede Protokollierungsbibliothek verwenden, die in `stdout` oder `stderr` schreibt.

Ausdrucken in das Protokoll

Um eine grundlegende Ausgabe an die Protokolle zu senden, können Sie in Ihrer Funktion eine `print`-Methode verwenden. Im folgenden Beispiel werden die Werte der CloudWatch Loggruppe und des Streams Logs sowie das Event-Objekt protokolliert.

Beachten Sie, dass Lambda Protokollausgaben nur im Klartextformat an Logs senden kann, wenn Ihre Funktion CloudWatch Logs mithilfe von `print` Python-Anweisungen ausgibt. Um Protokolle in strukturiertem JSON zu erfassen, müssen Sie eine unterstützte Protokollierungsbibliothek verwenden. Weitere Informationen finden Sie unter the section called “Verwenden von Lambda-Optionen für die erweiterte Protokollierung mit Python”.

Example lambda_function.py

```
import os
def lambda_handler(event, context):
    print('## ENVIRONMENT VARIABLES')
    print(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    print(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    print('## EVENT')
    print(event)
```

Example Protokollausgabe

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
```

```
/aws/lambda/my-function
2023/08/31/[$LATEST]3893xmpl7fac4485b47bb75b671a283c
## EVENT
{'key': 'value'}
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95  Duration: 15.74 ms  Billed
 Duration: 16 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmplf1fb44f07bc535a1   SegmentId: 07f5xmpl2d1f6f85
 Sampled: true
```

Die Python-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die `REPORT`-Zeile enthält die folgenden Daten:

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.
- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Verwendung einer Protokollierungsbibliothek

Für detailliertere Protokolle verwenden Sie das Modul zur Protokollierung in der Standardbibliothek oder eine beliebige Protokollierungsbibliothek eines Drittanbieters, die in `stdout` oder `stderr` schreibt.

Für unterstützte Python-Laufzeiten können Sie wählen, ob mit dem `logging`-Standardmodul erstellte Protokolle im Klartext oder in JSON erfasst werden. Weitere Informationen hierzu finden Sie unter the section called “Verwenden von Lambda-Optionen für die erweiterte Protokollierung mit Python”.

Derzeit ist das Standard-Protokollformat für alle Python-Laufzeiten das Klartextformat. Das folgende Beispiel zeigt, wie Protokollausgaben, die mit dem `logging` Standardmodul erstellt wurden, im Klartext in CloudWatch Logs erfasst werden.

```
import os
import logging
logger = logging.getLogger()
logger.setLevel("INFO")

def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES')
    logger.info(os.environ['AWS_LAMBDA_LOG_GROUP_NAME'])
    logger.info(os.environ['AWS_LAMBDA_LOG_STREAM_NAME'])
    logger.info('## EVENT')
    logger.info(event)
```

Die Ausgabe aus `logger` umfasst die Protokollebene, den Zeitstempel und die Anforderungs-ID.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO]  2023-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ##
 ENVIRONMENT VARIABLES
[INFO]  2023-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    /aws/
lambda/my-function
[INFO]  2023-08-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    2023/01/31/
[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d
[INFO]  2023-08-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ## EVENT
[INFO]  2023-08-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    {'key':
 'value'}
END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125  Duration: 2.75 ms   Billed
 Duration: 3 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl7c2534a87870b4370   SegmentId: 073cxmpl3e442861
 Sampled: true
```

> **Note**
>
> Wenn das Protokollformat Ihrer Funktion auf Klartext gesetzt ist, lautet die Standardeinstellung auf Protokollebene für Python-Laufzeiten WARN. Das bedeutet, dass Lambda nur Protokollausgaben der Stufe WARN und niedriger an CloudWatch Logs sendet. Um die Standardprotokollebene zu ändern, verwenden Sie die Python-

Methode `logging setLevel()`, wie in diesem Beispielcode gezeigt. Wenn Sie das Protokollformat Ihrer Funktion auf JSON setzen, empfehlen wir, die Protokollebene der Funktion mithilfe der erweiterten Lambda Advanced Logging Controls zu konfigurieren und nicht die Protokollebene im Code festzulegen. Weitere Informationen hierzu finden Sie unter the section called “Verwenden der Filterung auf Protokollebene mit Python”.

Verwenden von Lambda-Optionen für die erweiterte Protokollierung mit Python

Um Ihnen mehr Kontrolle darüber zu geben, wie die Protokolle Ihrer Funktionen erfasst, verarbeitet und verwendet werden, können Sie die folgenden Protokollierungsoptionen für unterstützte Lambda-Python-Laufzeiten konfigurieren:

- Protokollformat – Wählen Sie zwischen Klartext und einem strukturierten JSON-Format für die Protokolle Ihrer Funktion aus.
- Protokollebene — für Logs im JSON-Format wählen Sie die Detailebene der Logs, die Lambda an Amazon sendet CloudWatch, wie ERROR, DEBUG oder INFO
- Protokollgruppe — wählen Sie die CloudWatch Protokollgruppe aus, an die Ihre Funktion Protokolle sendet

Weitere Informationen zu diesen Protokollierungsoptionen und Anweisungen zur Konfiguration Ihrer Funktion für deren Verwendung finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.

Weitere Informationen zur Verwendung der Optionen für das Protokollformat und die Protokollebene mit Ihren Python-Lambda-Funktionen finden Sie in den folgenden Abschnitten.

Verwenden strukturierter JSON-Protokolle mit Python

Wenn Sie JSON für das Protokollformat Ihrer Funktion auswählen, sendet Lambda die von der Python-Standard-Logging-Bibliothek ausgegebenen Logs CloudWatch als strukturiertes JSON an. Jedes JSON-Protokollobjekt enthält mindestens vier Schlüssel-Wert-Paare mit den folgenden Schlüsseln:

- `"timestamp"` – die Uhrzeit, zu der die Protokollmeldung generiert wurde
- `"level"` – die der Meldung zugewiesene Protokollebene

- `"message"` – der Inhalt der Protokollmeldung
- `"requestId"` – die eindeutige Anforderungs-ID für den Funktionsaufruf

Die `logging`-Bibliothek von Python kann auch zusätzliche Schlüssel-Wert-Paare wie `"logger"` zu diesem JSON-Objekt hinzufügen.

Die Beispiele in den folgenden Abschnitten zeigen, wie mit der `logging` Python-Bibliothek generierte Protokollausgaben in CloudWatch Logs erfasst werden, wenn Sie das Protokollformat Ihrer Funktion als JSON konfigurieren.

Beachten Sie Folgendes: Wenn Sie die `print`-Methode verwenden, um grundlegende Protokollausgaben zu erzeugen, wie unter the section called “Ausdrucken in das Protokoll” beschrieben, erfasst Lambda diese Ausgaben als Klartext, auch wenn Sie das Protokollierungsformat Ihrer Funktion als JSON konfigurieren.

Standard-JSON-Protokollausgaben mithilfe der Python-Protokollierungsbibliothek

Der folgende Beispielcodeausschnitt und die Protokollausgabe zeigen, wie mit der `logging` Python-Bibliothek generierte Standardprotokollausgaben in CloudWatch Logs erfasst werden, wenn das Protokollformat Ihrer Funktion auf JSON gesetzt ist.

Example Python-Protokollierungscode

```
import logging
logger = logging.getLogger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example JSON-Protokolldatensatz

```
{
    "timestamp":"2023-10-27T19:17:45.586Z",
    "level":"INFO",
    "message":"Inside the handler function",
    "logger": "root",
    "requestId":"79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Protokollieren zusätzlicher Parameter in JSON

Wenn das Protokollformat Ihrer Funktion auf JSON gesetzt ist, können Sie auch zusätzliche Parameter mit der `logging` Python-Standardbibliothek protokollieren, indem Sie das `extra` Schlüsselwort verwenden, um ein Python-Wörterbuch an die Protokollausgabe zu übergeben.

Example Python-Protokollierungscode

```
import logging

def lambda_handler(event, context):
    logging.info(
        "extra parameters example",
        extra={"a":"b", "b": [3]},
    )
```

Example JSON-Protokolldatensatz

```
{
  "timestamp": "2023-11-02T15:26:28Z",
  "level": "INFO",
  "message": "extra parameters example",
  "logger": "root",
  "requestId": "3dbd5759-65f6-45f8-8d7d-5bdc79a3bd01",
  "a": "b",
  "b": [
    3
  ]
}
```

Protokollierungsausnahmen in JSON

Der folgende Codeausschnitt zeigt, wie Python-Ausnahmen in der Protokollausgabe Ihrer Funktion erfasst werden, wenn Sie das Protokollformat als JSON konfigurieren. Beachten Sie, dass den mit `logging.exception` generierten Protokollausgaben die Protokollebene ERROR zugewiesen wird.

Example Python-Protokollierungscode

```
import logging

def lambda_handler(event, context):
```

```
    try:
        raise Exception("exception")
    except:
        logging.exception("msg")
```

Example JSON-Protokolldatensatz

```
{
  "timestamp": "2023-11-02T16:18:57Z",
  "level": "ERROR",
  "message": "msg",
  "logger": "root",
  "stackTrace": [
    "  File \"/var/task/lambda_function.py\", line 15, in lambda_handler\n    raise
 Exception(\"exception\")\n"
  ],
  "errorType": "Exception",
  "errorMessage": "exception",
  "requestId": "3f9d155c-0f09-46b7-bdf1-e91dab220855",
  "location": "/var/task/lambda_function.py:lambda_handler:17"
}
```

Strukturierte JSON-Protokolle mit anderen Protokollierungstools

Wenn Ihr Code bereits eine andere Logging-Bibliothek wie Powertools for verwendet AWS Lambda, um strukturierte JSON-Logs zu erstellen, müssen Sie keine Änderungen vornehmen. AWS Lambda codiert keine Logs doppelt, die bereits JSON-kodiert sind. Selbst wenn Sie Ihre Funktion so konfigurieren, dass sie das JSON-Protokollformat verwendet, erscheinen Ihre Logging-Ausgaben CloudWatch in der von Ihnen definierten JSON-Struktur.

Das folgende Beispiel zeigt, wie Protokollausgaben, die mit dem AWS Lambda Paket Powertools for generiert wurden, in CloudWatch Logs erfasst werden. Das Format dieser Protokollausgabe ist dasselbe, unabhängig davon, ob die Protokollierungskonfiguration Ihrer Funktion auf JSON oder TEXT festgelegt ist. Weitere Informationen zur Verwendung von Powertools für finden Sie unter AWS Lambda und the section called “Verwendung von Powertools für AWS Lambda (Python) und AWS SAM für strukturiertes Logging” the section called “Verwendung von Powertools für AWS Lambda (Python) und AWS CDK für strukturiertes Logging”

Example Codeausschnitt für die Python-Protokollierung (mit Powertools für) AWS Lambda

```
from aws_lambda_powertools import Logger
```

```
logger = Logger()

def lambda_handler(event, context):
    logger.info("Inside the handler function")
```

Example JSON-Protokolldatensatz (unter Verwendung von Powertools für) AWS Lambda

```
{
    "level": "INFO",
    "location": "lambda_handler:7",
    "message": "Inside the handler function",
    "timestamp": "2023-10-31 22:38:21,010+0000",
    "service": "service_undefined",
    "xray_trace_id": "1-654181dc-65c15d6b0fecbdd1531ecb30"
}
```

Verwenden der Filterung auf Protokollebene mit Python

Durch die Konfiguration der Filterung auf Protokollebene können Sie festlegen, dass nur Protokolle mit einer bestimmten Protokollierungsebene oder niedriger an Logs gesendet werden. CloudWatch Informationen zur Konfiguration der Filterung auf Protokollebene für Ihre Funktion finden Sie unter the section called “Filterung auf Protokollebene”.

AWS Lambda Um Ihre Anwendungsprotokolle nach ihrer Protokollebene zu filtern, muss Ihre Funktion Protokolle im JSON-Format verwenden. Sie können dies auf zwei Arten erreichen:

- Erstellen Sie Protokollausgaben mit der `logging`-Python-Standardbibliothek und konfigurieren Sie Ihre Funktion so, dass sie die JSON-Protokollformatierung verwendet. AWS Lambda filtert dann Ihre Protokollausgaben mithilfe des Schlüssel-Wert-Paars „level“ im JSON-Objekt, wie unter the section called “Verwenden strukturierter JSON-Protokolle mit Python” beschrieben. Informationen zur Konfiguration des Protokollformats Ihrer Funktion finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.
- Verwenden Sie eine andere Protokollierungsbibliothek oder Methode, um strukturierte JSON-Protokolle in Ihrem Code zu erstellen, die ein „level“-Schlüssel-Wert-Paar enthalten, das die Ebene der Protokollausgabe definiert. Sie können Powertools beispielsweise verwenden, AWS Lambda um strukturierte JSON-Protokollausgaben aus Ihrem Code zu generieren.

  Sie können auch eine „print“-Anweisung verwenden, um ein JSON-Objekt auszugeben, das eine Protokollebenenkennung enthält. Die folgende Print-Anweisung erzeugt eine Ausgabe im JSON-

Format, bei der die Protokollebene auf INFO gesetzt ist. AWS Lambda sendet das JSON-Objekt an CloudWatch Logs, wenn die Protokollierungsebene Ihrer Funktion auf INFO, DEBUG oder TRACE gesetzt ist.

```
print('{"msg":"My log message", "level":"info"}')
```

Damit Lambda die Protokolle Ihrer Funktion filtern kann, müssen Sie auch ein `"timestamp"`-Schlüssel-Wert-Paar in Ihre JSON-Protokollausgabe aufnehmen. Die Uhrzeit muss im gültigen RFC 3339-Zeitstempelformat angegeben werden. Wenn Sie keinen gültigen Zeitstempel angeben, weist Lambda dem Protokoll die Stufe INFO zu und fügt einen Zeitstempel für Sie hinzu.

Anzeigen von Protokollen in der Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Logs in CloudWatch der Konsole anzeigen

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Logs anzeigen mit AWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
```

```
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Tools und Bibliotheken

Powertools for AWS Lambda (Python) ist ein Entwickler-Toolkit zur Implementierung serverloser Best Practices und zur Steigerung der Entwicklergeschwindigkeit. Das Logger-Serviceprogramm bietet einen für Lambda optimierten Logger, der zusätzliche Informationen über den Funktionskontext all Ihrer Funktionen enthält, wobei die Ausgabe als JSON strukturiert ist. Mit diesem Serviceprogramm können Sie Folgendes tun:

- Erfassung von Schlüsselfeldern aus dem Lambda-Kontext, Kaltstart und Strukturen der Protokollierungsausgabe als JSON
- Protokollieren Sie Ereignisse von Lambda-Aufrufen, wenn Sie dazu aufgefordert werden (standardmäßig deaktiviert)
- Alle Protokolle nur für einen bestimmten Prozentsatz der Aufrufe über Protokollstichproben drucken (standardmäßig deaktiviert)
- Fügen Sie dem strukturierten Protokoll zu einem beliebigen Zeitpunkt zusätzliche Schlüssel hinzu
- Verwenden Sie einen benutzerdefinierten Protokollformatierer (Bring Your Own Formatter), um Protokolle in einer Struktur auszugeben, die mit dem Logging RFC Ihres Unternehmens kompatibel ist

Verwendung von Powertools für AWS Lambda (Python) und AWS SAM für strukturiertes Logging

Führen Sie die nachstehenden Schritte aus, um eine Hello-World-Python-Beispielanwendung mit integrierten -Powertools for Python-Modulen unter Verwendung von AWS SAM bereitzustellen. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Python 3.9
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mit der Hello World Python-Vorlage.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type
 Zip --runtime python3.9 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name sam-app
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
 2023-02-03T14:59:50.371000 INIT_START Runtime Version:
 python:3.9.v16    Runtime Version ARN: arn:aws:lambda:us-
east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.112000
 START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
  "message": "Hello world API - HTTP 200",
  "timestamp": "2023-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
```

```
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYtOc9j",
  "function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
  "correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
  "xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "service": "PowertoolsHelloWorld",
  "ColdStart": [
    1.0
  ]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
```

```
          ]
        ],
        "Metrics": [
          {
            "Name": "HelloWorldInvocations",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "service": "PowertoolsHelloWorld",
  "HelloWorldInvocations": [
    1.0
  ]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000 END
 RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000
 REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be    Duration: 16.33 ms
 Billed Duration: 17 ms    Memory Size: 128 MB    Max Memory Used: 64 MB    Init
 Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299    SegmentId: 3c5d18d735a1ced0
 Sampled: true
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwalten der Protokollaufbewahrung

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um zu vermeiden, dass Protokolle auf unbestimmte Zeit gespeichert werden, löschen Sie die Protokollgruppe oder konfigurieren Sie einen Aufbewahrungszeitraum, nach dessen Ablauf die Protokolle CloudWatch automatisch gelöscht werden. Um die Aufbewahrung von Protokollen einzurichten, fügen Sie Ihrer AWS SAM Vorlage Folgendes hinzu:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
```

```
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Verwendung von Powertools für AWS Lambda (Python) und AWS CDK für strukturiertes Logging

Gehen Sie wie folgt vor, um eine Hello World Python-Beispielanwendung mit integrierten Powertools for AWS Lambda (Python) -Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu den AWS CDK. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine Hello-World-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Python 3.9
- AWS CLI Version 2
- AWS CDK Ausführung 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS CDK Beispielanwendung bereit

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

   ```
   mkdir hello-world
   cd hello-world
   ```

2. Initialisieren Sie die App.

```
cdk init app --language python
```

3. Installieren Sie die Python-Abhängigkeiten.

```
pip install -r requirements.txt
```

4. Erstellen Sie ein Verzeichnis lambda_function unter dem Stammordner.

```
mkdir lambda_function
cd lambda_function
```

5. Erstellen Sie eine Datei namens app.py und fügen Sie den folgenden Code zur Datei hinzu. Dies ist der Code für die Lambda-Funktion.

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools import Logger
from aws_lambda_powertools import Tracer
from aws_lambda_powertools import Metrics
from aws_lambda_powertools.metrics import MetricUnit

app = APIGatewayRestResolver()
tracer = Tracer()
logger = Logger()
metrics = Metrics(namespace="PowertoolsSample")

@app.get("/hello")
@tracer.capture_method
def hello():
    # adding custom metrics
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
 value=1)

    # structured log
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
```

```
# Adding tracer
# See: https://docs.powertools.aws.dev/lambda-python/latest/core/tracer/
@tracer.capture_lambda_handler
# ensures metrics are flushed upon request completion/failure and capturing
 ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Öffnen Sie das Verzeichnis hello_world. Sie sollten eine Datei mit dem Namen hello_world_stack.py sehen.

```
cd ..
cd hello_world
```

7. Öffnen Sie hello_world_stack.py und fügen Sie den folgenden Code in die Datei ein. Dies enthält den Lambda-Konstruktor, der die Lambda-Funktion erstellt, Umgebungsvariablen für Powertools konfiguriert und die Protokollspeicherung auf eine Woche festlegt, und den ApiGatewayv1-Konstruktor, der die REST-API erstellt.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        # Powertools Lambda Layer
        powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
            self,
            id="lambda-powertools",
            # At the moment we wrote this example, the aws_lambda_python_alpha CDK
 constructor is in Alpha, o we use layer to make the example simpler
            # See https://docs.aws.amazon.com/cdk/api/v2/python/
aws_cdk.aws_lambda_python_alpha/README.html
```

```
            # Check all Powertools layers versions here: https://
docs.powertools.aws.dev/lambda-python/latest/#lambda-layer
            layer_version_arn=f"arn:aws:lambda:
{self.region}:017000801446:layer:AWSLambdaPowertoolsPythonV2:21"
        )

        function = lambda_.Function(self,
            'sample-app-lambda',
            runtime=lambda_.Runtime.PYTHON_3_9,
            layers=[powertools_layer],
            code = lambda_.Code.from_asset("./lambda_function/"),
            handler="app.lambda_handler",
            memory_size=128,
            timeout=Duration.seconds(3),
            architecture=lambda_.Architecture.X86_64,
            environment={
                "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
                "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
                "LOG_LEVEL": "INFO"
            }
        )

        apigw = apigwv1.RestApi(self, "PowertoolsAPI",
 deploy_options=apigwv1.StageOptions(stage_name="dev"))

        hello_api = apigw.root.add_resource("hello")
        hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
 proxy=True))

        CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Stellen Sie die Anwendung bereit.

```
cd ..
cdk deploy
```

9. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Rufen Sie den API-Endpunkt auf:

```
curl GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

11. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name HelloWorldStack
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04
 2023-02-03T14:59:50.371000 INIT_START Runtime Version:
 python:3.9.v16    Runtime Version ARN: arn:aws:lambda:us-
east-1::runtime:07a48df201798d627f2b950f03bb227aab4a655a1d019c3296406f95937e2525
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.112000
 START RequestId: d455cfc4-7704-46df-901b-2a5cce9405be Version: $LATEST
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.114000 {
  "level": "INFO",
  "location": "hello:23",
    "message": "Hello world API - HTTP 200",
  "timestamp": "2023-02-03 14:59:51,113+0000",
  "service": "PowertoolsHelloWorld",
  "cold_start": true,
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "function_memory_size": "128",
  "function_arn": "arn:aws:lambda:us-east-1:111122223333:function:sam-app-
HelloWorldFunction-YBg8yfYtOc9j",
  "function_request_id": "d455cfc4-7704-46df-901b-2a5cce9405be",
  "correlation_id": "e73f8aef-5e07-436e-a30b-63e4b23f0047",
  "xray_trace_id": "1-63dd2166-434a12c22e1307ff2114f299"
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
```

```
        "Dimensions": [
          [
            "function_name",
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "function_name": "sam-app-HelloWorldFunction-YBg8yfYtOc9j",
  "service": "PowertoolsHelloWorld",
  "ColdStart": [
    1.0
  ]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.126000 {
  "_aws": {
    "Timestamp": 1675436391126,
    "CloudWatchMetrics": [
      {
        "Namespace": "Powertools",
        "Dimensions": [
          [
            "service"
          ]
        ],
        "Metrics": [
          {
            "Name": "HelloWorldInvocations",
            "Unit": "Count"
          }
        ]
      }
    ]
  },
  "service": "PowertoolsHelloWorld",
  "HelloWorldInvocations": [
    1.0
```

```
  ]
}
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000 END
 RequestId: d455cfc4-7704-46df-901b-2a5cce9405be
2023/02/03/[$LATEST]ea9a64ec87294bf6bbc9026c05a01e04 2023-02-03T14:59:51.128000
 REPORT RequestId: d455cfc4-7704-46df-901b-2a5cce9405be    Duration: 16.33 ms
 Billed Duration: 17 ms    Memory Size: 128 MB    Max Memory Used: 64 MB    Init
 Duration: 739.46 ms
XRAY TraceId: 1-63dd2166-434a12c22e1307ff2114f299    SegmentId: 3c5d18d735a1ced0
 Sampled: true
```

12. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
cdk destroy
```

AWS Lambda-Funktionstests in Python

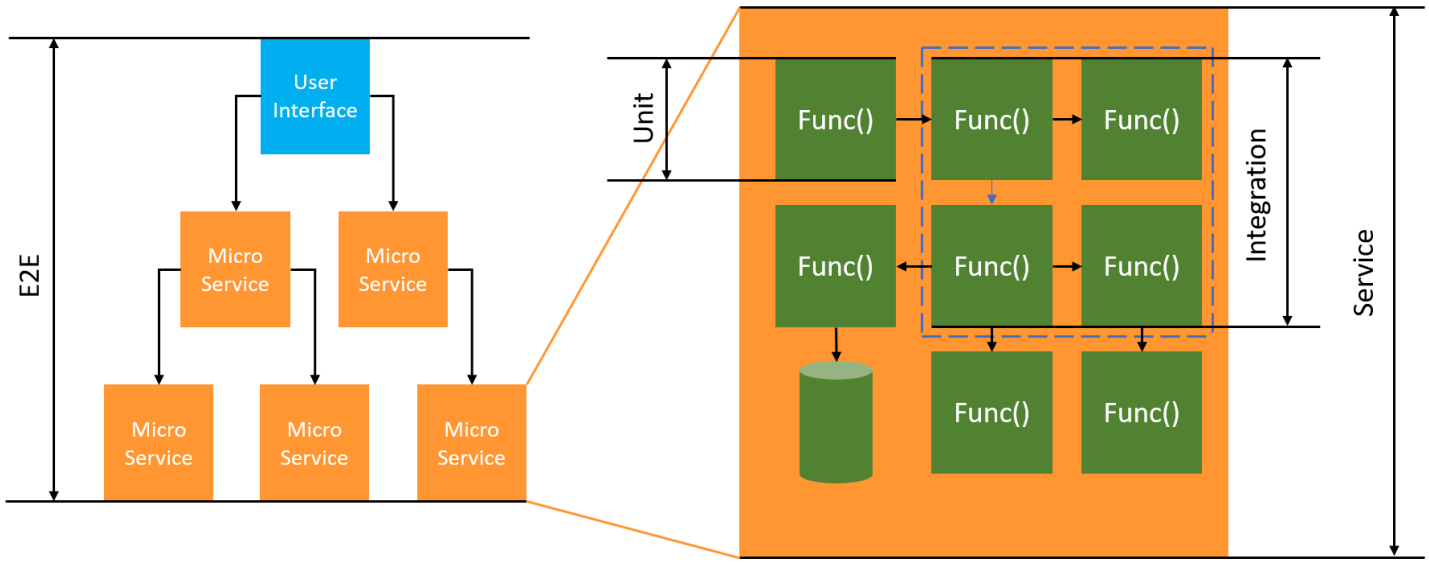
> **Note**
>
> Im Kapitel Testen von Funktionen finden Sie eine vollständige Einführung in Techniken und bewährte Methoden für das Testen von Serverless-Lösungen.

Beim Testen der Serverless-Funktionen werden herkömmliche Testtypen und -techniken verwendet. Erwägen Sie jedoch auch das Testen der Serverless-Anwendungen als Ganzes. Cloud-basierte Tests bieten das genaueste Maß für die Qualität sowohl Ihrer Funktionen als auch Ihrer Serverless-Anwendungen.

Eine Serverless-Anwendungsarchitektur umfasst verwaltete Services, die über API-Aufrufe wichtige Anwendungsfunktionen bereitstellen. Aus diesem Grund muss Ihr Entwicklungszyklus automatisierte Tests beinhalten, die bei der Interaktion Ihrer Funktionen und Services die Funktionalität überprüfen.

Wenn Sie keine cloud-basierten Tests erstellen, können aufgrund von Unterschieden zwischen Ihrer lokalen Umgebung und der bereitgestellten Umgebung Probleme auftreten. Ihr kontinuierlicher Integrationsprozess muss Tests anhand einer Reihe von Ressourcen durchführen, die in der Cloud bereitgestellt werden, bevor Ihr Code in die nächste Bereitstellungsumgebung wie QA, Staging oder Produktion übertragen wird.

Lesen Sie diesen kurzen Leitfaden weiter, um weitere Informationen zu Teststrategien für Serverless-Anwendungen zu erhalten, oder besuchen Sie das Serverless Test Samples Repository, um praktische Beispiele zu finden, die sich speziell auf die gewählte Sprache und Laufzeit beziehen.



Für Serverless-Tests schreiben Sie immer noch Einheiten , Integration und end-to-end Tests.

- Einheitentests — Tests, die an einem isolierten Codeblock ausgeführt werden. Zum Beispiel die Überprüfung der Geschäftslogik zur Berechnung der Bereitstellungskosten für einen bestimmten Artikel und Bestimmungsort.
- Integrationstests — Tests, an denen zwei oder mehr Komponenten oder Dienste beteiligt sind, die interagieren, in der Regel in einer Cloud-Umgebung. Bei der Überprüfung einer Funktion werden beispielsweise Ereignisse aus einer Warteschlange verarbeitet.
- E-nd-to-end Tests – Tests, die das Verhalten einer gesamten Anwendung überprüfen. Stellen Sie beispielsweise sicher, dass die Infrastruktur korrekt eingerichtet ist und die Ereignisse zwischen den Services wie erwartet ablaufen, um die Bestellungen der Kunden aufzuzeichnen.

Testen Ihrer Serverless-Anwendungen

In der Regel verwenden Sie eine Mischung aus verschiedenen Ansätzen, um Ihren Serverless-Anwendungscode zu testen, einschließlich Tests in der Cloud, Tests mit Mock-Code und gelegentlich Tests mit Emulatoren.

Testen in der Cloud

Tests in der Cloud sind für alle Testphasen nützlich, einschließlich Einheitentests, Integrationstests und end-to-end Tests. Sie führen Tests für Code durch, der in der Cloud bereitgestellt wird und mit cloud-basierten Services interagiert. Dieser Ansatz bietet das genaueste Maß für die Qualität Ihres Codes.

Eine bequeme Möglichkeit, Ihre Lambda-Funktion in der Cloud zu debuggen, ist die Verwendung der Konsole mit einem Testereignis. Ein Testereignis ist eine JSON-Eingabe für Ihre Funktion. Wenn Ihre Funktion keine Eingabe erfordert, kann das Ereignis ein leeres JSON-Dokument (`{}`) sein. Die Konsole bietet Beispielereignisse für eine Vielzahl von Service-Integrationen. Nachdem Sie ein Ereignis in der Konsole erstellt haben, können Sie es mit Ihrem Team teilen, um das Testen einfacher und einheitlicher zu gestalten.

> **Note**
>
> Das Testen einer Funktion in der Konsole ist ein schneller Einstieg, aber die Automatisierung Ihrer Testzyklen gewährleistet die Anwendungsqualität und die Entwicklungsgeschwindigkeit.

Test-Tools

Es gibt Tools und Techniken, um die Feedback-Schleifen bei der Entwicklung zu beschleunigen. AWSSAM Accelerate und AWSCDK Watch Mode reduzieren beispielsweise beide die Zeit, die für die Aktualisierung von Cloud-Umgebungen benötigt wird.

Moto ist eine Python-Bibliothek für das Mocking von AWS-Services und -Ressourcen, sodass Sie Ihre Funktionen mit wenigen oder gar keinen Änderungen testen können, indem Sie Dekoratoren zum Abfangen und Simulieren von Antworten verwenden.

Das Validierungsfeature von Powertools für AWS Lambda (Python) bietet Dekoratoren, mit denen Sie Eingabeereignisse und Ausgabeantworten Ihrer Python-Funktionen validieren können.

Weitere Informationen finden Sie im Blogbeitrag Unit Testing Lambda with Python and Mock AWS Services.

Informationen zur Verringerung der Latenzzeit bei Iterationen der Cloud-Bereitstellung finden Sie unter AWS Serverless Application Model (AWS SAM) Accelerate, AWS Cloud Development Kit (Watch-Modus AWS CDK). Diese Tools überwachen Ihre Infrastruktur und Ihren Code auf Änderungen. Sie reagieren auf diese Änderungen, indem sie automatisch inkrementelle Updates erstellen und in Ihrer Cloud-Umgebung bereitstellen.

Beispiele, in denen diese Tools verwendet werden, sind im Code-Repository mit Python-Testbeispielen verfügbar.

Instrumentierung von Python-Code in AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS -Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von drei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) — Eine sichere, produktionsbereite und AWS unterstützte Distribution des (OTel) SDK. OpenTelemetry
- AWS X-Ray-SDK for Python – Ein SDK zum Generieren und Senden von Nachverfolgungsdaten an X-Ray.
- Powertools for AWS Lambda (Python) — Ein Entwickler-Toolkit zur Implementierung serverloser Best Practices und zur Steigerung der Entwicklergeschwindigkeit.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda SDKs sind Teil einer eng integrierten Instrumentierungslösung von. AWS Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Ablaufverfolgung in X-Ray mit beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS -Distro für Open Telemetry und X-Ray-SDKs.

Sections

- Powertools für AWS Lambda (Python) und AWS SAM für das Tracing verwenden
- Verwendung von Powertools für AWS Lambda (Python) und AWS CDK für die Ablaufverfolgung
- Verwenden von ADOT zum Instrumentieren Ihrer Python-Funktionen

- Verwenden des X-Ray-SDK zum Instrumentieren Ihrer Python-Funktionen
- Aktivieren der Nachverfolgung mit der Lambda-Konsole
- Aktivieren der Nachverfolgung mit der Lambda-API
- Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation
- Interpretieren einer X-Ray-Nachverfolgung
- Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)

Powertools für AWS Lambda (Python) und AWS SAM für das Tracing verwenden

Gehen Sie wie folgt vor, um eine Hello World Python-Beispielanwendung mit integrierten Powertools for AWS Lambda (Python) -Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu die AWS SAM. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine Hello-World-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Python 3.9
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mit der Hello World Python-Vorlage.

```
sam init --app-template hello-world-powertools-python --name sam-app --package-type
 Zip --runtime python3.9 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
```

```
    - total requests: 1
    - ok count(2XX): 1
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
 - Edges: []
   Summary_statistics:
    - total requests: 1
    - ok count(2XX): 1
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 0.016
  Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
   Summary_statistics:
    - total requests: 0
    - ok count(2XX): 0
    - error count(4XX): 0
    - fault count(5XX): 0
    - total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
       - 0.000s - ## app.hello
   - 0.000s - Overhead
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

Verwendung von Powertools für AWS Lambda (Python) und AWS CDK für die Ablaufverfolgung

Gehen Sie wie folgt vor, um eine Hello World Python-Beispielanwendung mit integrierten Powertools for AWS Lambda (Python) -Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu die AWS CDK. Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine Hello-World-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Python 3.9
- AWS CLI Version 2
- AWS CDK Ausführung 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS CDK Beispielanwendung bereit

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie die App.

```
cdk init app --language python
```

3. Installieren Sie die Python-Abhängigkeiten.

```
pip install -r requirements.txt
```

4. Erstellen Sie ein Verzeichnis lambda_function unter dem Stammordner.

```
mkdir lambda_function
cd lambda_function
```

5. Erstellen Sie eine Datei namens app.py und fügen Sie den folgenden Code zur Datei hinzu. Dies ist der Code für die Lambda-Funktion.

```
from aws_lambda_powertools.event_handler import APIGatewayRestResolver
from aws_lambda_powertools.utilities.typing import LambdaContext
from aws_lambda_powertools.logging import correlation_paths
from aws_lambda_powertools import Logger
from aws_lambda_powertools import Tracer
from aws_lambda_powertools import Metrics
from aws_lambda_powertools.metrics import MetricUnit

app = APIGatewayRestResolver()
tracer = Tracer()
logger = Logger()
metrics = Metrics(namespace="PowertoolsSample")

@app.get("/hello")
@tracer.capture_method
def hello():
    # adding custom metrics
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/metrics/
    metrics.add_metric(name="HelloWorldInvocations", unit=MetricUnit.Count,
 value=1)

    # structured log
    # See: https://docs.powertools.aws.dev/lambda-python/latest/core/logger/
    logger.info("Hello world API - HTTP 200")
    return {"message": "hello world"}

# Enrich logging with contextual information from Lambda
@logger.inject_lambda_context(correlation_id_path=correlation_paths.API_GATEWAY_REST)
# Adding tracer
# See: https://docs.powertools.aws.dev/lambda-python/latest/core/tracer/
@tracer.capture_lambda_handler
```

```
# ensures metrics are flushed upon request completion/failure and capturing
 ColdStart metric
@metrics.log_metrics(capture_cold_start_metric=True)
def lambda_handler(event: dict, context: LambdaContext) -> dict:
    return app.resolve(event, context)
```

6. Öffnen Sie das Verzeichnis hello_world. Sie sollten eine Datei mit dem Namen hello_world_stack.py sehen.

```
cd ..
cd hello_world
```

7. Öffnen Sie hello_world_stack.py und fügen Sie den folgenden Code in die Datei ein. Dies enthält den Lambda-Konstruktor, der die Lambda-Funktion erstellt, Umgebungsvariablen für Powertools konfiguriert und die Protokollspeicherung auf eine Woche festlegt, und den ApiGatewayv1-Konstruktor, der die REST-API erstellt.

```
from aws_cdk import (
    Stack,
    aws_apigateway as apigwv1,
    aws_lambda as lambda_,
    CfnOutput,
    Duration
)
from constructs import Construct

class HelloWorldStack(Stack):

    def __init__(self, scope: Construct, construct_id: str, **kwargs) -> None:
        super().__init__(scope, construct_id, **kwargs)

        # Powertools Lambda Layer
        powertools_layer = lambda_.LayerVersion.from_layer_version_arn(
            self,
            id="lambda-powertools",
            # At the moment we wrote this example, the aws_lambda_python_alpha CDK
 constructor is in Alpha, o we use layer to make the example simpler
            # See https://docs.aws.amazon.com/cdk/api/v2/python/
aws_cdk.aws_lambda_python_alpha/README.html
            # Check all Powertools layers versions here: https://
docs.powertools.aws.dev/lambda-python/latest/#lambda-layer
            layer_version_arn=f"arn:aws:lambda:
{self.region}:017000801446:layer:AWSLambdaPowertoolsPythonV2:21"
```

```
        )

        function = lambda_.Function(self,
            'sample-app-lambda',
            runtime=lambda_.Runtime.PYTHON_3_9,
            layers=[powertools_layer],
            code = lambda_.Code.from_asset("./lambda_function/"),
            handler="app.lambda_handler",
            memory_size=128,
            timeout=Duration.seconds(3),
            architecture=lambda_.Architecture.X86_64,
            environment={
                "POWERTOOLS_SERVICE_NAME": "PowertoolsHelloWorld",
                "POWERTOOLS_METRICS_NAMESPACE": "PowertoolsSample",
                "LOG_LEVEL": "INFO"
            }
        )

        apigw = apigwv1.RestApi(self, "PowertoolsAPI",
 deploy_options=apigwv1.StageOptions(stage_name="dev"))

        hello_api = apigw.root.add_resource("hello")
        hello_api.add_method("GET", apigwv1.LambdaIntegration(function,
 proxy=True))

        CfnOutput(self, "apiUrl", value=f"{apigw.url}hello")
```

8. Stellen Sie die Anwendung bereit.

```
cd ..
cdk deploy
```

9. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`apiUrl`].OutputValue' --output text
```

10. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

11. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.016
  Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
```

```
        - 0.000s - ## app.hello
    - 0.000s - Overhead
```

12. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
cdk destroy
```

Verwenden von ADOT zum Instrumentieren Ihrer Python-Funktionen

ADOT bietet vollständig verwaltete Lambda-Ebenen, die alles packen, was Sie zum Sammeln von Telemetriedaten mit dem OTel-SDK benötigen. Indem Sie diese Ebene verwenden, können Sie Ihre Lambda-Funktionen instrumentieren, ohne einen Funktionscode ändern zu müssen. Sie können Ihren Ebenen auch für die benutzerdefinierte Initialisierung von OTel konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Konfiguration für den ADOT Collector auf Lambda in der ADOT-Dokumentation.

Für Python-Laufzeiten können Sie den AWS -verwaltete Lambda-Layer für ADOT Python hinzufügen, um Ihre Funktionen automatisch zu instrumentieren. Dieser Layer funktioniert sowohl für arm64- als auch für x86_64-Architekturen. Eine ausführliche Anleitung zum Hinzufügen dieser Ebene finden Sie unter AWS Distro for OpenTelemetry Lambda Support for Python in der ADOT-Dokumentation.

Verwenden des X-Ray-SDK zum Instrumentieren Ihrer Python-Funktionen

Um Details zu Aufrufen aufzuzeichnen, die Ihre Lambda-Funktion an andere Ressourcen in Ihrer Anwendung vornimmt, können Sie auch AWS X-Ray-SDK for Python verwenden. Um das SDK zu erhalten, fügen Sie das `aws-xray-sdk`-Paket den Abhängigkeiten Ihrer Anwendung hinzu.

Example requirements.txt

```
jsonpickle==1.3
aws-xray-sdk==2.4.3
```

In Ihrem Funktionscode können Sie AWS SDK-Clients instrumentieren, indem Sie die `boto3` Bibliothek mit dem Modul patchen. `aws_xray_sdk.core`

Example Funktion — Einen SDK-Client AWS verfolgen

```
import boto3
```

```
from aws_xray_sdk.core import xray_recorder
from aws_xray_sdk.core import patch_all

logger = logging.getLogger()
logger.setLevel(logging.INFO)
patch_all()

client = boto3.client('lambda')
client.get_account_settings()

def lambda_handler(event, context):
    logger.info('## ENVIRONMENT VARIABLES\r' + jsonpickle.encode(dict(**os.environ)))
  ...
```

Aktivieren Sie nach Hinzufügen der richtigen Abhängigkeiten die Nachverfolgung in der Konfiguration Ihrer Funktion über die Lambda-Konsole oder die API.

Aktivieren der Nachverfolgung mit der Lambda-Konsole

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

Aktivieren der Nachverfolgung mit der Lambda-API

Konfigurieren Sie die Ablaufverfolgung für Ihre Lambda-Funktion mit dem AWS CLI oder AWS SDK und verwenden Sie die folgenden API-Operationen:

- UpdateFunctionKonfiguration

- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
```

```
    ...
```

Interpretieren einer X-Ray-Nachverfolgung

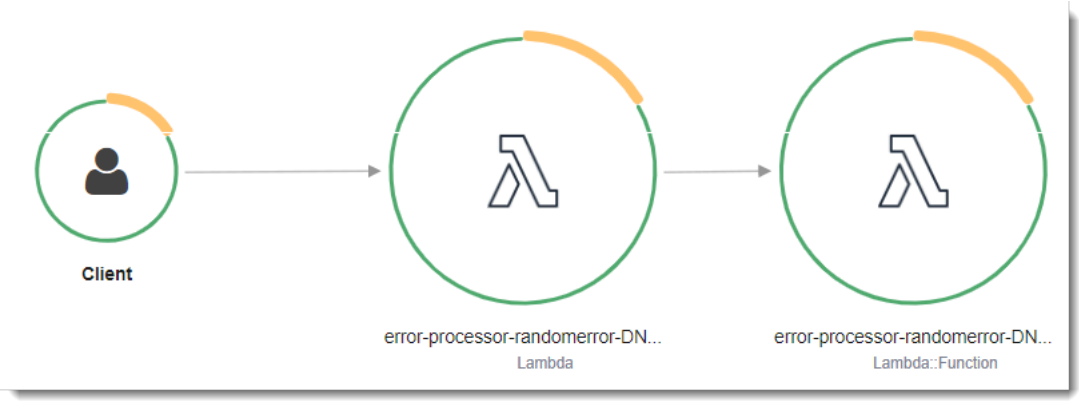
Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray. Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

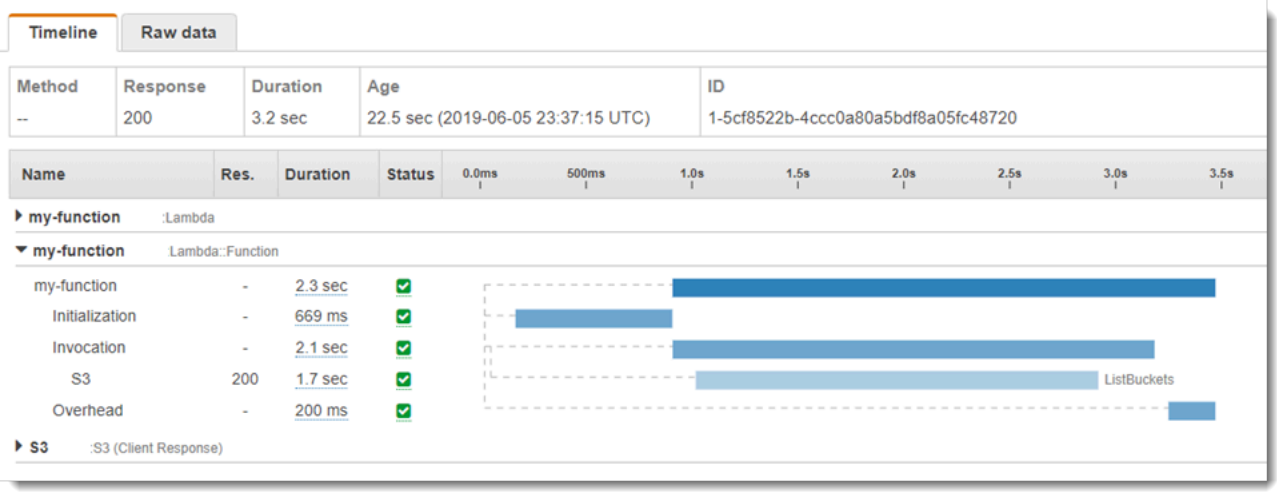
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.
- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter AWS X-Ray-SDK for Python im AWS X-Ray -Entwicklerhandbuch.

> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)

Wenn Sie das X-Ray-SDK verwenden, um AWS SDK-Clients Ihren Funktionscode zu instrumentieren, kann Ihr Bereitstellungspaket ziemlich umfangreich werden. Um Laufzeitabhängigkeiten bei jeder Aktualisierung des Funktionscodes zu vermeiden, verpacken Sie das X-Ray-SDK in einer Lambda-Ebene.

Das folgende Beispiel zeigt eine `AWS::Serverless::LayerVersion`-Ressource, die das AWS X-Ray-SDK for Python speichert.

Example template.yml – Abhängigkeitenebene

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
```

```
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-python-lib
      Description: Dependencies for the blank-python sample app.
      ContentUri: package/.
      CompatibleRuntimes:
        - python3.8
```

Bei dieser Konfiguration aktualisieren Sie die Bibliotheksebene nur, wenn Sie Ihre Laufzeitabhängigkeiten ändern. Da das Funktionsbereitstellungspaket nur Ihren Code enthält, kann dies dazu beitragen, die Upload-Zeiten zu reduzieren.

Das Erstellen einer Ebene für Abhängigkeiten erfordert Build-Konfigurationsänderungen, um das Ebenen-Archiv vor der Bereitstellung zu generieren. Ein funktionierendes Beispiel finden Sie in der Beispielanwendung blank-python .

Erstellen von Lambda-Funktionen mit Ruby

Sie können Ruby-Code in AWS Lambda ausführen. Lambda bietet Laufzeiten für Ruby, die Ihren Code ausführen, um Ereignisse zu verarbeiten. Ihr Code wird in einer Umgebung ausgeführt, die die Rolle AWS SDK for Ruby, with credentials from a AWS Identity and Access Management (IAM) enthält, die Sie verwalten. Weitere Informationen zu den SDK-Versionen, die in den Ruby-Runtimes enthalten sind, finden Sie unter. the section called “SDK-Versionen, die Runtime enthalten”

Lambda unterstützt die folgenden Ruby-Laufzeiten.

Ruby

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Ruby 3.3	`ruby3.3`	Amazon Linux 2023			
Ruby 3.2	`ruby3.2`	Amazon Linux 2			

So erstellen Sie eine Ruby-Funktion

1. Öffnen Sie die Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Konfigurieren Sie die folgenden Einstellungen:
   - Funktionsname: Geben Sie einen Namen für die Funktion ein.
   - Laufzeit: Wählen Sie Ruby 3.2 aus.
4. Wählen Sie Funktion erstellen.
5. Um ein Testereignis zu konfigurieren, wählen Sie Test.
6. Geben Sie für Event name (Ereignisname) **`test`** ein.
7. Wählen Sie Änderungen speichern aus.
8. Wählen Sie Test, um die Funktion aufzurufen.

Die Konsole erstellt eine Lambda-Funktion mit einer einzigen Quelldatei mit dem Namen `lambda_function.rb`. Mit dem integrierten Code-Editor können Sie diese Datei bearbeiten und weitere Dateien hinzufügen. Klicken Sie auf Save (Speichern), um die Änderungen zu speichern. Um Ihren Code auszuführen, wählen Sie Test.

> **Note**
>
> Die Lambda-Konsole dient AWS Cloud9 dazu, eine integrierte Entwicklungsumgebung im Browser bereitzustellen. Sie können es auch verwenden AWS Cloud9 , um Lambda-Funktionen in Ihrer eigenen Umgebung zu entwickeln. Weitere Informationen finden Sie AWS Toolkit im AWS Cloud9 Benutzerhandbuch unter Arbeiten mit AWS Lambda Funktionen unter Verwendung von.

Die `lambda_function.rb`-Datei exportiert eine Funktion mit dem Namen `lambda_handler`, die ein Ereignisobjekt und ein Kontext-Objekt übernimmt. Dies ist die Handler-Funktion, die bei einem Aufruf der Funktion von Lambda aufgerufen wird. Die Ruby-Funktionslaufzeit ruft Aufrufereignisse von Lambda ab und leitet sie an den Handler weiter. In der Konfiguration der Funktion lautet der Wert für den Handler `lambda_function.lambda_handler`.

Wenn Sie Ihren Funktionscode speichern, erstellt die Lambda-Konsole ein Bereitstellungspaket für das ZIP-Dateiarchiv. Wenn Sie Ihren Funktionscode außerhalb der Konsole (mit einer IDE) entwickeln, müssen Sie ein Bereitstellungspaket erstellen, um Ihren Code in die Lambda-Funktion hochzuladen.

> **Note**
>
> Um mit der Anwendungsentwicklung in Ihrer lokalen Umgebung zu beginnen, stellen Sie eine der Beispielanwendungen bereit, die im GitHub Repository dieses Handbuchs verfügbar sind.
>
> Lambda-Beispielanwendungen in Ruby
>
> - blank-ruby — Eine Ruby-Funktion, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK veranschaulicht. AWS
> - Ruby-Codebeispiele für AWS Lambda — In Ruby geschriebene Codebeispiele, die zeigen, wie man mit AWS Lambda interagiert.

Die Funktionslaufzeit übergibt neben dem Aufrufereignis ein Context-Objekt an den Handler. Das Context-Objekt enthält zusätzliche Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung. Weitere Informationen erhalten Sie über die Umgebungsvariablen.

Ihre Lambda-Funktion wird mit einer CloudWatch Logs-Protokollgruppe geliefert. Die Funktionslaufzeit sendet Details zu jedem Aufruf an CloudWatch Logs. Es leitet alle Protokolle weiter, die Ihre Funktion während des Aufrufs ausgibt. Wenn Ihre Funktion einen Fehler zurückgibt, formatiert Lambda den Fehler und gibt ihn an den Aufrufer zurück.

Themen

SDK-Versionen, die Runtime enthalten

Die Version des AWS SDK, die in der Ruby-Laufzeit enthalten ist, hängt von der Runtime-Version und Ihrer ab. AWS-Region Das AWS SDK for Ruby ist modular konzipiert und wird durch getrennt AWS-Service. Um die Versionsnummer eines bestimmten Service-Gems zu ermitteln, das in der von Ihnen verwendeten Runtime enthalten ist, erstellen Sie eine Lambda-Funktion mit Code im folgenden Format. Ersetzen Sie `aws-sdk-s3` und `Aws::S3` durch den Namen der Service-Gems, die Ihr Code verwendet.

```
require 'aws-sdk-s3'

def lambda_handler(event:, context:)
  puts "Service gem version: #{Aws::S3::GEM_VERSION}"
  puts "Core version: #{Aws::CORE_GEM_VERSION}"
end
```

Aktivieren von Yet Another Ruby JIT (YJIT)

Die Ruby-3.2-Laufzeit unterstützt YJIT, einen einfachen, minimalistischen Ruby-JIT-Compiler. YJIT bietet eine deutlich höhere Leistung, benötigt aber auch mehr Speicher als der Ruby-Interpreter. YJIT wird für Ruby-on-Rails-Workloads empfohlen.

YJIT ist standardmäßig nicht aktiviert. Um YJIT für eine Ruby-3.2-Funktion zu aktivieren, setzen Sie die Umgebungsvariable `RUBY_YJIT_ENABLE` auf 1. Um sicherzustellen, dass YJIT aktiviert ist, drucken Sie das Ergebnis der `RubyVM::YJIT.enabled?`-Methode aus.

Example – Sicherstellen, dass YJIT aktiviert ist

```
puts(RubyVM::YJIT.enabled?())
# => true
```

Definieren Sie den Lambda-Funktionshandler in Ruby

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Im folgenden Beispiel definiert die Datei `function.rb` eine Handler-Methode mit dem Namen `handler`. Die Handler-Funktion nimmt zwei Objekten als Eingabe und gibt ein JSON-Dokument zurück.

Example function.rb

```
require 'json'

def handler(event:, context:)
    { event: JSON.generate(event), context: JSON.generate(context.inspect) }
end
```

In Ihrer Funktionskonfiguration gibt die Einstellung `handler` Lambda die Stelle an, an der sich der Handler befindet. Im vorherigen Beispiel ist der korrekte Wert für diese Einstellung **`function.handler`**. Er enthält zwei Namen, die durch einen Punkt getrennt werden: den Namen der Datei und den Namen der Handler-Methode.

Sie können Ihre Handler-Methode außerdem in einer Klasse definieren. Das folgende Beispiel definiert eine Handler-Methode mit dem Namen `process` in einer Klasse mit dem Namen `Handler` in einem Modul mit dem Namen `LambdaFunctions`.

Example source.rb

```
module LambdaFunctions
  class Handler
    def self.process(event:,context:)
      "Hello!"
    end
  end
end
```

In diesem Fall ist die Handler-Einstellung **`source.LambdaFunctions::Handler.process`**.

Die zwei Objekte, die der Handler akzeptiert, sind das Aufrufereignis und Context. Das Ereignis ist ein Ruby-Objekt, das die vom Aufrufer bereitgestellte Nutzlast enthält. Wenn es sich bei der

Nutzlast um ein JSON-Dokument handelt, ist das Ereignisobjekt ein Ruby-Hash. Andernfalls ist es eine Zeichenfolge. Das Context-Objekt besitzt Methoden und Eigenschaften, die Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereitstellen.

Der Funktions-Handler wird jedes Mal ausgeführt, wenn Ihre Lambda-Funktion aufgerufen wird. Statischer Code außerhalb des Handler wird einmal pro Funktions-Instance ausgeführt. Wenn Ihr Handler Ressourcen wie SDK-Clients und Datenbankverbindungen verwendet, können Sie diese außerhalb der Handler-Methode erstellen, um sie für mehrere Aufrufe wiederzuverwenden.

Jede Instance Ihrer Funktion kann zwar mehrere Aufrufereignisse verarbeiten, verarbeitet jedoch jeweils nur ein Ereignis zur gleichen Zeit. Die Anzahl der Instances, die zu einem bestimmten Zeitpunkt ein Ereignis verarbeiten, ist die Nebenläufigkeit Ihrer Funktion. Weitere Informationen zur Lambda-Ausführungsumgebung finden Sie unter Lambda-Ausführungsumgebung.

Arbeiten mit ZIP-Dateiarchiven für Ruby-Lambda-Funktionen

Der Code Ihrer AWS Lambda Funktion besteht aus einer.rb-Datei, die den Handlercode Ihrer Funktion zusammen mit allen zusätzlichen Abhängigkeiten (Gems) enthält, von denen Ihr Code abhängt. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Dieses Paket kann entweder ein ZIP-Dateiarchiv oder ein Container-Image sein. Weitere Informationen zur Verwendung von Container-Images mit Ruby finden Sie unter Bereitstellen von Ruby-Lambda-Funktionen mit Container-Images.

Zum Erstellen des Bereitstellungspakets für ein ZIP-Dateiarchiv können Sie ein integriertes Dienstprogramm für ZIP-Dateien Ihres Befehlszeilen-Tools oder ein anderes Dienstprogramm für ZIP-Dateien verwenden, wie 7zip. In den Beispiele in den folgenden Abschnitten wird davon ausgegangen, dass Sie ein `zip`-Befehlszeilen-Tool in einer Linux- oder MacOS-Umgebung verwenden. Unter Windows können Sie das Windows-Subsystem für Linux installieren, um eine Windows-Version von Ubuntu und Bash zu erhalten und dieselben Befehle zu verwenden.

Da Lambda POSIX-Dateiberechtigungen verwendet, müssen Sie möglicherweise Berechtigungen für den Bereitstellungspaketordner festlegen, bevor Sie das ZIP-Dateiarchiv erstellen.

In den Beispielbefehlen in den folgenden Abschnitten wird das Hilfsprogramm Bundler verwendet, um Ihrem Bereitstellungspaket Abhängigkeiten hinzuzufügen. Führen Sie zum Installieren von Bundler den folgenden Befehl aus:

```
gem install bundler
```

Sections

Abhängigkeiten in Ruby

Bei Lambda-Funktionen, die die Ruby-Laufzeit verwenden, kann eine Abhängigkeit ein beliebiges Ruby-Gem sein. Bei Bereitstellung Ihrer Funktion mithilfe eines ZIP-Archivs können Sie diese

Abhängigkeiten entweder mit Ihrem Funktionscode zu Ihrer ZIP-Datei hinzufügen oder eine Lambda-Ebene verwenden. Eine Ebene ist ein separates ZIP-Dateiarchiv, das zusätzlichen Code und andere Daten enthalten kann. Weitere Informationen zur Verwendung von Lambda-Ebenen finden Sie unter Lambda-Ebenen.

Die Ruby-Laufzeit beinhaltet die AWS SDK for Ruby. Wenn Ihre Funktion das SDK verwendet, müssen Sie es nicht mit Ihrem Code bündeln. Wenn Sie jedoch die volle Kontrolle über Ihre Abhängigkeiten behalten oder eine bestimmte Version des SDK verwenden möchten, können Sie es dem Bereitstellungspaket Ihrer Funktion hinzufügen. Sie können das SDK entweder in Ihre ZIP-Datei aufnehmen oder es mithilfe einer Lambda-Ebene hinzufügen. Abhängigkeiten in Ihrer ZIP-Datei oder auf Lambda-Ebenen haben Vorrang vor Versionen, die in der Laufzeit enthalten sind. Informationen darüber, welche Version des SDK for Ruby in Ihrer Runtime-Version enthalten ist, finden Sie unterthe section called “SDK-Versionen, die Runtime enthalten”.

Im Rahmen des AWS -Modells der geteilten Verantwortung sind Sie für die Verwaltung aller Abhängigkeiten in den Bereitstellungspaketen Ihrer Funktionen verantwortlich. Dies beinhaltet das Durchführen von Updates und Sicherheitspatches. Zum Aktualisieren von Abhängigkeiten im Bereitstellungspaket Ihrer Funktion erstellen Sie zunächst eine neue ZIP-Datei und laden Sie diese dann in Lambda hoch. Weitere Informationen finden Sie unter Erstellen eines ZIP-Bereitstellungspakets mit Abhängigkeiten und Erstellen und Aktualisieren von Ruby-Lambda-Funktionen mithilfe von ZIP-Dateien.

ZIP-Bereitstellungspakets ohne Abhängigkeiten erstellen

Hat Ihr Funktionscode keine Abhängigkeiten, enthält Ihre ZIP-Datei nur die RB-Datei mit dem Handler-Code Ihrer Funktion. Erstellen Sie mit Ihrem bevorzugten ZIP-Programm eine ZIP-Datei mit Ihrer RB-Datei im Stammverzeichnis. Befindet sich die RB-Datei nicht im Stammverzeichnis Ihrer ZIP-Datei, kann Lambda Ihren Code nicht ausführen.

Informationen zum Bereitstellen Ihrer ZIP-Datei zum Erstellen einer neuen Lambda-Funktion oder Aktualisieren einer vorhandenen Funktion, finden Sie unter Erstellen und Aktualisieren von Ruby-Lambda-Funktionen mithilfe von ZIP-Dateien.

Erstellen eines ZIP-Bereitstellungspakets mit Abhängigkeiten

Hängt Ihr Funktionscode von zusätzlichen Ruby-Gems ab, können Sie diese Abhängigkeiten entweder mit Ihrem Funktionscode in Ihre ZIP-Datei aufnehmen oder eine Lambda-Ebene verwenden. In diesem Abschnitt erfahren Sie, wie Sie Ihre Abhängigkeiten in Ihr ZIP-

Bereitstellungspaket aufnehmen. Anweisungen zum Einschließen Ihrer Abhängigkeiten in eine Ebene finden Sie unter the section called “Erstellen einer Ruby-Ebene für Ihre Abhängigkeiten”.

Angenommen, Ihr Funktionscode ist in einer Datei mit dem Namen `lambda_function.rb` in Ihrem Projektverzeichnis gespeichert. Die folgenden CLI-Befehle erstellen Sie eine ZIP-Datei mit dem Namen „`my_deployment_package.zip`“, die Ihren Funktionscode und seine Abhängigkeiten enthält.

Erstellen des Bereitstellungspakets

1. Erstellen Sie in Ihrem Projektverzeichnis eine `Gemfile`-Datei für die Angabe Ihrer Abhängigkeiten.

   ```
   bundle init
   ```

2. Bearbeiten Sie die `Gemfile`-Datei mit Ihrem bevorzugten Texteditor, um die Abhängigkeiten Ihrer Funktion anzugeben. Wenn Sie also beispielsweise das TZInfo-Gem verwenden möchten, bearbeiten Sie Ihre `Gemfile`-Datei so, dass sie wie folgt aussieht:

   ```
   source "https://rubygems.org"
   gem "tzinfo"
   ```

3. Führen Sie den folgenden Befehl aus, um die in Ihrer `Gemfile`-Datei angegebenen Gems in Ihrem Projektverzeichnis zu installieren. Durch diesen Befehl wird `vendor/bundle` als Standardpfad für Gem-Installationen festgelegt:

   ```
   bundle config set --local path 'vendor/bundle' && bundle install
   ```

   Die Ausgabe sollte in etwa wie folgt aussehen:

   ```
   Fetching gem metadata from https://rubygems.org/...........
   Resolving dependencies...
   Using bundler 2.4.13
   Fetching tzinfo 2.0.6
   Installing tzinfo 2.0.6
   ...
   ```

> **Note**
>
> Wenn Sie Gems später wieder global installieren möchten, können Sie den folgenden Befehl ausführen:
>
> ```
> bundle config set --local system 'true'
> ```

4. Erstellen Sie ein ZIP-Dateiarchiv, das die `lambda_function.rb`-Datei mit dem Handler-Code Ihrer Funktion sowie mit den Abhängigkeiten enthält, die Sie im vorherigen Schritt installiert haben.

   ```
   zip -r my_deployment_package.zip lambda_function.rb vendor
   ```

   Die Ausgabe sollte in etwa wie folgt aussehen:

   ```
   adding: lambda_function.rb (deflated 37%)
     adding: vendor/ (stored 0%)
     adding: vendor/bundle/ (stored 0%)
     adding: vendor/bundle/ruby/ (stored 0%)
     adding: vendor/bundle/ruby/3.2.0/ (stored 0%)
     adding: vendor/bundle/ruby/3.2.0/build_info/ (stored 0%)
     adding: vendor/bundle/ruby/3.2.0/cache/ (stored 0%)
     adding: vendor/bundle/ruby/3.2.0/cache/aws-eventstream-1.0.1.gem (deflated 36%)
   ...
   ```

Erstellen einer Ruby-Ebene für Ihre Abhängigkeiten

Die Anweisungen in diesem Abschnitt zeigen Ihnen, wie Sie Ihre Abhängigkeiten in eine Ebene einschließen. Anweisungen zum Einschließen Ihrer Abhängigkeiten in Ihr Bereitstellungspaket finden Sie unter the section called “Erstellen eines ZIP-Bereitstellungspakets mit Abhängigkeiten”.

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Layer-Inhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

- `ruby/gems/2.7.0` (`GEM_PATH`)
- `ruby/lib` (`RUBYLIB`)

Die Struktur Ihrer Ebene-ZIP-Datei könnte beispielsweise wie folgt aussehen:

```
json.zip
# ruby/gems/2.7.0/
                | build_info
                | cache
                | doc
                | extensions
                | gems
                | # json-2.1.0
                # specifications
                  # json-2.1.0.gemspec
```

Darüber hinaus erkennt Lambda automatisch alle Bibliotheken im `/opt/lib`-Verzeichnis und alle Binärdateien im `/opt/bin`-Verzeichnis. Um sicherzustellen, dass Lambda Ihren Ebeneninhalt korrekt findet, können Sie auch eine Ebene mit der folgenden Struktur erstellen:

```
custom-layer.zip
# lib
    | lib_1
    | lib_2
# bin
    | bin_1
    | bin_2
```

Nachdem Sie Ihre Ebene gebündelt haben, sehen Sie sich the section called “Erstellen und Löschen von Ebenen” und the section called “Hinzufügen von Ebenen” an, um die Einrichtung Ihrer Ebene abzuschließen.

Erstellen von ZIP-Bereitstellungspaketen mit nativen Bibliotheken

Viele gängige Ruby-Gems wie `nokogiri`, `nio4r` und `mysql` enthalten native, in C geschriebene Erweiterungen. Wenn Sie Ihrem Bereitstellungspaket Bibliotheken hinzufügen, die C-Code enthalten, müssen Sie Ihr Paket korrekt erstellen, damit es mit der Lambda-Ausführungsumgebung kompatibel ist.

Für Produktionsanwendungen empfehlen wir, Ihren Code mithilfe von AWS Serverless Application Model (AWS SAM) zu erstellen und bereitzustellen. AWS SAM Verwenden Sie die `sam build --use-container` Option, um Ihre Funktion in einem Lambda-ähnlichen Docker-Container zu erstellen. Weitere Informationen AWS SAM zur Bereitstellung Ihres Funktionscodes finden Sie im Entwicklerhandbuch unter Anwendungen erstellen.AWS SAM

Um ein .zip-Bereitstellungspaket zu erstellen, das Gems mit nativen Erweiterungen enthält AWS SAM, ohne es zu verwenden, können Sie alternativ einen Container verwenden, um Ihre Abhängigkeiten in einer Umgebung zu bündeln, die der Lambda Ruby-Laufzeitumgebung entspricht. Für diese Schritte muss Docker auf Ihrem Build-Computer installiert sein. Weitere Informationen zur Installation von Docker finden Sie unter Install Docker Engine.

So erstellen Sie ein ZIP-Bereitstellungspaket in einem Docker-Container

1. Erstellen Sie auf Ihrem lokalen Build-Computer einen Ordner als Speicherort für Ihren Container. Erstellen Sie in diesem Ordner eine Datei mit dem Namen `dockerfile` und fügen Sie folgenden Code in die Datei ein:

   ```
   FROM public.ecr.aws/sam/build-ruby3.2:latest-x86_64
   RUN gem update bundler
   CMD "/bin/bash"
   ```

2. Führen Sie in dem Ordner, in dem Sie Ihre `dockerfile`-Datei erstellt haben, den folgenden Befehl aus, um den Docker-Container zu erstellen:

   ```
   docker build -t awsruby32 .
   ```

3. Navigieren Sie zu dem Projektverzeichnis, das die Datei vom Typ `.rb` mit dem Handler-Code Ihrer Funktion sowie die `Gemfile`-Datei mit den Abhängigkeiten Ihrer enthält. Führen Sie in diesem Verzeichnis den folgenden Befehl aus, um den Lambda-Ruby-Container zu starten:

   Linux/MacOS

   ```
   docker run --rm -it -v $PWD:/var/task -w /var/task awsruby32
   ```

> **Note**
>
> In macOS wird möglicherweise eine Warnung mit dem Hinweis angezeigt, dass die Plattform des angeforderten Images nicht der erkannten Hostplattform entspricht. Ignorieren Sie diese Warnung.

Windows PowerShell

```
docker run --rm -it -v ${pwd}:var/task -w /var/task awsruby32
```

Wenn Ihr Container startet, sollte eine Bash-Aufforderung angezeigt werden.

```
bash-4.2#
```

4. Konfigurieren Sie das Hilfsprogramm „bundle“, um die in Ihrer `Gemfile`-Datei angegebenen Gems in einem lokalen Verzeichnis namens `vendor/bundle` zu installieren und Ihre Abhängigkeiten zu installieren.

```
bash-4.2# bundle config set --local path 'vendor/bundle' && bundle install
```

5. Erstellen Sie das ZIP-Bereitstellungspaket mit Ihrem Funktionscode und den zugehörigen Abhängigkeiten. In diesem Beispiel hat die Datei, die den Handler-Code Ihrer Funktion enthält, den Namen `lambda_function.rb`.

```
bash-4.2# zip -r my_deployment_package.zip lambda_function.rb vendor
```

6. Verlassen Sie den Container und kehren Sie zu Ihrem lokalen Projektverzeichnis zurück.

```
bash-4.2# exit
```

Nun können Sie Ihre Lambda-Funktion mithilfe des ZIP-Bereitstellungspakets erstellen oder aktualisieren. Siehe Erstellen und Aktualisieren von Ruby-Lambda-Funktionen mithilfe von ZIP-Dateien

Erstellen und Aktualisieren von Ruby-Lambda-Funktionen mithilfe von ZIP-Dateien

Nach der Erstellung Ihres ZIP-Bereitstellungspakets können Sie es verwenden, um eine neue Lambda-Funktion zu erstellen oder eine vorhandene zu aktualisieren. Sie können Ihr .zip-Paket mithilfe der Lambda-Konsole, der und der AWS Command Line Interface Lambda-API bereitstellen. Sie können Lambda-Funktionen auch mit AWS Serverless Application Model (AWS SAM) und AWS CloudFormation erstellen und aktualisieren.

Die maximale Größe eines ZIP-Bereitstellungspakets für Lambda beträgt 250 MB (entpackt). Beachten Sie, dass dieser Grenzwert für die kombinierte Größe aller hochgeladenen Dateien gilt, einschließlich aller Lambda-Ebenen.

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Schreibweise von Linux-Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen () für Verzeichnisse und ausführbare Dateien. rwxr-xr-x

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Konsole

Eine neue Funktion müssen Sie zuerst in der Konsole erstellen und dann Ihr ZIP-Archiv hochladen. Zum Aktualisieren einer bestehenden Funktion öffnen Sie die Seite für Ihre Funktion und gehen dann genauso vor, um Ihre aktualisierte ZIP-Datei hinzuzufügen.

Bei einer ZIP-Datei mit unter 50 MB können Sie eine Funktion erstellen oder aktualisieren, indem Sie die Datei direkt von Ihrem lokalen Computer hochladen. Bei ZIP-Dateien mit einer Größe von mehr als 50 MB müssen Sie Ihr Paket zuerst in einen Amazon-S3-Bucket hochladen. Anweisungen zum

Hochladen einer Datei in einen Amazon S3-Bucket mithilfe von finden Sie unter Erste Schritte mit Amazon S3. AWS Management Console Informationen zum Hochladen von Dateien mit dem AWS CLI finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch.

> **Note**
>
> Sie können den Bereitstellungspakettyp (.zip oder Container-Image) für eine bestehende Funktion nicht ändern. Sie können beispielsweise eine Container-Image-Funktion nicht so konvertieren, dass sie ein ZIP-Dateiarchiv verwendet. Sie müssen eine neue Funktion erstellen.

So erstellen Sie eine neue Funktion (Konsole)

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Funktion erstellen aus.
2. Wählen Sie Author from scratch aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie als Funktionsname den Namen Ihrer Funktion ein.
   b. Wählen Sie für Laufzeit die Laufzeit aus, die Sie verwenden möchten.
   c. (Optional) Für Architektur wählen Sie die Befehlssatz-Architektur für Ihre Funktion aus. Die Standardarchitektur ist x86_64. Stellen Sie sicher, dass das ZIP-Bereitstellungspaket für Ihre Funktion mit der von Ihnen gewählten Befehlssatzarchitektur kompatibel ist.
4. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
5. Wählen Sie Funktion erstellen. Lambda erstellt eine grundlegende „Hello World“-Funktion mit der von Ihnen gewählten Laufzeit.

So laden Sie ein ZIP-Archiv von Ihrem lokalen Computer hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie die ZIP-Datei aus.
5. Laden Sie die ZIP-Datei wie folgt hoch:

a. Wählen Sie Hochladen und dann Ihre ZIP-Datei in der Dateiauswahl aus.

b. Klicken Sie auf Open.

c. Wählen Sie Speichern.

So laden Sie ein ZIP-Archiv aus einem Amazon-S3-Bucket hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie eine neue ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie den Amazon-S3-Speicherort aus.
5. Fügen Sie die Amazon-S3-Link-URL Ihrer ZIP-Datei ein und wählen Sie Speichern aus.

ZIP-Dateifunktionen mithilfe des Konsolencode-Editors aktualisieren

Für einige Funktionen mit ZIP-Bereitstellungspaketen können Sie Ihren Funktionscode direkt mit dem in der Lambda-Konsole integrierten Code-Editor aktualisieren. Zur Verwendung dieses Features muss Ihre Funktion folgende Kriterien erfüllen:

- Ihre Funktion muss eine der interpretierten Sprache der Laufzeit verwenden (Python, Node.js oder Ruby).
- Das Bereitstellungspaket Ihrer Funktion muss kleiner als 3 MB sein.

Funktionscode für Funktionen mit Container-Image-Bereitstellungspaketen kann nicht direkt in der Konsole bearbeitet werden.

So aktualisieren Sie Ihren Funktionscode mit dem Code-Editor

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Ihre Funktion aus.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle Ihre Quellcodedatei aus und bearbeiten Sie sie im integrierten Code-Editor.
4. Nach der Bearbeitung Ihres Codes wählen Sie Bereitstellen aus, um Ihre Änderungen zu speichern und Ihre Funktion zu aktualisieren.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe der AWS CLI

Sie können die AWS CLI verwenden, um eine neue Funktion zu erstellen oder eine vorhandene unter Verwendung einer ZIP-Datei zu aktualisieren. Verwenden Sie die Erstellungsfunktion und die update-function-codeBefehle, um Ihr .zip-Paket bereitzustellen. Wenn Ihre ZIP-Datei kleiner als 50 MB ist, können Sie das ZIP-Paket von einem Dateispeicherort auf Ihrem lokalen Build-Computer hochladen. Bei größeren Dateien müssen Sie Ihr ZIP-Paket aus einem Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

> **Note**
>
> Wenn Sie Ihre ZIP-Datei mithilfe von aus einem Amazon S3 S3-Bucket hochladen AWS CLI, muss sich der Bucket im selben Verzeichnis befinden AWS-Region wie Ihre Funktion.

Um eine neue Funktion mithilfe einer .zip-Datei mit dem zu erstellen AWS CLI, müssen Sie Folgendes angeben:

- Den Namen Ihrer Funktion (`--function-name`)
- Die Laufzeit Ihrer Funktion (`--runtime`)
- Den Amazon-Ressourcennamen (ARN) der Ausführungsrolle der Funktion (`--role`).
- Den Namen der Handler-Methode in Ihrem Funktionscode (`--handler`)

Sie müssen auch den Speicherort Ihrer ZIP-Datei angeben. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda create-function --function-name myFunction \
--runtime ruby3.2 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigte `--code`-Option. Sie müssen den `S3ObjectVersion`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda create-function --function-name myFunction \
```

```
--runtime ruby3.2 --handler lambda_function.lambda_handler \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=DOC-EXAMPLE-BUCKET,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Um eine vorhandene Funktion mit der CLI zu aktualisieren, geben Sie den Namen Ihrer Funktion unter Verwendung des `--function-name`-Parameters an. Sie müssen auch den Speicherort der ZIP-Datei angeben, die Sie zum Aktualisieren Ihres Funktionscodes verwenden möchten. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigten `--s3-bucket`- und `--s3-key`-Optionen. Sie müssen den `--s3-object-version`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket DOC-EXAMPLE-BUCKET --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Lambda-API

Um Funktionen zu erstellen und zu konfigurieren, die ein ZIP-Dateiarchiv verwenden, verwenden Sie die folgenden API-Operationen:

- CreateFunction
- UpdateFunctionCode

Funktionen mit ZIP-Dateien erstellen und aktualisieren mit AWS SAM

Das AWS Serverless Application Model (AWS SAM) ist ein Toolkit, das dabei hilft, den Prozess der Erstellung und Ausführung serverloser Anwendungen zu optimieren. AWS Sie definieren die Ressourcen für Ihre Anwendung in einer YAML- oder JSON-Vorlage und verwenden die AWS SAM Befehlszeilenschnittstelle (AWS SAM CLI), um Ihre Anwendungen zu erstellen, zu verpacken und bereitzustellen. Wenn Sie eine Lambda-Funktion aus einer AWS SAM Vorlage erstellen, AWS SAM wird automatisch ein ZIP-Bereitstellungspaket oder ein Container-Image mit Ihrem Funktionscode

und allen von Ihnen angegebenen Abhängigkeiten erstellt. Weitere Informationen zur Verwendung AWS SAM zum Erstellen und Bereitstellen von Lambda-Funktionen finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model Entwicklerhandbuch.

Sie können es auch verwenden AWS SAM , um eine Lambda-Funktion mithilfe eines vorhandenen ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion zu erstellen AWS SAM, können Sie Ihre ZIP-Datei in einem Amazon S3 S3-Bucket oder in einem lokalen Ordner auf Ihrem Build-Computer speichern. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS SAM Vorlage spezifiziert die `AWS::Serverless::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `CodeUri`- auf die Amazon S3 S3-URI, den Pfad zum lokalen Ordner oder FunctionCodeObjekt des Funktionscodes gesetzt
- `Runtime` – festlegen auf die gewünschte Laufzeit

Wenn Ihre ZIP-Datei größer als 50 MB ist, müssen Sie sie nicht zuerst in einen Amazon S3 S3-Bucket hochladen. AWS SAM AWS SAM kann .zip-Pakete bis zur maximal zulässigen Größe von 250 MB (entpackt) von einem Speicherort auf Ihrem lokalen Build-Computer hochladen.

Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei in finden Sie AWS::Serverless::Functionim AWS SAM Entwicklerhandbuch.AWS SAM

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe von AWS CloudFormation

Sie können verwenden AWS CloudFormation , um eine Lambda-Funktion mithilfe eines ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion aus einer ZIP-Datei zu erstellen, müssen Sie Ihre Datei zunächst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS CloudFormation Vorlage spezifiziert die `AWS::Lambda::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `Code` – Geben Sie den Namen des Amazon-S3-Buckets und den ZIP-Dateinamen in die Felder `S3Bucket` und `S3Key` ein
- `Runtime` – festlegen auf die gewünschte Laufzeit

Die AWS CloudFormation generierte ZIP-Datei darf 4 MB nicht überschreiten. Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei finden Sie AWS::Lambda::Functionim AWS CloudFormation Benutzerhandbuch. AWS CloudFormation

Bereitstellen von Ruby-Lambda-Funktionen mit Container-Images

Es gibt drei Möglichkeiten, ein Container-Image für eine Ruby-Lambda-Funktion zu erstellen:

- Verwenden Sie ein AWS Basis-Image für Ruby

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.

- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ruby in das Image aufnehmen.

- Verwenden Sie ein Nicht-Basis-Image AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Ruby in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

Themen

- Verwenden Sie ein AWS Basis-Image für Ruby
- Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

AWS Basis-Images für Ruby

AWS stellt die folgenden Basis-Images für Ruby bereit:

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
3.3	Rubin 3.3	Amazon Linux 2023	Dockerfile für Ruby 3.3 auf GitHub	
3.2	Ruby 3.2	Amazon Linux 2	Dockerfile für Ruby 3.2 auf GitHub	

Amazon-ECR-Repository: gallery.ecr.aws/lambda/ruby

Verwenden Sie ein AWS Basis-Image für Ruby

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker
- Ruby

Erstellen eines Images aus einem Base Image

Erstellen eines Container-Images für Ruby

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir example
cd example
```

2. Erstellen Sie eine neue Datei mit dem Namen `Gemfile`. Hier listen Sie die benötigten RubyGems Pakete für Ihre Anwendung auf. Das AWS SDK for Ruby ist erhältlich bei RubyGems. Sie sollten bestimmte AWS Service Gems für die Installation auswählen. Um beispielsweise das Ruby-Gem für Lambda zu verwenden, sollte Ihr Gemfile so aussehen:

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

   Alternativ enthält das aws-sdk-Gem jedes verfügbare AWS Service-Gem. Dieses Gem ist sehr groß. Wir empfehlen, es nur zu verwenden, wenn Sie auf viele AWS Dienste angewiesen sind.

3. Installieren Sie die im Gemfile angegebenen Abhängigkeiten mithilfe von bundle install.

```
bundle install
```

4. Erstellen Sie eine neue Datei mit dem Namen `lambda_function.rb`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example Ruby-Funktion

```
module LambdaFunction
  class Handler
    def self.process(event:,context:)
      "Hello from Lambda!"
    end
  end
end
```

5. Erstellen Sie eine neue Docker-Datei. Es folgt ein Beispiel für ein Dockerfile, das ein AWS - Basis-Image verwendet. Dieses Dockerfile verwendet die folgende Konfiguration:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.
   - Verwenden Sie den Befehl COPY, um den Funktionscode und die Laufzeitabhängigkeiten in eine von Lambda definierte Umgebungsvariable zu `{LAMBDA_TASK_ROOT}` kopieren.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

   Example Dockerfile

```
FROM public.ecr.aws/lambda/ruby:3.2
```

```
# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. In diesem Beispiel ist `docker-image` der Image-Name und `test` der Tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis an den lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden Befehl aus: `Invoke-WebRequest`

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
    "application/json"
   ```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.
   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
```

```
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Beispiel:

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world:latest
   ```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.

7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

Wenn Sie ein OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Laufzeitschnittstellen-Client erweitert die Lambda-Laufzeiten-API, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet.

Installieren Sie den Lambda Runtime Interface Client für Ruby mit dem Paketmanager RubyGems .org:

```
gem install aws_lambda_ric
```

Sie können den Ruby-Runtime-Interface-Client auch von GitHub herunterladen. Der Laufzeitschnittstellen-Client unterstützt die Ruby-Versionen 2.5.x bis 2.7.x.

Das folgende Beispiel zeigt, wie ein Container-Image für Ruby mithilfe eines AWS Nicht-Basis-Images erstellt wird. Das Beispiel-Dockerfile verwendet ein offizielles Ruby-Basis-Image. Das Docker-File enthält den Laufzeitschnittstellen-Client.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- Docker
- Ruby

Erstellen eines Images aus einem alternativen Basis-Image

Erstellen eines Container-Images für Ruby mit einem alternativen Basis-Image

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

   ```
   mkdir example
   cd example
   ```

2. Erstellen Sie eine neue Datei mit dem Namen `Gemfile`. Hier listen Sie die benötigten RubyGems Pakete für Ihre Anwendung auf. Das AWS SDK for Ruby ist erhältlich bei

RubyGems. Sie sollten bestimmte AWS Service Gems für die Installation auswählen. Um beispielsweise das Ruby-Gem für Lambda zu verwenden, sollte Ihr Gemfile so aussehen:

```
source 'https://rubygems.org'

gem 'aws-sdk-lambda'
```

Alternativ enthält das aws-sdk-Gem jedes verfügbare AWS Service-Gem. Dieses Gem ist sehr groß. Wir empfehlen, es nur zu verwenden, wenn Sie auf viele AWS Dienste angewiesen sind.

3. Installieren Sie die im Gemfile angegebenen Abhängigkeiten mithilfe von bundle install.

```
bundle install
```

4. Erstellen Sie eine neue Datei mit dem Namen `lambda_function.rb`. Sie können der Datei zum Testen den folgenden Beispielfunktionscode hinzufügen oder Ihren eigenen verwenden.

   Example Ruby-Funktion

```
module LambdaFunction
  class Handler
    def self.process(event:,context:)
      "Hello from Lambda!"
    end
  end
end
```

5. Erstellen Sie eine neue Docker-Datei. Das folgende Dockerfile verwendet ein Ruby-Basis-Image anstelle eines AWS -Basis-Images. Das Dockerfile enthält den Laufzeitschnittstellen-Client für Ruby, der das Image mit Lambda kompatibel macht. Alternativ können Sie den Laufzeitschnittstellen-Client zum Gemfile Ihrer Anwendung hinzufügen.

   - Legen Sie die `FROM`-Eigenschaft auf das Ruby-Basis-Image fest.
   - Erstellen Sie ein Verzeichnis für den Funktionscode und eine Umgebungsvariable, die auf dieses Verzeichnis verweist. In diesem Beispiel ist das Verzeichnis`/var/task`, das die Lambda-Ausführungsumgebung widerspiegelt. Sie können jedoch ein beliebiges Verzeichnis für den Funktionscode wählen, da das Dockerfile kein Basis-Image verwendet. AWS
   - Legen Sie `ENTRYPOINT` auf das Modul fest, das der Docker-Container beim Start ausführen soll. In diesem Fall ist das Modul der Laufzeitschnittstellen-Client.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

Example Dockerfile

```
FROM ruby:2.7

# Install the runtime interface client for Ruby
RUN gem install aws_lambda_ric

# Add the runtime interface client to the PATH
ENV PATH="/usr/local/bundle/bin:${PATH}"

# Create a directory for the Lambda function
ENV LAMBDA_TASK_ROOT=/var/task
RUN mkdir -p ${LAMBDA_TASK_ROOT}
WORKDIR ${LAMBDA_TASK_ROOT}

# Copy Gemfile and Gemfile.lock
COPY Gemfile Gemfile.lock ${LAMBDA_TASK_ROOT}/

# Install Bundler and the specified gems
RUN gem install bundler:2.4.20 && \
    bundle config set --local path 'vendor/bundle' && \
    bundle install

# Copy function code
COPY lambda_function.rb ${LAMBDA_TASK_ROOT}/

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "aws_lambda_ric" ]

# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "lambda_function.LambdaFunction::Handler.process" ]
```

6. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um das Image lokal zu testen. Sie können den Emulator in Ihr Image einbauen oder ihn mit dem folgenden Verfahren auf Ihrem lokalen Computer installieren.

Installieren des Laufzeitschnittstellen-Emulators auf Ihrem lokalen Computer

1. Führen Sie in Ihrem Projektverzeichnis den folgenden Befehl aus, um den Runtime-Interface-Emulator (x86-64-Architektur) herunterzuladen GitHub und auf Ihrem lokalen Computer zu installieren.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie die GitHub Repository-URL im vorherigen Befehl durch Folgendes:

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   ```

```
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Um den arm64-Emulator zu installieren, ersetzen Sie das `$downloadLink` durch Folgendes:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.
   - `aws_lambda_ric lambda_function.LambdaFunction::Handler.process` ist der `ENTRYPOINT` gefolgt von dem `CMD` aus Ihrem Dockerfile.

   Linux/macOS

   ```
   docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
    9000:8080 \
       --entrypoint /aws-lambda/aws-lambda-rie \
       docker-image:test \
           aws_lambda_ric lambda_function.LambdaFunction::Handler.process
   ```

   PowerShell

   ```
   docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
    9000:8080 `
   --entrypoint /aws-lambda/aws-lambda-rie `
   docker-image:test `
       aws_lambda_ric lambda_function.LambdaFunction::Handler.process
   ```

   Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

3. Veröffentlichen Sie ein Ereignis auf dem lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
    "application/json"
   ```

4. Die Container-ID erhalten.

```
docker ps
```

5. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.
   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
```

```
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Beispiel:

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world:latest
   ```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.

7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

AWS Lambda-Context-Objekt in Ruby

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Methoden

- `get_remaining_time_in_millis` – Gibt die Anzahl der verbleibenden Millisekunden zurück, bevor die Ausführung das Zeitlimit überschreitet.

Context-Eigenschaften

- `function_name` – Der Name der Lambda-Funktion.
- `function_version` – Die Version der Funktion.
- `invoked_function_arn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `memory_limit_in_mb` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `aws_request_id` – Der Bezeichner der Aufrufanforderung.
- `log_group_name` – Protokollgruppe für die Funktion.
- `log_stream_name` – Der Protokollstrom für die Funktionsinstance.
- `deadline_ms` – Das Datum, an dem eine Zeitüberschreitung für die Ausführung eintritt (in Unix-Millisekunden).
- `identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
- `client_context` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.

AWS Lambda Funktionsprotokollierung in Ruby

AWS Lambda überwacht automatisch Lambda-Funktionen in Ihrem Namen und sendet Protokolle an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Auf dieser Seite wird beschrieben, wie Sie eine Protokollausgabe aus dem Code Ihrer Lambda-Funktion erstellen oder mit der AWS Command Line Interface Lambda-Konsole oder der CloudWatch Konsole auf Logs zugreifen.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus dem Code Ihrer Funktion auszugeben, können Sie `puts`-Anweisungen verwenden oder eine Protokollierungsbibliothek, die zu `stdout` oder `stderr` schreibt. Das folgende Beispiel protokolliert die Werte der Umgebungsvariablen und dem Ereignisobjekt.

Example lambda_function.rb

```
# lambda_function.rb

def handler(event:, context:)
    puts "## ENVIRONMENT VARIABLES"
    puts ENV.to_a
    puts "## EVENT"
    puts event.to_a
end
```

Example Protokollformat

```
START RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95 Version: $LATEST
## ENVIRONMENT VARIABLES
environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
 'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]3893xmpl7fac4485b47bb75b671a283c',
 'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})
## EVENT
{'key': 'value'}
END RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95
REPORT RequestId: 8f507cfc-xmpl-4697-b07a-ac58fc914c95  Duration: 15.74 ms  Billed
 Duration: 16 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 130.49 ms
XRAY TraceId: 1-5e34a614-10bdxmplf1fb44f07bc535a1   SegmentId: 07f5xmpl2d1f6f85
 Sampled: true
```

Die Ruby-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die Berichtszeile enthält die folgenden Details.

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.
- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Für detailliertere Protokolle verwenden Sie die the section called “Logger-Bibliothek”.

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der Konsole CloudWatch

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
```

```
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Logger-Bibliothek

Die Ruby-Logger-Bibliothek gibt optimierte Protokolle zurück, die leicht zu lesen sind. Verwenden Sie das Logger-Serviceprogramm, um detaillierte Informationen, Meldungen und Fehlercodes im Zusammenhang mit Ihrer Funktion auszugeben.

```
# lambda_function.rb

require 'logger'

def handler(event:, context:)
  logger = Logger.new($stdout)
  logger.info('## ENVIRONMENT VARIABLES')
  logger.info(ENV.to_a)
  logger.info('## EVENT')
  logger.info(event)
  event.to_a
end
```

Die Ausgabe aus `logger` umfasst die Protokollebene, den Zeitstempel und die Anforderungs-ID.

```
START RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125 Version: $LATEST
[INFO]  2020-01-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ##
 ENVIRONMENT VARIABLES

[INFO]  2020-01-31T22:12:58.534Z    1c8df7d3-xmpl-46da-9778-518e6eca8125
    environ({'AWS_LAMBDA_LOG_GROUP_NAME': '/aws/lambda/my-function',
 'AWS_LAMBDA_LOG_STREAM_NAME': '2020/01/31/[$LATEST]1bbe51xmplb34a2788dbaa7433b0aa4d',
 'AWS_LAMBDA_FUNCTION_NAME': 'my-function', ...})

[INFO]  2020-01-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    ## EVENT

[INFO]  2020-01-31T22:12:58.535Z    1c8df7d3-xmpl-46da-9778-518e6eca8125    {'key':
 'value'}

END RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125
```

```
REPORT RequestId: 1c8df7d3-xmpl-46da-9778-518e6eca8125  Duration: 2.75 ms   Billed
 Duration: 3 ms Memory Size: 128 MB Max Memory Used: 56 MB  Init Duration: 113.51 ms
XRAY TraceId: 1-5e34a66a-474xmpl7c2534a87870b4370   SegmentId: 073cxmpl3e442861
 Sampled: true
```

Instrumentierung von Ruby-Code in AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , damit Sie Lambda-Anwendungen verfolgen, debuggen und optimieren können. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, von der Frontend-API bis hin zu Speicher und Datenbank im Backend. Indem Sie einfach die X-Ray-SDK-Bibliothek zu Ihrer Build-Konfiguration hinzufügen, können Sie Fehler und Latenz für jeden Aufruf aufzeichnen, den Ihre Funktion an einen AWS Dienst tätigt.

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).

4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

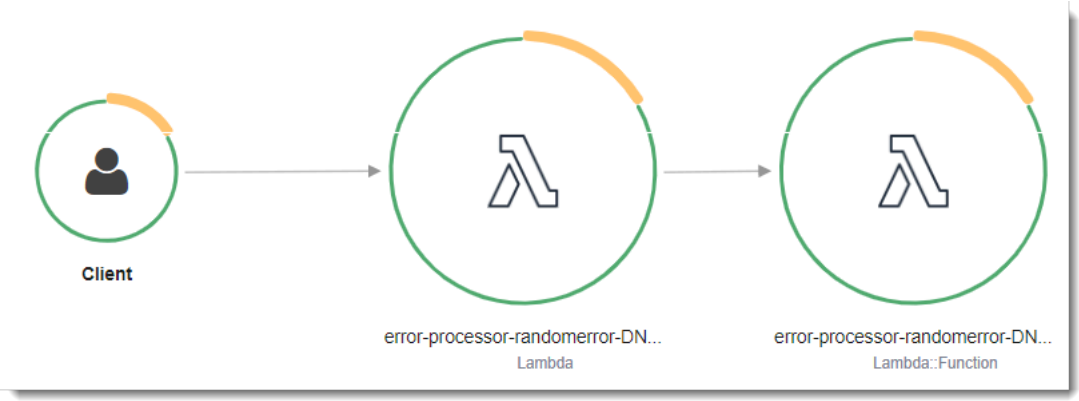
> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray. Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

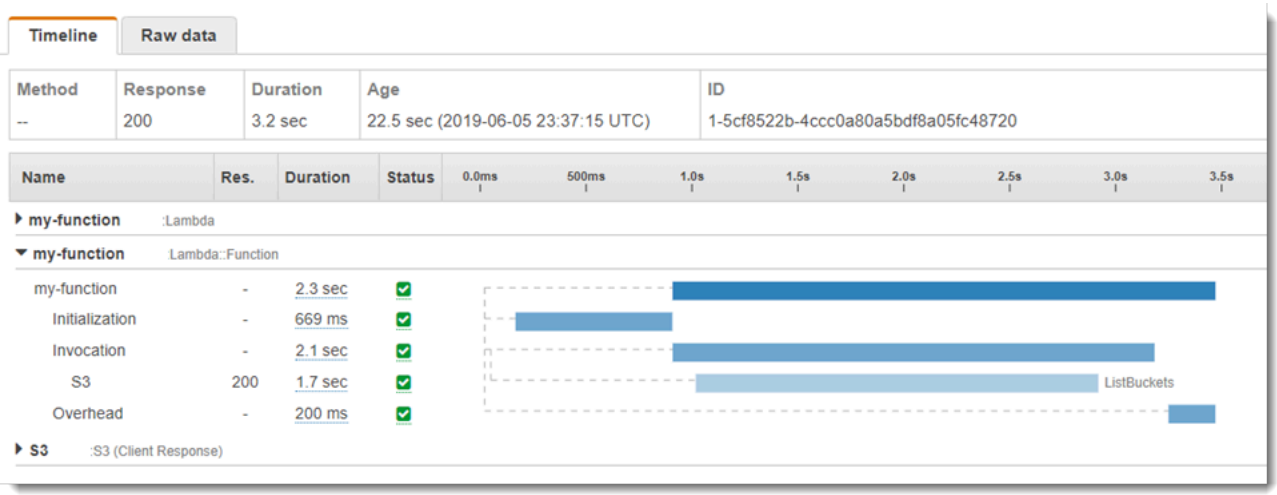
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.

- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können Ihren Handler-Code instrumentieren, um Metadaten aufzuzeichnen und Downstream-Aufrufe nachzuverfolgen. Um Details zu Aufrufen aufzuzeichnen, die Ihr Handler an andere Ressourcen und Services macht, verwenden Sie das X-Ray-SDK für Ruby. Um das SDK zu erhalten, fügen Sie das `aws-xray-sdk`-Paket den Abhängigkeiten Ihrer Anwendung hinzu.

Example blank-ruby/function/Gemfile

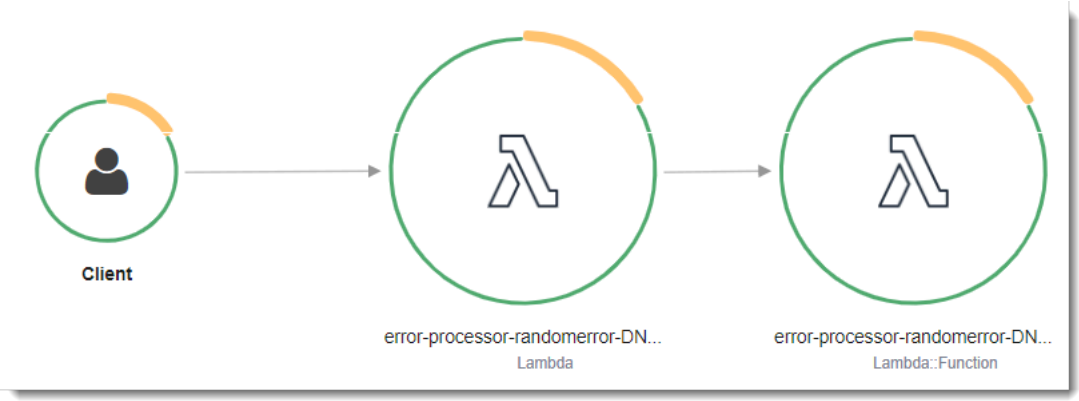
```
# Gemfile
source 'https://rubygems.org'

gem 'aws-xray-sdk', '0.11.4'
gem 'aws-sdk-lambda', '1.39.0'
gem 'test-unit', '3.3.5'
```

Um AWS SDK-Clients zu instrumentieren, benötigen Sie das `aws-xray-sdk/lambda` Modul, nachdem Sie einen Client im Initialisierungscode erstellt haben.

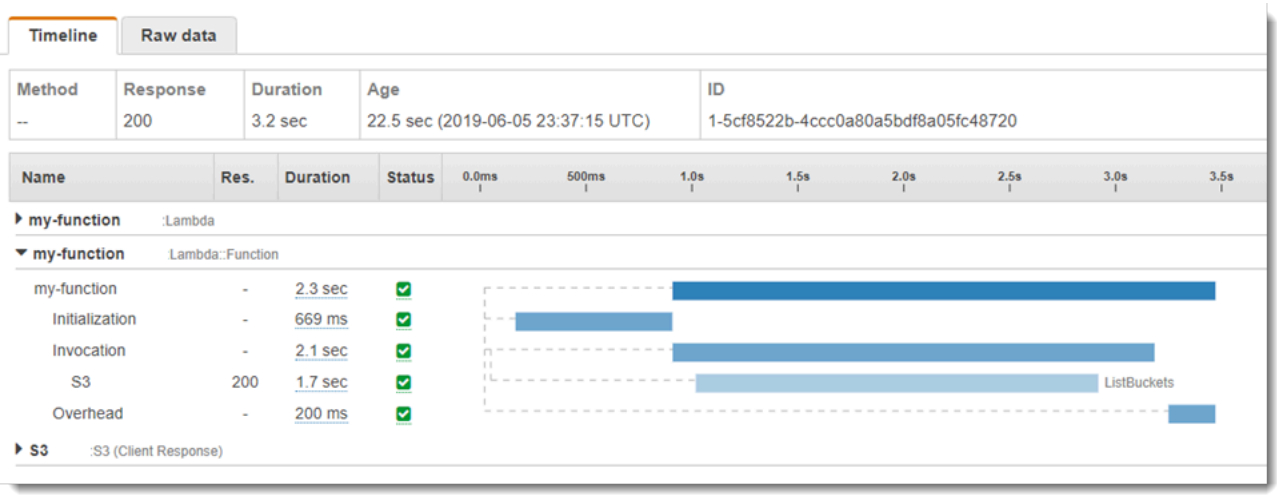
Example blank-ruby/function/lambda_function.rb — Einen SDK-Client verfolgen AWS

```
# lambda_function.rb
require 'logger'
require 'json'
require 'aws-sdk-lambda'
$client = Aws::Lambda::Client.new()
$client.get_account_settings()

require 'aws-xray-sdk/lambda'

def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  ...
```

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.

- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter Das X-Ray-SDK SDK for Ruby im AWS X-Ray Entwicklerhandbuch.

Sections

Aktivieren der aktiven Ablaufverfolgung mit der Lambda-API

Verwenden Sie die folgenden API-Operationen, um die Tracing-Konfiguration mit dem AWS SDK AWS CLI oder zu verwalten:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Aktiviert die aktive Ablaufverfolgung mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Speichern von Laufzeitabhängigkeiten in einer Ebene

Wenn Sie das X-Ray-SDK verwenden, um AWS SDK-Clients Ihren Funktionscode zu instrumentieren, kann Ihr Bereitstellungspaket ziemlich umfangreich werden. Um Laufzeitabhängigkeiten bei jeder Aktualisierung des Funktionscodes zu vermeiden, verpacken Sie das X-Ray-SDK in einer Lambda-Ebene.

Das folgende Beispiel zeigt eine `AWS::Serverless::LayerVersion`-Ressource, die das X-Ray-SDK für Ruby speichert.

Example template.yml – Abhängigkeitenebene

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: function/.
      Tracing: Active
      Layers:
```

```
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-ruby-lib
      Description: Dependencies for the blank-ruby sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - ruby2.5
```

Bei dieser Konfiguration aktualisieren Sie die Bibliotheksebene nur, wenn Sie Ihre Laufzeitabhängigkeiten ändern. Da das Funktionsbereitstellungspaket nur Ihren Code enthält, kann dies dazu beitragen, die Upload-Zeiten zu reduzieren.

Das Erstellen einer Ebene für Abhängigkeiten erfordert Build-Konfigurationsänderungen, um das Ebenen-Archiv vor der Bereitstellung zu generieren. Ein funktionierendes Beispiel finden Sie in der Beispielanwendung blank-ruby .

Erstellen von Lambda-Funktionen mit Java

Sie können Java-Code in AWS Lambda ausführen. Lambda bietet Laufzeiten für Java, die Ihren Code ausführen, um Ereignisse zu verarbeiten. Ihr Code wird in einer Amazon Linux-Umgebung ausgeführt, die AWS Anmeldeinformationen von einer AWS Identity and Access Management (IAM-) Rolle enthält, die Sie verwalten.

Lambda unterstützt die folgenden Java-Laufzeiten.

Java

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Java 21	`java21`	Amazon Linux 2023			
Java 17	`java17`	Amazon Linux 2			
Java 11	`java11`	Amazon Linux 2			
Java 8	`java8.al2`	Amazon Linux 2			

Lambda stellt die folgenden Bibliotheken für Java-Funktionen bereit:

- com.amazonaws:aws-lambda-java-core (erforderlich) – definiert Handler-Methodenschnittstellen und das Kontextobjekt, das die Laufzeit an den Handler übergibt. Wenn Sie eigene Eingabetypen definieren, benötigen Sie nur diese eine Bibliothek.
- com.amazonaws:aws-lambda-java-events – Eingabetypen für Ereignisse von Services, die Lambda-Funktionen aufrufen.
- com.amazonaws:aws-lambda-java-log4j2 – Eine Appender-Bibliothek für Apache Log4j 2, mit der Sie die Anfrage-ID für den aktuellen Aufruf zu Ihren Funktionsprotokollen hinzufügen können.
- AWS SDK for Java 2.0 — Das offizielle AWS SDK für die Programmiersprache Java.

> **Important**
>
> Verwenden Sie keine privaten Komponenten der JDK API, wie private Felder, Methoden oder Klassen. Nicht öffentliche API-Komponenten können sich bei jedem Update ändern oder entfernt werden, was dazu führen kann, dass Ihre Anwendung nicht mehr funktioniert.

So erstellen Sie eine Java-Funktion

1. Öffnen Sie die Lambda-Konsole.
2. Wählen Sie Funktion erstellen.
3. Konfigurieren Sie die folgenden Einstellungen:
   - Funktionsname: Geben Sie einen Namen für die Funktion ein.
   - Runtime: Wählen Sie Java 21.
4. Wählen Sie Funktion erstellen.
5. Um ein Testereignis zu konfigurieren, wählen Sie Test.
6. Geben Sie für Event name (Ereignisname) **`test`** ein.
7. Wählen Sie Änderungen speichern aus.
8. Wählen Sie Test, um die Funktion aufzurufen.

Die Konsole erstellt eine Lambda-Funktion mit einer Handler-Klasse namens `Hello`. Da es sich bei Java um eine kompilierte Sprache handelt, können Sie den Quellcode in der Lambda-Konsole nicht anzeigen oder bearbeiten, aber Sie können seine Konfiguration ändern, ihn aufrufen und Auslöser konfigurieren.

> **Note**
>
> Um mit der Anwendungsentwicklung in Ihrer lokalen Umgebung zu beginnen, stellen Sie eine der Beispielanwendungen bereit, die im GitHub Repository dieses Handbuchs verfügbar sind.

Die `Hello`-Klasse hat eine Funktion mit dem Namen `handleRequest`, die ein Ereignisobjekt und ein Kontext-Objekt übernimmt. Dies ist die Handler-Funktion, die bei einem Aufruf der Funktion von Lambda aufgerufen wird. Die Java-Funktionslaufzeit ruft Aufrufereignisse von Lambda ab und

leitet sie an den Handler weiter. In der Konfiguration der Funktion lautet der Wert für den Handler `example.Hello::handleRequest`.

Um den Funktionscode zu aktualisieren, erstellen Sie ein Bereitstellungspaket, d. h. ein ZIP-Datei-Archiv handelt, das Ihren Funktionscode enthält. Mit fortschreitender Funktionserstellung sollten Sie Ihren Funktionscode in der Versionskontrolle speichern, Bibliotheken hinzufügen und Bereitstellungen automatisieren. Beginnen Sie mit der Erstellung eines Bereitstellungspakets und der Aktualisierung Ihres Codes in der Befehlszeile.

Die Funktionslaufzeit übergibt neben dem Aufrufereignis ein Context-Objekt an den Handler. Das Context-Objekt enthält zusätzliche Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung. Weitere Informationen erhalten Sie über die Umgebungsvariablen.

Ihre Lambda-Funktion wird mit einer CloudWatch Logs-Protokollgruppe geliefert. Die Funktionslaufzeit sendet Details zu jedem Aufruf an CloudWatch Logs. Es leitet alle Protokolle weiter, die Ihre Funktion während des Aufrufs ausgibt. Wenn Ihre Funktion einen Fehler zurückgibt, formatiert Lambda den Fehler und gibt ihn an den Aufrufer zurück.

Themen

Definieren Sie den Lambda-Funktionshandler in Java

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Das GitHub Repo für dieses Handbuch enthält easy-to-deploy Beispielanwendungen, die eine Vielzahl von Handlertypen demonstrieren. Weitere Informationen finden Sie am Ende dieses Themas.

Sections

Beispiel-Handler: Java-17-Laufzeiten

Im folgenden Java-17-Beispiel definiert eine Klasse mit dem Namen `HandlerIntegerJava17` eine Handler-Methode mit dem Namen `handleRequest`. Die Handler-Methode nimmt die folgenden Eingaben auf:

- Einen `IntegerRecord`, wobei es sich um einen benutzerdefinierten Java-Datensatz handelt, der Ereignisdaten darstellt. In diesem Beispiel definieren wir `IntegerRecord` wie folgt:

```
record IntegerRecord(int x, int y, String message) {
}
```

- Ein Kontextobjekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Angenommen, wir möchten eine Funktion schreiben, die `message` aus der Eingabe `IntegerRecord` protokolliert und die Summe von `x` und `y` zurückgibt. Das Folgende ist der Funktionscode:

Example HandlerIntegerJava17.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

// Handler value: example.HandlerInteger
public class HandlerIntegerJava17 implements RequestHandler<IntegerRecord, Integer>{

  @Override
  /*
   * Takes in an InputRecord, which contains two integers and a String.
   * Logs the String, then returns the sum of the two Integers.
   */
  public Integer handleRequest(IntegerRecord event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    logger.log("String found: " + event.message());
    return event.x() + event.y();
  }
}

record IntegerRecord(int x, int y, String message) {
}
```

Sie geben an, welche Methode Lambda aufrufen soll, indem Sie den Handler-Parameter für die Konfiguration Ihrer Funktion festlegen. Sie können den Hander in den folgenden Formaten ausdrücken:

- *package*.*Class*::*method* – Vollständiges Format. Beispiel: `example.Handler::handleRequest`.
- *package*.*Class* – Abgekürztes Format für Funktionen, die eine Handler-Schnittstelle implementieren. Zum Beispiel: `example.Handler`.

Wenn Lambda Ihren Handler aufruft, empfängt die Lambda-Laufzeit ein Ereignis als JSON-formatierte Zeichenfolge und wandelt es in ein Objekt um. Für das vorherige Beispiel könnte ein Beispielereignis wie folgt aussehen:

Example event.json

```
{
  "x": 1,
  "y": 20,
  "message": "Hello World!"
}
```

Sie können diese Datei speichern und Ihre Funktion lokal mit dem folgenden AWS Command Line Interface (CLI-) Befehl testen:

```
aws lambda invoke --function-name function_name --payload file://event.json out.json
```

Beispiel-Handler: Java-11-Laufzeiten und darunter

Lambda unterstützt Datensätze in der Laufzeit Java 17 und höher In allen Java-Laufzeiten können Sie eine Klasse verwenden, um Ereignisdaten darzustellen. Das folgende Beispiel verwendet eine Liste von Ganzzahlen und ein Kontextobjekt als Eingabe und gibt die Summe aller Ganzzahlen in der Liste zurück.

Example handler.java

Im folgenden Beispiel definiert eine Klasse mit dem Namen `Handler` eine Handler-Methode mit dem Namen `handleRequest`. Die Handler-Methode nimmt ein Ereignis- und ein Kontextobjekt als Eingabe an und gibt eine Zeichenfolge zurück.

Example HandlerList.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.List;

// Handler value: example.HandlerList
public class HandlerList implements RequestHandler<List<Integer>, Integer>{

  @Override
  /*
```

```
    * Takes a list of Integers and returns its sum.
    */
  public Integer handleRequest(List<Integer> event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    logger.log("EVENT TYPE: " + event.getClass().toString());
    return event.stream().mapToInt(Integer::intValue).sum();
  }
}
```

Weitere Beispiele finden Sie unter Beispiel-Handler-Code.

Initialisierungscode

Lambda führt Ihren statischen Code und den Klassenkonstruktor während der Initialisierungsphase aus, bevor Ihre Funktion zum ersten Mal aufgerufen wird. Ressourcen, die während der Initialisierung erstellt werden, bleiben zwischen Aufrufen im Speicher und können vom Handler tausende Male wiederverwendet werden. Daher können Sie Initialisierungscode außerhalb Ihrer Haupt-Handler-Methode hinzufügen, um Rechenzeit zu sparen und Ressourcen für mehrere Aufrufe wiederzuverwenden.

Im folgenden Beispiel befindet sich der Client-Initialisierungscode außerhalb der Haupt-Handler-Methode. Die Laufzeit initialisiert den Client, bevor die Funktion ihr erstes Ereignis ausführt. Nachfolgende Ereignisse sind viel schneller, da Lambda den Client nicht erneut initialisieren muss.

Example handler.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.Map;

import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.GetAccountSettingsResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;

// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, String> {
```

```
    private static final LambdaClient lambdaClient = LambdaClient.builder().build();

    @Override
    public String handleRequest(Map<String,String> event, Context context) {

        LambdaLogger logger = context.getLogger();
        logger.log("Handler invoked");

        GetAccountSettingsResponse response = null;
        try {
            response = lambdaClient.getAccountSettings();
        } catch(LambdaException e) {
            logger.log(e.getMessage());
        }
        return response != null ? "Total code size for your account is " +
 response.accountLimit().totalCodeSize() + " bytes" : "Error";
    }
}
```

Auswählen von Ein- und Ausgabetypen

In der Signatur der Handler-Methode geben Sie den Objekttyp an, dem das Ereignis zugeordnet wird. Im vorangegangenen Beispiel deserialisiert die Java-Laufzeitumgebung das Ereignis in einen Typ, der die `Map<String,String>`-Schnittstelle implementiert. tring-to-string S-Maps funktionieren für flache Ereignisse wie die folgenden:

Example Event.json – Wetterdaten

```
{
  "temperatureK": 281,
  "windKmh": -3,
  "humidityPct": 0.55,
  "pressureHPa": 1020
}
```

Der Wert jedes Feldes muss jedoch eine Zeichenfolge oder eine Zahl sein. Wenn das Ereignis ein Feld mit einem Objekt als Wert enthält, kann es von der Laufzeit nicht deserialisiert werden und gibt einen Fehler zurück.

Wählen Sie einen Eingabetyp aus, der mit den Ereignisdaten arbeitet, die Ihre Funktion verarbeitet. Sie können einen Basistyp, einen generischen Typ oder einen gut definierten Typ verwenden.

Eingabetypen

- `Integer`, `Long`, `Double`, usw. – Das Ereignis ist eine Zahl ohne zusätzliche Formatierung, zum Beispiel: `3.5`. Die Laufzeit wandelt den Wert in ein Objekt des angegebenen Typs um.
- `String` – Das Ereignis ist eine JSON-Zeichenfolge mit Anführungszeichen, z. B.: `"My string."`. Die Laufzeit wandelt den Wert (ohne Anführungszeichen) in ein `String`-Objekt um.
- *`Type`*, `Map<String,`*`Type`*`>` usw. – Das Ereignis ist ein JSON-Objekt. Die Laufzeitumgebung deserialisiert sie in ein Objekt des angegebenen Typs oder der angegebenen Schnittstelle.
- `List<Integer>`, `List<String>`, `List<Object>`, usw. – Das Ereignis ist ein JSON-Array. Die Laufzeitumgebung deserialisiert sie in ein Objekt des angegebenen Typs oder der angegebenen Schnittstelle.
- `InputStream` – Das Ereignis ist ein beliebiger JSON-Typ. Die Laufzeit übergibt einen Bytestream des Dokuments ohne Änderung an den Handler. Sie deserialisieren die Eingabe und schreiben Ausgabe in einen Ausgabestream.
- Bibliothekstyp — Verwenden Sie für Ereignisse, die von AWS Diensten gesendet werden, die Typen in der Bibliothek aws-lambda-java-events.

Wenn Sie Ihren eigenen Eingabetyp definieren, sollte es sich um ein deserialisierbares, veränderbares einfaches altes Java-Objekt (POJO) mit einem Standardkonstruktor und Eigenschaften für jedes Feld im Ereignis handeln. Schlüssel für das Ereignis, die nicht einer Eigenschaft zugeordnet werden, sowie Eigenschaften, die nicht im Ereignis enthalten sind, werden fehlerfrei gelöscht.

Der Ausgabetyp kann ein Objekt oder sei `void`. Die Laufzeit serialisiert Rückgabewerte in Text. Wenn es sich bei der Ausgabe um ein Objekt mit Feldern handelt, wird dies von der Laufzeitumgebung in ein JSON-Dokument serialisiert. Wenn es sich um einen Typ handelt, der einen primitiven Wert umschließt, gibt die Laufzeit eine Textdarstellung dieses Wertes zurück.

Handler-Schnittstellen

Die aws-lambda-java-core-Bibliothek definiert zwei Schnittstellen für Handler-Methoden. Verwenden Sie die bereitgestellten Schnittstellen, um die Handler-Konfiguration zu vereinfachen und die Handler-Methodensignatur zur Kompilierzeit zu validieren.

- com.amazonaws.services.lambda.runtime. RequestHandler
- com.amazonaws.services.lambda.runtime. RequestStreamHandler

Die `RequestHandler`-Schnittstelle ist ein generischer Typ, der zwei Parameter verwendet: den Eingabetyp und den Ausgabetyp. Beide Typen müssen Objekte sein. Wenn Sie diese Schnittstelle verwenden, deserialisiert die Java-Laufzeitumgebung das Ereignis in ein Objekt mit dem Eingabetyp und serialisiert die Ausgabe in Text. Verwenden Sie diese Schnittstelle, wenn die integrierte Serialisierung mit Ihren Ein- und Ausgabetypen funktioniert.

Example Handler.java – Handler-Schnittstelle

```
// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, String>{
  @Override
  public String handleRequest(Map<String,String> event, Context context)
```

Um Ihre eigene Serialisierung zu verwenden, implementieren Sie die `RequestStreamHandler`-Schnittstelle. Mit dieser Schnittstelle übergibt Lamda Ihrem Handler einen Eingabestream und einen Ausgabestream. Der Handler liest Bytes aus dem Eingabestream, schreibt in den Ausgabestream und gibt „void“ zurück.

Im folgenden Beispiel werden gepufferte Lese- und Schreibtypen verwendet, um mit den Eingabe- und Ausgabestreams zu arbeiten.

Example HandlerStream.java

```
import com.amazonaws.services.lambda.runtime.Context
import com.amazonaws.services.lambda.runtime.LambdaLogger
import com.amazonaws.services.lambda.runtime.RequestStreamHandler
...
// Handler value: example.HandlerStream
public class HandlerStream implements RequestStreamHandler {
  @Override
  /*
   * Takes an InputStream and an OutputStream. Reads from the InputStream,
   * and copies all characters to the OutputStream.
   */
  public void handleRequest(InputStream inputStream, OutputStream outputStream, Context
 context) throws IOException
  {
    LambdaLogger logger = context.getLogger();
    BufferedReader reader = new BufferedReader(new InputStreamReader(inputStream,
 Charset.forName("US-ASCII")));
    PrintWriter writer = new PrintWriter(new BufferedWriter(new
 OutputStreamWriter(outputStream, Charset.forName("US-ASCII"))));
```

```
    int nextChar;
    try {
      while ((nextChar = reader.read()) != -1) {
        outputStream.write(nextChar);
      }
    } catch (IOException e) {
      e.printStackTrace();
    } finally {
      reader.close();
      String finalString = writer.toString();
      logger.log("Final string result: " + finalString);
      writer.close();
    }
  }
}
```

Beispiel-Handler-Code

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung verschiedener Handlertypen und Schnittstellen demonstrieren. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS SAM Vorlage und unterstützende Ressourcen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend

verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Die `s3-java` Anwendungen `java-events` und verwenden ein AWS Dienstereignis als Eingabe und geben eine Zeichenfolge zurück. Die `java-basic`-Anwendung umfasst verschiedene Arten von Handlern:

- Handler.java – Nimmt `Map<String,String>` als Eingabe an.
- HandlerInteger.java — Nimmt eine `Integer` als Eingabe entgegen.
- HandlerList.java — Nimmt a `List<Integer>` als Eingabe.
- HandlerStream.java — Nimmt ein `InputStream` und `OutputStream` als Eingabe an.
- HandlerString.java — Akzeptiert ein `String` als Eingabe.
- HandlerWeatherData.java — Nimmt einen benutzerdefinierten Typ als Eingabe.

Um verschiedene Handlertypen zu testen, ändern Sie einfach den Handlerwert in der AWS SAM Vorlage. Ausführliche Anweisungen finden Sie in der Liesmich-Datei der Beispielanwendung.

Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven

Der Code Ihrer AWS Lambda Funktion besteht aus Skripten oder kompilierten Programmen und deren Abhängigkeiten. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Lambda unterstützt zwei Arten von Bereitstellungspaketen: Container-Images und ZIP-Dateiarchiven.

Auf dieser Seite wird beschrieben, wie Sie Ihr Bereitstellungspaket als ZIP-Datei oder Jar-Datei erstellen und dann das Bereitstellungspaket verwenden, um Ihren Funktionscode AWS Lambda mithilfe von AWS Command Line Interface (AWS CLI) bereitzustellen.

Sections

Voraussetzungen

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Tools und Bibliotheken

Lambda stellt die folgenden Bibliotheken für Java-Funktionen bereit:

- com.amazonaws: aws-lambda-java-core (erforderlich) — Definiert Handler-Methodenschnittstellen und das Kontextobjekt, das die Runtime an den Handler übergibt. Wenn Sie eigene Eingabetypen definieren, benötigen Sie nur diese eine Bibliothek.
- com.amazonaws: aws-lambda-java-events — Eingabetypen für Ereignisse von Diensten, die Lambda-Funktionen aufrufen.
- com.amazonaws: aws-lambda-java-log 4j2 — Eine Appender-Bibliothek für Apache Log4j 2, mit der Sie die Anforderungs-ID für den aktuellen Aufruf zu Ihren Funktionsprotokollen hinzufügen können.
- AWS SDK for Java 2.0 — Das offizielle AWS SDK für die Programmiersprache Java.

Diese Bibliotheken sind über Maven Central Repositoryverfügbar. Fügen Sie sie wie folgt der Build-Definition hinzu.

Gradle

```
dependencies {
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'
}
```

Maven

```
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-core</artifactId>
      <version>1.2.2</version>
    </dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-events</artifactId>
      <version>3.11.1</version>
    </dependency>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-log4j2</artifactId>
      <version>1.5.1</version>
    </dependency>
  </dependencies>
```

Um ein Bereitstellungspaket zu erstellen, kompilieren Sie den Funktionscode und die Abhängigkeiten in einer einzelnen ZIP- oder Java-Archivdatei (JAR). Verwenden Sie für Gradle den `Zip`-Build-Typ. Verwenden Sie für Apache Maven das Maven Shade Plugin. Verwenden Sie zum Hochladen Ihres Bereitstellungspakets die Lambda-Konsole, die Lambda-API oder AWS Serverless Application Model ()AWS SAM.

> **Note**
>
> Um den Umfang des Bereitstellungspakets gering zu halten, verpacken Sie die Abhängigkeiten Ihrer Funktion in Ebenen. Ebenen ermöglichen Ihnen, Ihre Abhängigkeiten unabhängig zu verwalten, können von mehreren Funktionen genutzt werden und können für andere Konten zur gemeinsamen Nutzung freigegeben werden. Weitere Informationen finden Sie unter Lambda-Ebenen.

Erstellen eines Bereitstellungspakets mit Gradle

Um in Gradle ein Bereitstellungspaket mit dem Code Ihrer Funktion und deren Abhängigkeiten zu erstellen, verwenden Sie den Build-Typ `Zip`. Hier ist ein Beispiel aus einer vollständigen build.gradle Datei:

Example build.gradle – Entwicklungs-Aufgabe

```
task buildZip(type: Zip) {
    into('lib') {
        from(jar)
        from(configurations.runtimeClasspath)
    }
}
```

Diese Build-Konfiguration erzeugt ein Bereitstellungspaket im `build/distributions`-Ordner. Innerhalb der `into('lib')`-Anweisung stellt die `jar`-Aufgabe ein JAR-Archiv mit Ihren Hauptklassen in einem Ordner mit dem Namen „`lib`“ zusammen. Die `configurations.runtimeClassPath`-Aufgabe kopiert außerdem Abhängigkeitsbibliotheken aus dem Klassenpfad des Builds in denselben Ordner mit dem Namen „`lib`“.

Example build.gradle – Abhängigkeiten

```
dependencies {
    ...
```

```
    implementation 'com.amazonaws:aws-lambda-java-core:1.2.2'
    implementation 'com.amazonaws:aws-lambda-java-events:3.11.1'
    implementation 'org.apache.logging.log4j:log4j-api:2.17.1'
    implementation 'org.apache.logging.log4j:log4j-core:2.17.1'
    runtimeOnly 'org.apache.logging.log4j:log4j-slf4j18-impl:2.17.1'
    runtimeOnly 'com.amazonaws:aws-lambda-java-log4j2:1.5.1'
    ...
}
```

Lambda lädt JAR-Dateien in alphabetischer Reihenfolge (Unicode). Wenn mehrere JAR-Dateien im `lib`-Verzeichnis die gleiche Klasse enthalten, wird die erste verwendet. Sie können das folgende Shell-Skript zum Identifizieren von doppelten Klassen verwenden.

Example test-zip.sh

```
mkdir -p expanded
unzip path/to/my/function.zip -d expanded
find ./expanded/lib -name '*.jar' | xargs -n1 zipinfo -1 | grep '.*.class' | sort |
 uniq -c | sort
```

Erstellen einer Java-Ebene für Ihre Abhängigkeiten

> **Note**
>
> Die Verwendung von Ebenen mit Funktionen in einer kompilierten Sprache wie Java bietet möglicherweise nicht den gleichen Nutzen wie in einer interpretierten Sprache wie Python. Da es sich bei Java um eine kompilierte Sprache handelt, müssen Ihre Funktionen während der Initialisierungsphase alle freigegebenen Baugruppen manuell in den Speicher laden, was die Kaltstartzeiten erhöhen kann. Stattdessen empfehlen wir, den freigegebenen Code bei der Kompilierung einzuschließen, um die Vorteile der integrierten Compiler-Optimierungen zu nutzen.

Die Anweisungen in diesem Abschnitt zeigen Ihnen, wie Sie Ihre Abhängigkeiten in eine Ebene einschließen. Anweisungen zum Einschließen Ihrer Abhängigkeiten in Ihr Bereitstellungspaket finden Sie unter the section called “Erstellen eines Bereitstellungspakets mit Gradle” oder the section called “Erstellen eines Bereitstellungspakets mit Maven”.

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits

spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Layer-Inhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

- `java/lib` (`CLASSPATH`)

Die Struktur Ihrer Ebene-ZIP-Datei könnte beispielsweise wie folgt aussehen:

```
jackson.zip
# java/lib/jackson-core-2.2.3.jar
```

Darüber hinaus erkennt Lambda automatisch alle Bibliotheken im `/opt/lib`-Verzeichnis und alle Binärdateien im `/opt/bin`-Verzeichnis. Um sicherzustellen, dass Lambda Ihren Ebeneninhalt korrekt findet, können Sie auch eine Ebene mit der folgenden Struktur erstellen:

```
custom-layer.zip
# lib
    | lib_1
    | lib_2
# bin
    | bin_1
    | bin_2
```

Nachdem Sie Ihre Ebene gebündelt haben, sehen Sie sich the section called “Erstellen und Löschen von Ebenen” und the section called “Hinzufügen von Ebenen” an, um die Einrichtung Ihrer Ebene abzuschließen.

Erstellen eines Bereitstellungspakets mit Maven

Verwenden Sie das Maven Shade-Plugin, um ein Bereitstellungspaket mit Maven zu erstellen. Das Plugin erstellt eine JAR-Datei mit dem kompilierten Funktionscode und allen seinen Abhängigkeiten.

Example pom.xml – Plugin-Konfiguration

```
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-shade-plugin</artifactId>
        <version>3.2.2</version>
        <configuration>
          <createDependencyReducedPom>false</createDependencyReducedPom>
```

```
        </configuration>
        <executions>
          <execution>
            <phase>package</phase>
            <goals>
              <goal>shade</goal>
            </goals>
          </execution>
        </executions>
      </plugin>
```

Verwenden Sie den `mvn package`-Befehl, um das Bereitstellungspaket zu erstellen.

```
[INFO] Scanning for projects...
[INFO] -----------------------< com.example:java-maven >-----------------------
[INFO] Building java-maven-function 1.0-SNAPSHOT
[INFO] --------------------------------[ jar ]---------------------------------
...
[INFO] --- maven-jar-plugin:2.4:jar (default-jar) @ java-maven ---
[INFO] Building jar: target/java-maven-1.0-SNAPSHOT.jar
[INFO]
[INFO] --- maven-shade-plugin:3.2.2:shade (default) @ java-maven ---
[INFO] Including com.amazonaws:aws-lambda-java-core:jar:1.2.2 in the shaded jar.
[INFO] Including com.amazonaws:aws-lambda-java-events:jar:3.11.1 in the shaded jar.
[INFO] Including joda-time:joda-time:jar:2.6 in the shaded jar.
[INFO] Including com.google.code.gson:gson:jar:2.8.6 in the shaded jar.
[INFO] Replacing original artifact with shaded artifact.
[INFO] Replacing target/java-maven-1.0-SNAPSHOT.jar with target/java-maven-1.0-
SNAPSHOT-shaded.jar
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  8.321 s
[INFO] Finished at: 2020-03-03T09:07:19Z
[INFO] ------------------------------------------------------------------------
```

Mit diesem Befehl wird eine JAR-Datei im `target`-Verzeichnis generiert.

> **Note**
>
> Wenn Sie mit einem Multi-Release-JAR (MRJAR) arbeiten, müssen Sie das MRJAR (d.h. das vom Maven Shade-Plugin erzeugte shaded JAR) in das `lib`-Verzeichnis aufnehmen und

es zippen, bevor Sie Ihr Bereitstellungspaket zu Lambda hochladen. Andernfalls entpackt Lambda Ihre JAR-Datei möglicherweise nicht richtig, sodass Ihre `MANIFEST.MF`-Datei ignoriert wird.

Wenn Sie die Appender-Bibliothek (`aws-lambda-java-log4j2`) verwenden, müssen Sie auch einen Transformator für das Maven Shade-Plugin konfigurieren. Die Transformator-Bibliothek kombiniert Versionen einer Cache-Datei, die sowohl in der Appender-Bibliothek als auch in Log4j angezeigt wird.

Example pom.xml – Plugin-Konfiguration mit Log4j-2-Appender

```
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-shade-plugin</artifactId>
        <version>3.2.2</version>
        <configuration>
          <createDependencyReducedPom>false</createDependencyReducedPom>
        </configuration>
        <executions>
          <execution>
            <phase>package</phase>
            <goals>
              <goal>shade</goal>
            </goals>
            <configuration>
              <transformers>
                <transformer
implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCacheFile
                </transformer>
              </transformers>
            </configuration>
          </execution>
        </executions>
        <dependencies>
          <dependency>
            <groupId>com.github.edwgiz</groupId>
            <artifactId>maven-shade-plugin.log4j2-cachefile-transformer</artifactId>
            <version>2.13.0</version>
          </dependency>
        </dependencies>
      </plugin>
```

Hochladen eines Bereitstellungspakets mit der Lambda-Konsole

Eine neue Funktion müssen Sie zuerst in der Konsole erstellen und dann Ihre ZIP- oder JAR-Datei hochladen. Zum Aktualisieren einer bestehenden Funktion öffnen Sie die Seite für Ihre Funktion und gehen dann genauso vor, um Ihre aktualisierte ZIP- oder JAR-Datei hinzuzufügen.

Bei einer Bereitstellungspaketdatei unter 50 MB können Sie eine Funktion erstellen oder aktualisieren, indem Sie die Datei direkt von Ihrem lokalen Computer hochladen. Bei ZIP-oder JAR-Dateien mit einer Größe von mehr als 50 MB müssen Sie Ihr Paket zuerst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3-Bucket mithilfe von finden Sie unter Erste Schritte mit Amazon S3. AWS Management Console Informationen zum Hochladen von Dateien mit dem AWS CLI finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch.

> **Note**
>
> Sie können den Bereitstellungspakettyp (.zip oder Container-Image) für eine bestehende Funktion nicht ändern. Sie können beispielsweise eine Container-Image-Funktion nicht so konvertieren, dass sie ein ZIP-Dateiarchiv verwendet. Sie müssen eine neue Funktion erstellen.

So erstellen Sie eine neue Funktion (Konsole)

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Funktion erstellen aus.
2. Wählen Sie Author from scratch aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie als Funktionsname den Namen Ihrer Funktion ein.
   b. Wählen Sie für Laufzeit die Laufzeit aus, die Sie verwenden möchten.
   c. (Optional) Für Architektur wählen Sie die Befehlssatz-Architektur für Ihre Funktion aus. Die Standardarchitektur ist x86_64. Stellen Sie sicher, dass das ZIP-Bereitstellungspaket für Ihre Funktion mit der von Ihnen gewählten Befehlssatzarchitektur kompatibel ist.
4. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
5. Wählen Sie Funktion erstellen. Lambda erstellt eine grundlegende „Hello World“-Funktion mit der von Ihnen gewählten Laufzeit.

So laden Sie ein ZIP- oder JAR-Archiv von Ihrem lokalen Computer (Konsole) hoch

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die ZIP- oder JAR-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie ZIP- oder JAR-Datei aus.
5. Laden Sie die ZIP- oder JAR-Datei wie folgt hoch:
   a. Wählen Sie Hochladen und dann Ihre ZIP- oder JAR-Datei in der Dateiauswahl aus.
   b. Klicken Sie auf Open.
   c. Wählen Sie Speichern.

So laden Sie ein ZIP-Archiv aus einem Amazon-S3-Bucket hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die neue ZIP- oder JAR-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie den Amazon-S3-Speicherort aus.
5. Fügen Sie die Amazon-S3-Link-URL Ihrer ZIP-Datei ein und wählen Sie Speichern aus.

Hochladen eines Bereitstellungspakets mit AWS CLI

Sie können die AWS CLI verwenden, um eine neue Funktion zu erstellen oder eine vorhandene unter Verwendung einer ZIP- oder JAR-Datei zu aktualisieren. Verwenden Sie die Create-Funktion und die update-function-codeBefehle, um Ihr .zip- oder JAR-Paket bereitzustellen. Wenn Ihre Datei kleiner als 50 MB ist, können Sie das Paket von einem Dateispeicherort auf Ihrem lokalen Build-Computer hochladen. Bei größeren Dateien müssen Sie Ihr ZIP-oder JAR-Paket aus einem Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

> **Note**
>
> Wenn Sie Ihre .zip- oder JAR-Datei mithilfe von aus einem Amazon S3 S3-Bucket hochladen AWS CLI, muss sich der Bucket im selben Verzeichnis befinden AWS-Region wie Ihre Funktion.

Um eine neue Funktion mithilfe einer .zip- oder JAR-Datei mit der zu erstellen AWS CLI, müssen Sie Folgendes angeben:

- Den Namen Ihrer Funktion (`--function-name`)
- Die Laufzeit Ihrer Funktion (`--runtime`)
- Den Amazon-Ressourcennamen (ARN) der Ausführungsrolle der Funktion (`--role`).
- Den Namen der Handler-Methode in Ihrem Funktionscode (`--handler`)

Sie müssen auch den Speicherort Ihrer ZIP- oder JAR-Datei angeben. Befindet sich Ihre ZIP- oder JAR-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda create-function --function-name myFunction \
--runtime java21 --handler example.handler \
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigte `--code`-Option. Sie müssen den `S3ObjectVersion`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda create-function --function-name myFunction \
--runtime java21 --handler example.handler \
--role arn:aws:iam::123456789012:role/service-role/my-lambda-role \
--code S3Bucket=DOC-EXAMPLE-BUCKET,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Um eine vorhandene Funktion mit der CLI zu aktualisieren, geben Sie den Namen Ihrer Funktion unter Verwendung des `--function-name`-Parameters an. Sie müssen auch den Speicherort der ZIP-Datei angeben, die Sie zum Aktualisieren Ihres Funktionscodes verwenden möchten. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigten `--s3-bucket`- und `--s3-key`-Optionen. Sie müssen den `--s3-object-version`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket DOC-EXAMPLE-BUCKET --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Hochladen eines Bereitstellungspakets mit AWS SAM

Sie können AWS SAM es verwenden, um die Bereitstellung Ihres Funktionscodes, Ihrer Konfiguration und Ihrer Abhängigkeiten zu automatisieren. AWS SAM ist eine Erweiterung von AWS CloudFormation , die eine vereinfachte Syntax für die Definition serverloser Anwendungen bietet. Die folgende Beispielvorlage definiert eine Funktion mit einem Bereitstellungspaket in dem `build/distributions`-Verzeichnis, das Gradle verwendet.

Example template.yml

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: An AWS Lambda application that calls the Lambda API.
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: build/distributions/java-basic.zip
      Handler: example.Handler
      Runtime: java21
      Description: Java function
      MemorySize: 512
      Timeout: 10
      # Function's execution role
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
        - AWSLambdaVPCAccessExecutionRole
```

```
      Tracing: Active
```

Um die Funktion zu erstellen, verwenden Sie die Befehle „`package`“ und „`deploy`“. Bei diesen Befehlen handelt es sich um Anpassungen an der AWS CLI. Sie umschließen andere Befehle, um das Bereitstellungspaket zu Amazon S3 hochzuladen, die Vorlage mit dem Objekt-URI neu zu schreiben und den Code der Funktion zu aktualisieren.

Im folgenden Beispielskript wird ein Gradle-Build ausgeführt und das von ihm erstellte Bereitstellungspaket wird hochgeladen. Es erstellt einen AWS CloudFormation Stack, wenn Sie es zum ersten Mal ausführen. Wenn der Stack bereits vorhanden ist, wird der vom Skript aktualisiert.

Example deploy.sh

```
#!/bin/bash
set -eo pipefail
aws cloudformation package --template-file template.yml --s3-bucket MY_BUCKET --output-
template-file out.yml
aws cloudformation deploy --template-file out.yml --stack-name java-basic --
capabilities CAPABILITY_NAMED_IAM
```

Ein vollständiges funktionierendes Beispiel finden Sie in den folgenden Beispielanwendungen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-eventsBibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend

verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Bereitstellen von Java-Lambda-Funktionen mit Container-Images

Es gibt drei Möglichkeiten, ein Container-Image für eine Java-Lambda-Funktion zu erstellen:

- Verwenden Sie ein Basis-Image für Java AWS

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.

- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Java in das Image aufnehmen.

- Verwenden Sie ein Nicht-Basis-Image AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für Java in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

Themen

- AWS Basis-Images für Java

- Verwenden Sie ein Basis-Image für Java AWS
- Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

AWS Basis-Images für Java

AWS stellt die folgenden Basis-Images für Java bereit:

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
21	Java 21	Amazon Linux 2023	Dockerfile für Java 2.1 auf GitHub	
17	Java 17	Amazon Linux 2	Dockerfile für Java 17 auf GitHub	
11	Java 11	Amazon Linux 2	Dockerfile für Java 11 auf GitHub	
8.al2	Java 8	Amazon Linux 2	Dockerfile für Java 8 auf GitHub	

Amazon-ECR-Repository: gallery.ecr.aws/lambda/java

Die Basis-Images für Java 21 und höher basieren auf dem Minimal-Container-Image von Amazon Linux 2023. Frühere Basis-Images verwenden Amazon Linux 2. AL2023 bietet mehrere Vorteile gegenüber Amazon Linux 2, darunter einen geringeren Bereitstellungsaufwand und aktualisierte Versionen von Bibliotheken wie `glibc`.

AL2023-basierte Images verwenden `microdnf` (symbolisiert als`dnf`) als Paketmanager anstelle von`yum`, dem Standard-Paketmanager in Amazon Linux 2. `microdnf`ist eine eigenständige Implementierung von. `dnf` Eine Liste der Pakete, die in AL2023-basierten Images enthalten sind, finden Sie in den Spalten Minimal Container unter Comparing packages installed on Amazon Linux 2023 Container Images. Weitere Informationen zu den Unterschieden zwischen AL2023 und Amazon Linux 2 finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.

> **Note**
>
> Um AL2023-basierte Images lokal auszuführen, auch mit AWS Serverless Application Model (AWS SAM), müssen Sie Docker-Version 20.10.10 oder höher verwenden.

Verwenden Sie ein Basis-Image für Java AWS

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Java (zum Beispiel Amazon Corretto)
- Docker (Mindestversion 20.10.10 für Java 21 und spätere Basis-Images)
- Apache Maven oder Gradle
- AWS Command Line Interface () Version 2 AWS CLI

Erstellen eines Images aus einem Base Image

Maven

1. Führen Sie den folgenden Befehl aus, um ein Maven-Projekt mit dem Archetyp für Lambda zu erstellen. Die folgenden Parameter sind erforderlich:

   - service — Der AWS-Service Client, der in der Lambda-Funktion verwendet werden soll. Eine Liste der verfügbaren Quellen finden Sie unter aws-sdk-java-v2/services on. GitHub
   - region — Der AWS-Region Ort, an dem Sie die Lambda-Funktion erstellen möchten.
   - groupId – Der vollständige Paket-Namespace Ihrer Anwendung.
   - artifactId – Ihr Projektname. Dies wird der Name des Verzeichnisses für Ihr Projekt.

   Führen Sie unter Linux und macOS folgenden Befehl aus:

   ```
   mvn -B archetype:generate \
      -DarchetypeGroupId=software.amazon.awssdk \
      -DarchetypeArtifactId=archetype-lambda -Dservice=s3 -Dregion=US_WEST_2 \
      -DgroupId=com.example.myapp \
      -DartifactId=myapp
   ```

Führen Sie in PowerShell diesen Befehl aus:

```
mvn -B archetype:generate `
   "-DarchetypeGroupId=software.amazon.awssdk" `
   "-DarchetypeArtifactId=archetype-lambda" "-Dservice=s3" "-Dregion=US_WEST_2"
 `
   "-DgroupId=com.example.myapp" `
   "-DartifactId=myapp"
```

Der Maven-Archetyp für Lambda ist für die Kompilierung mit Java SE 8 vorkonfiguriert und enthält eine Abhängigkeit von der AWS SDK for Java. Wenn Sie Ihr Projekt mit einem anderen Archetyp oder mit einer anderen Methode erstellen, müssen Sie den Java-Compiler für Maven konfigurieren und das SDK als Abhängigkeit deklarieren.

2. Öffnen Sie das *myapp*`/src/main/java/com/example/`*myapp*-Verzeichnis, und suchen Sie die `App.java`-Datei. Dies ist der Code für die Lambda-Funktion. Sie können den bereitgestellten Beispielcode zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.
3. Navigieren Sie zurück zum Stammverzeichnis des Projekts und erstellen Sie ein neues Dockerfile mit der folgenden Konfiguration:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

   Example Dockerfile

   ```
   FROM public.ecr.aws/lambda/java:21

   # Copy function code and runtime dependencies from Maven layout
   COPY target/classes ${LAMBDA_TASK_ROOT}
   COPY target/dependency/* ${LAMBDA_TASK_ROOT}/lib/

   # Set the CMD to your handler (could also be done as a parameter override
    outside of the Dockerfile)
   CMD [ "com.example.myapp.App::handleRequest" ]
   ```

4. Kompilieren Sie das Projekt und erfassen Sie die Laufzeitabhängigkeiten.

   ```
   mvn compile dependency:copy-dependencies -DincludeScope=runtime
   ```

5. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

Gradle

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir example
cd example
```

2. Führen Sie den folgenden Befehl aus, um Gradle ein neues Java-Anwendungsprojekt im Verzeichnis `example` der Umgebung generieren zu lassen. Wählen Sie für Select Build Script DSL die Option 2: Groovy aus.

```
gradle init --type java-application
```

3. Öffnen Sie das */example*`/app/src/main/java/`*example*-Verzeichnis, und suchen Sie die `App.java`-Datei. Dies ist der Code für die Lambda-Funktion. Sie können den folgenden Beispielcode zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.

   Example App.java

```
package com.example;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
public class App implements RequestHandler<Object, String> {
    public String handleRequest(Object input, Context context) {
```

```
        return "Hello world!";
    }
}
```

4. Öffnen Sie die `build.gradle` Datei. Wenn Sie den Beispiel-Funktionscode aus dem vorherigen Schritt verwenden, ersetzen Sie den Inhalt von `build.gradle` durch den folgenden. Wenn Sie Ihren eigenen Funktionscode verwenden, ändern Sie Ihre `build.gradle`-Datei nach Bedarf.

   Example build.gradle (Groovy DSL)

```
plugins {
  id 'java'
}
group 'com.example'
version '1.0-SNAPSHOT'
sourceCompatibility = 1.8
repositories {
  mavenCentral()
}
dependencies {
  implementation 'com.amazonaws:aws-lambda-java-core:1.2.1'
}
jar {
  manifest {
      attributes 'Main-Class': 'com.example.App'
  }
}
```

5. Der `gradle init`-Befehl aus Schritt 2 generierte auch einen Dummy-Testfall im `app/test`-Verzeichnis. Überspringen Sie in diesem Tutorial das Ausführen von Tests, indem Sie das `/test`-Verzeichnis löschen.
6. Erstellen Sie das Projekt.

```
gradle build
```

7. Erstellen Sie im Stammverzeichnis (`/example`) des Projekts eine Docker-Datei mit der folgenden Konfiguration:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.

- Verwenden Sie den Befehl COPY, um den Funktionscode und die Laufzeitabhängigkeiten in eine von Lambda definierte Umgebungsvariable zu `{LAMBDA_TASK_ROOT}` kopieren.
- Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

Example Dockerfile

```
FROM public.ecr.aws/lambda/java:21

# Copy function code and runtime dependencies from Gradle layout
COPY app/build/classes/java/main ${LAMBDA_TASK_ROOT}

# Set the CMD to your handler (could also be done as a parameter override
 outside of the Dockerfile)
CMD [ "com.example.App::handleRequest" ]
```

8. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. In diesem Beispiel ist `docker-image` der Image-Name und `test` der Tag.

```
docker run --platform linux/amd64 -p 9000:8080 docker-image:test
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis an den lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
    '{"payload":"hello world!"}'
   ```

   PowerShell

   Führen Sie in PowerShell den folgenden Befehl aus: `Invoke-WebRequest`

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{}' -ContentType "application/json"
   ```

   Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

   ```
   Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
   invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
    "application/json"
   ```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
```

```
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:
   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

   ```
   docker tag docker-image:test <ECRrepositoryUri>:latest
   ```

   Beispiel:

   ```
   docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world:latest
   ```
5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

   ```
   docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
   ```
6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.

7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

Wenn Sie ein OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Laufzeitschnittstellen-Client erweitert die Lambda-Laufzeiten-API, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet.

Installieren Sie den Laufzeitschnittstellen-Client für Java in Ihrem Dockerfile oder als Abhängigkeit in Ihrem Projekt. Um beispielsweise den Laufzeitschnittstellen-Client mit dem Maven-Paketmanager zu installieren, fügen Sie Ihrer `pom.xml`-Datei Folgendes hinzu:

```
<dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
    <version>2.3.2</version>
</dependency>
```

Einzelheiten zum Paket finden Sie unter AWS Lambda Java Runtime Interface Client im Maven-Central-Repository. Sie können den Quellcode des Runtime-Interface-Clients auch im GitHub Repository der AWS Lambda Java Support Libraries überprüfen.

Das folgende Beispiel zeigt, wie Sie mithilfe eines Amazon-Corretto-Images ein Container-Image für Java erstellen. Amazon Corretto ist eine kostenlose, plattformübergreifende und produktionsbereite Distribution des Open Java Development Kit (OpenJDK). Das Maven-Projekt beinhaltet den Laufzeitschnittstellen-Client als Abhängigkeit.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Java (zum Beispiel Amazon Corretto)
- Docker
- Apache Maven
- AWS Command Line Interface (AWS CLI) Version 2

Erstellen eines Images aus einem alternativen Basis-Image

1. Erstellen Sie ein Maven-Projekt. Die folgenden Parameter sind erforderlich:

- groupId – Der vollständige Paket-Namespace Ihrer Anwendung.
- artifactId – Ihr Projektname. Dies wird der Name des Verzeichnisses für Ihr Projekt.

Linux/macOS

```
mvn -B archetype:generate \
   -DarchetypeArtifactId=maven-archetype-quickstart \
   -DgroupId=example \
   -DartifactId=myapp \
   -DinteractiveMode=false
```

PowerShell

```
mvn -B archetype:generate `
   -DarchetypeArtifactId=maven-archetype-quickstart `
   -DgroupId=example `
   -DartifactId=myapp `
   -DinteractiveMode=false
```

2. Öffnen Sie das Projektverzeichnis.

```
cd myapp
```

3. Öffnen Sie die Datei `pom.xml` und ersetzen Sie den Inhalt durch Folgendes. Diese Datei enthält aws-lambda-java-runtime-interface-client als Abhängigkeit. Alternativ können Sie den Laufzeitschnittstellen-Client im Dockerfile installieren. Der einfachste Ansatz besteht jedoch darin, die Bibliothek als Abhängigkeit einbinden.

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>example</groupId>
  <artifactId>hello-lambda</artifactId>
  <packaging>jar</packaging>
  <version>1.0-SNAPSHOT</version>
  <name>hello-lambda</name>
  <url>http://maven.apache.org</url>
  <properties>
```

```
    <maven.compiler.source>1.8</maven.compiler.source>
    <maven.compiler.target>1.8</maven.compiler.target>
  </properties>
  <dependencies>
    <dependency>
      <groupId>com.amazonaws</groupId>
      <artifactId>aws-lambda-java-runtime-interface-client</artifactId>
      <version>2.3.2</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId>
        <artifactId>maven-dependency-plugin</artifactId>
        <version>3.1.2</version>
        <executions>
          <execution>
            <id>copy-dependencies</id>
            <phase>package</phase>
            <goals>
              <goal>copy-dependencies</goal>
            </goals>
          </execution>
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

4. Öffnen Sie das *myapp*`/src/main/java/com/example/`*myapp*-Verzeichnis, und suchen Sie die `App.java`-Datei. Dies ist der Code für die Lambda-Funktion. Ersetzen Sie den Code durch Folgendes:

   Example Funktions-Handler

```
package example;

public class App {
    public static String sayHello() {
        return "Hello world!";
    }
}
```

5. Der `mvn -B archetype:generate`-Befehl aus Schritt 1 generierte auch einen Dummy-Testfall im `src/test`-Verzeichnis. Überspringen Sie in diesem Tutorial das Ausführen von Tests, indem Sie das gesamte generierte Verzeichnis `/test` löschen.
6. Navigieren Sie zurück zum Stammverzeichnis des Projekts und erstellen Sie dann ein neues Dockerfile. Das folgende Beispiel-Dockerfile verwendet ein Amazon-Corretto-Image. Amazon Corretto ist eine kostenlose, plattformübergreifende und produktionsbereite Distribution des OpenJDK.

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images.
   - Legen Sie `ENTRYPOINT` auf das Modul fest, das der Docker-Container beim Start ausführen soll. In diesem Fall ist das Modul der Laufzeitschnittstellen-Client.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest.

   Example Dockerfile

```
FROM public.ecr.aws/amazoncorretto/amazoncorretto:21 as base

# Configure the build environment
FROM base as build
RUN yum install -y maven
WORKDIR /src

# Cache and copy dependencies
ADD pom.xml .
RUN mvn dependency:go-offline dependency:copy-dependencies

# Compile the function
ADD . .
RUN mvn package

# Copy the function artifact and dependencies onto a clean base
FROM base
WORKDIR /function

COPY --from=build /src/target/dependency/*.jar ./
COPY --from=build /src/target/*.jar ./

# Set runtime interface client as default command for the container runtime
ENTRYPOINT [ "/usr/bin/java", "-cp", "./*",
 "com.amazonaws.services.lambda.runtime.api.client.AWSLambda" ]
```

```
# Pass the name of the function handler as an argument to the runtime
CMD [ "example.App::sayHello" ]
```

7. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um das Image lokal zu testen. Sie können den Emulator in Ihr Image einbauen oder ihn mit dem folgenden Verfahren auf Ihrem lokalen Computer installieren.

Installieren des Laufzeitschnittstellen-Emulators auf Ihrem lokalen Computer

1. Führen Sie in Ihrem Projektverzeichnis den folgenden Befehl aus, um den Runtime-Interface-Emulator (x86-64-Architektur) herunterzuladen GitHub und auf Ihrem lokalen Computer zu installieren.

   Linux/macOS

```
mkdir -p ~/.aws-lambda-rie && \
    curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
    chmod +x ~/.aws-lambda-rie/aws-lambda-rie
```

   Um den arm64-Emulator zu installieren, ersetzen Sie die GitHub Repository-URL im vorherigen Befehl durch Folgendes:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

PowerShell

```
$dirPath = "$HOME\.aws-lambda-rie"
if (-not (Test-Path $dirPath)) {
    New-Item -Path $dirPath -ItemType Directory
}

$downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/
releases/latest/download/aws-lambda-rie"
$destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
```

Um den arm64-Emulator zu installieren, ersetzen Sie das `$downloadLink` durch Folgendes:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.
   - `/usr/bin/java -cp './*' com.amazonaws.services.lambda.runtime.api.client.AWSLambda example.App::sayHello` ist der `ENTRYPOINT` gefolgt von dem `CMD` aus Ihrem Dockerfile.

   Linux/macOS

```
docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
 9000:8080 \
    --entrypoint /aws-lambda/aws-lambda-rie \
    docker-image:test \
        /usr/bin/java -cp './*'
 com.amazonaws.services.lambda.runtime.api.client.AWSLambda
 example.App::sayHello
```

PowerShell

```
docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
 9000:8080 `
--entrypoint /aws-lambda/aws-lambda-rie `
docker-image:test `
    /usr/bin/java -cp './*'
 com.amazonaws.services.lambda.runtime.api.client.AWSLambda
 example.App::sayHello
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

> **Note**
>
> Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

3. Veröffentlichen Sie ein Ereignis auf dem lokalen Endpunkt.

Linux/macOS

Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Die Container-ID erhalten.

```
docker ps
```

5. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.
   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
```

```
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Arbeiten mit Ebenen für Java-Lambda-Funktionen

Eine Lambda-Schicht ist ein ZIP-Dateiarchiv, das zusätzlichen Code oder Daten enthält. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien. Das Erstellen einer Ebene umfasst drei allgemeine Schritte:

1. Package Sie Ihren Layer-Inhalt. Das bedeutet, dass Sie ein ZIP-Dateiarchiv erstellen müssen, das die Abhängigkeiten enthält, die Sie in Ihren Funktionen verwenden möchten.
2. Erstellen Sie die Ebene in Lambda.
3. Fügen Sie die Ebene zu Ihren Funktionen hinzu.

Dieses Thema enthält Schritte und Anleitungen zum ordnungsgemäßen Verpacken und Erstellen einer Java-Lambda-Schicht mit externen Bibliotheksabhängigkeiten.

Themen

Voraussetzungen

Um die Schritte in diesem Abschnitt ausführen zu können, benötigen Sie Folgendes:

- Java 21
- Apache Maven 3.8.6 oder höher
- AWS Command Line Interface (AWS CLI) Version 2

> **Note**
>
> Stellen Sie sicher, dass die Java-Version, auf die sich Maven bezieht, mit der Java-Version der Funktion übereinstimmt, die Sie bereitstellen möchten. Für eine Java 21-Funktion sollte der `mvn -v` Befehl beispielsweise die Java-Version 21 in der Ausgabe auflisten:

```
Apache Maven 3.8.6
...
Java version: 21.0.2, vendor: Oracle Corporation, runtime: /Library/Java/
JavaVirtualMachines/jdk-21.jdk/Contents/Home
...
```

In diesem Thema verweisen wir auf die `layer-java`Beispielanwendung im awsdocs-Repository GitHub . Diese Anwendung enthält Skripte, die die Abhängigkeiten herunterladen und die Ebene generieren. Die Anwendung enthält auch eine entsprechende Funktion, die Abhängigkeiten aus der Ebene verwendet. Nachdem Sie eine Ebene erstellt haben, können Sie die entsprechende Funktion bereitstellen und aufrufen, um zu überprüfen, ob alles ordnungsgemäß funktioniert. Da Sie die Java 21-Runtime für die Funktionen verwenden, müssen die Ebenen auch mit Java 21 kompatibel sein.

Die `layer-java` Beispielanwendung enthält ein einzelnes Beispiel in zwei Unterverzeichnissen. Das `layer` Verzeichnis enthält eine `pom.xml` Datei, die die Layer-Abhängigkeiten definiert, sowie Skripts zur Generierung der Ebene. Das `function` Verzeichnis enthält eine Beispielfunktion, mit deren Hilfe getestet werden kann, ob der Layer funktioniert. In diesem Tutorial wird beschrieben, wie Sie diesen Layer erstellen und verpacken.

Java-Layer-Kompatibilität mit Amazon Linux

Der erste Schritt beim Erstellen einer Ebene besteht darin, den gesamten Ebeneninhalt in einem ZIP-Dateiarchiv zu bündeln. Da Lambda-Funktionen unter Amazon Linux ausgeführt werden, muss Ihr Ebeneninhalt in einer Linux-Umgebung kompiliert und erstellt werden können.

Java-Code ist plattformunabhängig konzipiert, sodass Sie Ihre Ebenen auf Ihrem lokalen Computer packen können, auch wenn dieser keine Linux-Umgebung verwendet. Nachdem Sie den Java-Layer auf Lambda hochgeladen haben, ist er weiterhin mit Amazon Linux kompatibel.

Layer-Pfade für Java-Laufzeiten

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Layer-Inhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

- `java/lib`

Die resultierende Layer-ZIP-Datei, die Sie in diesem Tutorial erstellen, hat beispielsweise die folgende Verzeichnisstruktur:

```
layer_content.zip
# java
    # lib
        # layer-java-layer-1.0-SNAPSHOT.jar
```

Die `layer-java-layer-1.0-SNAPSHOT.jar` JAR-Datei (eine Uber-JAR-Datei, die alle unsere erforderlichen Abhängigkeiten enthält) befindet sich korrekt im Verzeichnis. `java/lib` Dadurch wird sichergestellt, dass Lambda die Bibliothek bei Funktionsaufrufen finden kann.

Verpacken des Layer-Inhalts

In diesem Beispiel packen Sie die folgenden zwei Java-Bibliotheken in eine einzige JAR-Datei:

- aws-lambda-java-core— Ein minimaler Satz von Schnittstellendefinitionen für die Arbeit mit Java in AWS Lambda
- Jackson — Eine beliebte Suite von Datenverarbeitungstools, insbesondere für die Arbeit mit JSON.

Gehen Sie wie folgt vor, um den Layer-Inhalt zu installieren und zu verpacken.

So installieren und verpacken Sie Ihre Layer-Inhalte

1. Klonen Sie das `aws-lambda-developer-guide` GitHub Repo, das den Beispielcode enthält, den Sie im `sample-apps/layer-java` Verzeichnis benötigen.

   ```
   git clone https://github.com/awsdocs/aws-lambda-developer-guide.git
   ```

2. Navigieren Sie zum `layer` Verzeichnis der `layer-java` Beispiel-App. Dieses Verzeichnis enthält die Skripts, die Sie verwenden, um den Layer ordnungsgemäß zu erstellen und zu verpacken.

   ```
   cd aws-lambda-developer-guide/sample-apps/layer-java/layer
   ```

3. Untersuchen Sie die `pom.xml`Datei. In `<dependencies>` diesem Abschnitt definieren Sie die Abhängigkeiten, die Sie in die Ebene aufnehmen möchten, nämlich die `jackson-databind`

Bibliotheken `aws-lambda-java-core` und. Sie können diese Datei so aktualisieren, dass sie alle Abhängigkeiten enthält, die Sie in Ihre eigene Ebene aufnehmen möchten.

Example pom.xml

```
<dependencies>
    <dependency>
        <groupId>com.amazonaws</groupId>
        <artifactId>aws-lambda-java-core</artifactId>
        <version>1.2.3</version>
    </dependency>

    <dependency>
        <groupId>com.fasterxml.jackson.core</groupId>
        <artifactId>jackson-databind</artifactId>
        <version>2.17.0</version>
    </dependency>
</dependencies>
```

> **Note**
>
> Der `<build>` Abschnitt dieser `pom.xml` Datei enthält zwei Plugins. Das maven-compiler-pluginkompiliert den Quellcode. Das maven-shade-pluginpackt deine Artefakte in ein einziges Uber-Jar.

4. Stellen Sie sicher, dass Sie berechtigt sind, beide Skripts auszuführen.

```
chmod 744 1-install.sh && chmod 744 2-package.sh
```

5. Führen Sie das `1-install.sh`Skript mit dem folgenden Befehl aus:

```
./1-install.sh
```

Dieses Skript wird `mvn clean install` im aktuellen Verzeichnis ausgeführt. Dadurch wird das Uber-Jar mit allen erforderlichen Abhängigkeiten im `target/` Verzeichnis erstellt.

Example 1-install.sh

```
mvn clean install
```

6. Führen Sie das `2-package.sh`Skript mit dem folgenden Befehl aus:

```
./2-package.sh
```

Dieses Skript erstellt die `java/lib` Verzeichnisstruktur, die Sie benötigen, um Ihren Layer-Inhalt ordnungsgemäß zu verpacken. Anschließend kopiert es die Uber-Jar-Datei aus dem `/target` Verzeichnis in das neu erstellte `java/lib` Verzeichnis. Schließlich komprimiert das Skript den Inhalt des `java` Verzeichnisses in eine Datei mit dem Namen. `layer_content.zip` Dies ist die ZIP-Datei für Ihren Layer. Sie können die Datei entpacken und überprüfen, ob sie die richtige Dateistruktur enthält, wie im the section called “Layer-Pfade für Java-Laufzeiten” Abschnitt gezeigt.

Example 2-package.sh

```
mkdir java
mkdir java/lib
cp -r target/layer-java-layer-1.0-SNAPSHOT.jar java/lib/
zip -r layer_content.zip java
```

Die Ebene erstellen

In diesem Abschnitt nehmen Sie die `layer_content.zip` Datei, die Sie im vorherigen Abschnitt generiert haben, und laden sie als Lambda-Schicht hoch. Sie können eine Ebene mit der AWS Management Console oder der Lambda-API über die AWS Command Line Interface (AWS CLI) hochladen. Wenn Sie Ihre Layer-.zip-Datei hochladen, geben Sie `java21` im folgenden PublishLayerVersion AWS CLI Befehl die kompatible Laufzeit und die kompatible `arm64` Architektur an.

```
aws lambda publish-layer-version --layer-name java-jackson-layer \
    --zip-file fileb://layer_content.zip \
    --compatible-runtimes java21 \
    --compatible-architectures "arm64"
```

Notieren Sie sich aus der Antwort den`LayerVersionArn`, der wie `arn:aws:lambda:us-east-1:`*`123456789012`*`:layer:java-jackson-layer:1` aussieht. Sie benötigen diesen Amazon-Ressourcennamen (ARN) im nächsten Schritt dieses Tutorials, wenn Sie den Layer zu Ihrer Funktion hinzufügen.

Hinzufügen der Ebene zu Ihrer Funktion

In diesem Abschnitt stellen Sie eine Lambda-Beispielfunktion bereit, die die Jackson-Bibliothek in ihrem Funktionscode verwendet, und fügen dann den Layer hinzu. Um die Funktion bereitzustellen, benötigen Sie einethe section called “Ausführungsrolle (Berechtigungen für Funktionen zum Zugriff auf andere Ressourcen)”. Wenn Sie noch keine Ausführungsrolle haben, folgen Sie den Schritten im Abschnitt „Zusammenklappbar“. Fahren Sie andernfalls mit dem nächsten Abschnitt fort, um die Funktion bereitzustellen.

(Optional) Erstellen Sie eine Ausführungsrolle

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Erstellen Sie eine Rolle mit den folgenden Eigenschaften.

   - Trusted entity (Vertrauenswürdige Entität) – Lambda.
   - Berechtigungen — AWSLambdaBasicExecutionRole.
   - Role name (Name der Rolle – **`lambda-role`**.

   Die AWSLambdaBasicExecutionRoleRichtlinie verfügt über die Berechtigungen, die die Funktion benötigt, um Protokolle in Logs zu CloudWatch schreiben.

So stellen Sie die Lambda-Funktion bereit

1. Navigieren Sie zum `function/` Verzeichnis . Wenn Sie sich derzeit in dem `layer/` Verzeichnis befinden, führen Sie den folgenden Befehl aus:

   ```
   cd ../function
   ```

2. Überprüfen Sie den Funktionscode. Die Funktion nimmt eine `Map<String, String>` als Eingabe auf und verwendet Jackson, um die Eingabe als JSON-Zeichenfolge zu schreiben, bevor sie in ein vordefiniertes F1Car-Java-Objekt konvertiert wird. Schließlich verwendet die Funktion Felder aus dem F1Car-Objekt, um einen String zu erstellen, den die Funktion zurückgibt.

   ```
   package example;
   ```

```
import com.amazonaws.services.lambda.runtime.Context;
import com.fasterxml.jackson.databind.ObjectMapper;

import java.io.IOException;
import java.util.Map;

public class Handler {

    public String handleRequest(Map<String, String> input, Context context) throws
 IOException {
        // Parse the input JSON
        ObjectMapper objectMapper = new ObjectMapper();
        F1Car f1Car =
 objectMapper.readValue(objectMapper.writeValueAsString(input), F1Car.class);

        StringBuilder finalString = new StringBuilder();
        finalString.append(f1Car.getDriver());
        finalString.append(" is a driver for team ");
        finalString.append(f1Car.getTeam());
        return finalString.toString();
    }
}
```

3. Erstellen Sie das Projekt mit dem folgenden Maven-Befehl:

```
mvn package
```

Dieser Befehl erzeugt eine JAR-Datei in dem `target/` Verzeichnis mit dem Namen`layer-java-function-1.0-SNAPSHOT.jar`.

4. Stellen Sie die Funktion bereit. Ersetzen Sie im folgenden AWS CLI Befehl den `--role` Parameter durch den ARN Ihrer Ausführungsrolle:

```
aws lambda create-function --function-name java_function_with_layer \
    --runtime java21 \
    --architectures "arm64" \
    --handler example.Handler::handleRequest \
    --timeout 30 \
    --role arn:aws:iam::123456789012:role/lambda-role \
    --zip-file fileb://target/layer-java-function-1.0-SNAPSHOT.jar
```

(Optional) Rufen Sie Ihre Funktion auf, ohne eine Ebene anzuhängen

An dieser Stelle können Sie optional versuchen, Ihre Funktion aufzurufen, bevor Sie den Layer anhängen. Wenn Sie dies versuchen, sollten Sie eine erhalten, `ClassNotFoundException` da Ihre Funktion nicht auf das `requests` Paket verweisen kann. Verwenden Sie den folgenden AWS CLI Befehl, um Ihre Funktion aufzurufen:

```
aws lambda invoke --function-name java_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "driver": "Max Verstappen", "team": "Red Bull" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "StatusCode": 200,
    "FunctionError": "Unhandled",
    "ExecutedVersion": "$LATEST"
}
```

Um den spezifischen Fehler anzuzeigen, öffnen Sie die `response.json` Ausgabedatei. Sie sollten eine `ClassNotFoundException` mit der folgenden Fehlermeldung sehen:

```
"errorMessage":"com.fasterxml.jackson.databind.ObjectMapper","errorType":"java.lang.ClassNotFou
```

Als Nächstes fügen Sie die Ebene Ihrer Funktion hinzu. Ersetzen Sie im folgenden AWS CLI Befehl den `--layers` Parameter durch den ARN der Layer-Version, den Sie zuvor notiert haben:

```
aws lambda update-function-configuration --function-name java_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --layers "arn:aws:lambda:us-east-1:123456789012:layer:java-jackson-layer:1"
```

Versuchen Sie abschließend, Ihre Funktion mit dem folgenden AWS CLI Befehl aufzurufen:

```
aws lambda invoke --function-name java_function_with_layer \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "driver": "Max Verstappen", "team": "Red Bull" }' response.json
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
```

```
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

Dies deutet darauf hin, dass die Funktion die Jackson-Abhängigkeit verwenden konnte, um die Funktion ordnungsgemäß auszuführen. Sie können überprüfen, ob die `response.json` Ausgabedatei den richtigen zurückgegebenen String enthält:

```
"Max Verstappen is a driver for team Red Bull"
```

(Optional) Bereinigen Sie Ihre Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

Um die Lambda-Ebene zu löschen

1. Öffnen Sie die Seite Ebenen der Lambda-Konsole.
2. Wählen Sie die Ebene aus, die Sie erstellt haben.
3. Wählen Sie „Löschen“ und anschließend erneut „Löschen“.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

Verbesserung der Startleistung mit Lambda SnapStart

Lambda SnapStart für Java kann die Startleistung latenzempfindlicher Anwendungen ohne zusätzliche Kosten um das bis zu 10-fache verbessern, in der Regel ohne Änderungen an Ihrem Funktionscode. Der größte Beitrag zur Startup-Latenz (oft als Kaltstartzeit bezeichnet) ist die Zeit, die Lambda für die Initialisierung der Funktion aufwendet. Dazu gehören das Laden des Funktionscodes, der Start der Laufzeit und die Initialisierung des Funktionscodes.

Mit initialisiert Lambda Ihre Funktion SnapStart, wenn Sie eine Funktionsversion veröffentlichen. Lambda erstellt einen Firecracker-microVM-Snapshot des Arbeitsspeichers und des Festplattenstatus der initialisierten Ausführungsumgebung, verschlüsselt den Snapshot und speichert ihn im Cache für den Zugriff mit geringer Latenz. Wenn Sie die Funktionsversion zum ersten Mal aufrufen und wenn die Aufrufe hochskalieren, nimmt Lambda neue Ausführungsumgebungen aus dem im Cache gespeicherten Snapshot wieder auf, anstatt sie von Grund auf neu zu initialisieren, wodurch die Startup-Latenz verbessert wird.

> **Important**
>
> Wenn Ihre Anwendungen von der Eindeutigkeit des Zustands abhängen, müssen Sie Ihren Funktionscode auswerten und sicherstellen, dass er gegenüber Snapshot-Vorgängen widerstandsfähig ist. Weitere Informationen finden Sie unter Umgang mit Eindeutigkeit mit Lambda SnapStart.

Themen

- Sicherheitsmodell für Lambda SnapStart
- Maximieren Sie die Lambda-Leistung SnapStart

Unterstützte Funktionen und Einschränkungen

SnapStart unterstützt Java 11 und neuere Java-verwaltete Laufzeiten. Andere verwaltete Laufzeiten (wie `nodejs20.x` und `python3.12`), Reine OS-Laufzeiten und Container-Images werden nicht unterstützt.

SnapStart unterstützt keine bereitgestellte Parallelität, die arm64-Architektur, Amazon Elastic File System (Amazon EFS) oder kurzlebigen Speicher mit mehr als 512 MB.

Um damit zu arbeiten SnapStart, können Sie die Lambda-Konsole, die AWS Command Line Interface (AWS CLI), die Lambda-API, die, AWS SDK for Java AWS CloudFormation, AWS Serverless Application Model (AWS SAM) und verwenden. AWS Cloud Development Kit (AWS CDK) Weitere Informationen finden Sie unter Aktivieren und Verwalten von Lambda SnapStart.

> **Note**
>
> Sie können sie SnapStart nur für veröffentlichte Funktionsversionen und Aliase verwenden, die auf Versionen verweisen. Sie können es nicht für die unveröffentlichte Version einer Funktion ($LATEST) verwenden SnapStart .

Unterstützte Regionen

SnapStart ist in den folgenden Versionen verfügbar: AWS-Regionen

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asien-Pazifik (Mumbai)

- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Tokio)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Kanada (Zentral)
- Europa (Stockholm)
- Europa (Frankfurt)
- Europa (Zürich)
- Europa (Irland)
- Europe (London)
- Europa (Paris)
- Europa (Milan)
- Europa (Spain)
- Naher Osten (VAE)
- Naher Osten (Bahrain)
- Südamerika (São Paulo)

Erwägungen zur Kompatibilität

Mit SnapStart verwendet Lambda einen einzelnen Snapshot als Ausgangszustand für mehrere Ausführungsumgebungen. Wenn Ihre Funktion während der Initialisierungsphase eines der folgenden Elemente verwendet, müssen Sie vor der Verwendung möglicherweise einige Änderungen vornehmen: SnapStart

Eindeutigkeit

Wenn Ihr Initialisierungscode eindeutigen Inhalt generiert, der im Snapshot enthalten ist, ist der Inhalt möglicherweise nicht eindeutig, wenn er in Ausführungsumgebungen wiederverwendet

wird. Um die Einzigartigkeit bei der Verwendung zu wahren SnapStart, müssen Sie nach der Initialisierung eindeutige Inhalte generieren. Dazu gehören eindeutige IDs, eindeutige Geheimnisse und Entropie, die zum Generieren von Pseudozufälligkeiten verwendet wird. Informationen zum Wiederherstellen von Eindeutigkeit finden Sie unter Umgang mit Eindeutigkeit mit Lambda SnapStart.

Netzwerkverbindungen

Der Zustand der Verbindungen, die Ihre Funktion während der Initialisierungsphase herstellt, ist nicht garantiert, wenn Lambda Ihre Funktion von einem Snapshot fortsetzt. Überprüfen Sie den Status Ihrer Netzwerkverbindungen und stellen Sie diese bei Bedarf wieder her. In den meisten Fällen werden Netzwerkverbindungen, die ein AWS SDK herstellt, automatisch wieder aufgenommen. Für andere Verbindungen lesen Sie die bewährten Methoden.

Temporäre Daten

Einige Funktionen laden während der Initialisierungsphase kurzlebige Daten herunter oder initialisieren diese, wie etwa temporäre Anmeldeinformationen oder im Cache gespeicherte Zeitstempel. Aktualisieren Sie kurzlebige Daten im Funktionshandler, bevor Sie sie verwenden, auch wenn Sie sie nicht verwenden. SnapStart

SnapStart Preisgestaltung

Es fallen keine zusätzlichen Kosten für an SnapStart. Die Abrechnung erfolgt basierend auf der Anzahl der Anfragen für Ihre Funktionen, der Zeit, die Ihr Code zum Ausführen benötigt, und dem für Ihre Funktion konfigurierten Arbeitsspeicher. Die Dauer wird vom Beginn der Ausführung Ihres Codes bis zur Rückgabe oder einem anderen Ende berechnet, aufgerundet auf die nächste 1 ms.

Die Gebühren für die Dauer gelten für Code, der im Funktions-Handler ausgeführt wird, Initialisierungscode, der außerhalb des Handlers deklariert ist, die Zeit, die zum Laden der Laufzeit (JVM) benötigt wird, und Code, der in einem Laufzeit-Hook ausgeführt wird. Weitere Informationen zur Berechnung von Gebühren durch Lambda finden Sie unter Überwachung für Lambda SnapStart.

Für Funktionen, die mit konfiguriert sind SnapStart, recycelt Lambda regelmäßig die Ausführungsumgebungen und führt Ihren Initialisierungscode erneut aus. Um die Ausfallsicherheit zu gewährleisten, erstellt Lambda Snapshots in mehreren Availability Zones. Jedes Mal, wenn Lambda Ihren Initialisierungscode in einer anderen Availability Zone erneut ausführt, fallen Gebühren an. Weitere Informationen zur Berechnung von Gebühren durch Lambda finden Sie unter AWS Lambda - Preise.

Vergleich von Lambda SnapStart und bereitgestellter Parallelität

Sowohl Lambda als auch bereitgestellte Parallelität können Kaltstarts SnapStart und Latenzen bei Ausreißern reduzieren, wenn eine Funktion skaliert wird. SnapStart hilft Ihnen dabei, die Startleistung ohne zusätzliche Kosten um das bis zu 10-fache zu verbessern. Die bereitgestellte Gleichzeitigkeit sorgt dafür, dass die Funktionen im zweistelligen Millisekundenbereich initialisiert und reaktionsbereit sind. Für die Konfiguration der bereitgestellten Parallelität fallen Gebühren für Sie an. AWS-Konto Verwenden Sie die bereitgestellte Gleichzeitigkeit, wenn Ihre Anwendung strenge Anforderungen an die Kaltstartlatenz hat. Sie können nicht beide SnapStart und die bereitgestellte Parallelität auf derselben Funktionsversion verwenden.

> **Note**
>
> SnapStart funktioniert am besten, wenn es mit Funktionsaufrufen in großem Maßstab verwendet wird. Funktionen, die selten aufgerufen werden, weisen möglicherweise nicht dieselben Leistungsverbesserungen auf.

Weitere Ressourcen

Zusätzlich zur Lektüre der anderen Themen in diesem Kapitel empfehlen wir Ihnen auch, den AWS Lambda SnapStart Workshop Schneller starten mit zu testen und sich die Sitzung Schnelle Kaltstarts für Ihre Java-Funktionen aus AWS re:Invent 2022 anzusehen.

Aktivieren und Verwalten von Lambda SnapStart

Um zu verwenden SnapStart, aktivieren Sie SnapStart für eine neue oder vorhandene Lambda-Funktion. Veröffentlichen und rufen Sie dann eine Funktionsversion auf.

Themen

Aktivieren von SnapStart (Konsole)

So aktivieren Sie SnapStart für eine Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann General configuration (Allgemeine Konfiguration).
4. Wählen Sie im Bereich General configuration (Allgemeine Konfiguration) die Option Edit (Bearbeiten) aus.
5. Wählen Sie auf der Seite Grundlegende Einstellungen bearbeiten für die SnapStartOption Veröffentlichte Versionen aus.
6. Wählen Sie Speichern.
7. Veröffentlichen einer Funktionsversion. Lambda initialisiert Ihren Code, erstellt einen Snapshot der initialisierten Ausführungsumgebung und speichert den Snapshot im Cache für einen Zugriff mit geringer Latenz.
8. Rufen Sie die Funktionsversion auf.

Aktivieren von SnapStart (AWS CLI)

So aktivieren Sie SnapStart für eine vorhandene Funktion

1. Aktualisieren Sie die Funktionskonfiguration, indem Sie den update-function-configuration Befehl mit der --snap-start Option ausführen.

```
aws lambda update-function-configuration \
  --function-name my-function \
  --snap-start ApplyOn=PublishedVersions
```

2. Veröffentlichen Sie eine Funktionsversion mit dem publish-version-Befehl.

```
aws lambda publish-version \
  --function-name my-function
```

3. Bestätigen Sie, dass für die Funktionsversion aktiviert SnapStart ist, indem Sie den get-function-configuration Befehl ausführen und die Versionsnummer angeben. Das folgende Beispiel legt Version 1 fest.

```
aws lambda get-function-configuration \
  --function-name my-function:1
```

   Wenn die Antwort zeigt, dass OptimizationStatus ist On und Status ist`Active`, dann SnapStart ist aktiviert und ein Snapshot ist für die angegebene Funktionsversion verfügbar.

```
"SnapStart": {
    "ApplyOn": "PublishedVersions",
    "OptimizationStatus": "On"
 },
 "State": "Active",
```

4. Rufen Sie die Funktionsversion auf, indem Sie den Aufruf-Befehl ausführen und die Version angeben. Das folgende Beispiel ruft Version 1 auf.

```
aws lambda invoke \
  --cli-binary-format raw-in-base64-out \
  --function-name my-function:1 \
  --payload '{ "name": "Bob" }' \
  response.json
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

So aktivieren Sie SnapStart , wenn Sie eine neue Funktion erstellen

1. Erstellen Sie eine Funktion, indem Sie den create-function-Befehl mit der --snap-start-Option ausführen. Geben Sie für --role den Amazon-Ressourcennamen (ARN) Ihrer Ausführungsrolle an.

```
aws lambda create-function \
  --function-name my-function \
  --runtime "java21" \
  --zip-file fileb://my-function.zip \
  --handler my-function.handler \
  --role arn:aws:iam::111122223333:role/lambda-ex \
  --snap-start ApplyOn=PublishedVersions
```

2. Erstellen Sie eine Version mit dem publish-version-Befehl.

```
aws lambda publish-version \
  --function-name my-function
```

3. Bestätigen Sie, dass für die Funktionsversion aktiviert SnapStart ist, indem Sie den get-function-configuration Befehl ausführen und die Versionsnummer angeben. Das folgende Beispiel legt Version 1 fest.

```
aws lambda get-function-configuration \
  --function-name my-function:1
```

Wenn die Antwort zeigt, dass OptimizationStatus ist On und Status ist`Active`, dann SnapStart ist aktiviert und ein Snapshot ist für die angegebene Funktionsversion verfügbar.

```
"SnapStart": {
     "ApplyOn": "PublishedVersions",
     "OptimizationStatus": "On"
  },
```

```
  "State": "Active",
```

4. Rufen Sie die Funktionsversion auf, indem Sie den Aufruf-Befehl ausführen und die Version angeben. Das folgende Beispiel ruft Version 1 auf.

```
aws lambda invoke \
  --cli-binary-format raw-in-base64-out \
  --function-name my-function:1 \
  --payload '{ "name": "Bob" }' \
  response.json
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Aktivieren von SnapStart (API)

So aktivieren Sie SnapStart

1. Führen Sie eine der folgenden Aktionen aus:
   - Erstellen Sie eine neue Funktion mit SnapStart aktivierter , indem Sie die CreateFunction -API-Aktion mit dem -SnapStartParameter verwenden.
   - Aktivieren Sie SnapStart für eine vorhandene Funktion, indem Sie die -UpdateFunctionConfigurationAktion mit dem -SnapStartParameter verwenden.
2. Veröffentlichen Sie eine Funktionsversion mit der -PublishVersionAktion. Lambda initialisiert Ihren Code, erstellt einen Snapshot der initialisierten Ausführungsumgebung und speichert den Snapshot im Cache für einen Zugriff mit geringer Latenz.
3. Bestätigen Sie, dass für die Funktionsversion aktiviert SnapStart ist, indem Sie die GetFunctionConfiguration Aktion verwenden. Geben Sie eine Versionsnummer an, um zu bestätigen, dass für diese Version aktiviert SnapStart ist. Wenn die Antwort zeigt, dass OptimizationStatus ist 0n und Status ist`Active`, dann SnapStart ist aktiviert und ein Snapshot ist für die angegebene Funktionsversion verfügbar.

```
"SnapStart": {
        "ApplyOn": "PublishedVersions",
```

```
        "OptimizationStatus": "On"
    },
    "State": "Active",
```

4. Rufen Sie die Funktionsversion mit der Aufruf-Aktion auf.

Lambda- SnapStart und -Funktionsstatus

Die folgenden Funktionszustände können auftreten, wenn Sie verwenden SnapStart. Sie können auch auftreten, wenn Lambda die Ausführungsumgebung regelmäßig recycelt und den Initialisierungscode für eine Funktion erneut ausführt, die mit konfiguriert ist SnapStart.

- `Pending` – Lambda initialisiert Ihren Code und erstellt einen Snapshot der initialisierten Ausführungsumgebung. Alle Aufrufe oder andere API-Aktionen, die auf der Funktionsversion ausgeführt werden, schlagen fehl.
- `Active` – Die Snapshot-Erstellung ist abgeschlossen und Sie können die Funktion aufrufen. Um zu verwenden SnapStart, müssen Sie die veröffentlichte Funktionsversion aufrufen, nicht die unveröffentlichte Version ($LATEST).
- `Inactive` – Die Funktionsversion wurde seit 14 Tagen nicht aufgerufen. Wenn die Funktionsversion `Inactive` wird, löscht Lambda den Snapshot. Wenn Sie die Funktionsversion nach 14 Tagen aufrufen, gibt Lambda eine `SnapStartNotReadyException`-Antwort zurück und beginnt mit der Initialisierung eines neuen Snapshots. Warten Sie, bis die Funktionsversion den `Active`-Status erreicht hat, und rufen Sie es dann erneut auf.
- `Failed` – Lambda hat beim Ausführen des Initialisierungscodes oder beim Erstellen des Snapshots einen Fehler festgestellt.

Aktualisieren eines Snapshots

Lambda erstellt für jede veröffentlichte Funktionsversion einen Snapshot. Um einen Snapshot zu aktualisieren, veröffentlichen Sie eine neue Funktionsversion. Lambda aktualisiert Ihre Snapshots automatisch mit den neuesten Laufzeit- und Sicherheits-Patches.

Verwenden von SnapStart mit der AWS SDK for Java

Um AWS-SDK-Aufrufe von Ihrer Funktion aus zu tätigen, generiert Lambda einen ephemeren Satz von Anmeldeinformationen, indem es die Ausführungsrolle Ihrer Funktion übernimmt. Diese Anmeldeinformationen sind während des Aufrufs Ihrer Funktion als Umgebungsvariablen

verfügbar. Sie müssen keine Anmeldeinformationen für das SDK direkt im Code bereitstellen. Standardmäßig überprüft die Kette der Anbieter von Anmeldeinformationen nacheinander jeden Ort, an dem Sie Anmeldeinformationen festlegen können, und wählt die erste verfügbare aus – in der Regel die Umgebungsvariablen (`AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` und `AWS_SESSION_TOKEN`).

> **Note**
>
> Wenn aktiviert SnapStart ist, verwendet die Java-Laufzeit automatisch die Container-Anmeldeinformationen (`AWS_CONTAINER_CREDENTIALS_FULL_URI` und `AWS_CONTAINER_AUTHORIZATION_TOKEN`) anstelle der Umgebungsvariablen des Zugriffsschlüssels. Dadurch wird verhindert, dass Anmeldeinformationen ablaufen, bevor die Funktion wiederhergestellt wird.

Verwenden von SnapStart mit AWS CloudFormationAWS SAM, und AWS CDK

- AWS CloudFormation: Deklarieren Sie die SnapStart Entität in Ihrer Vorlage.
- AWS Serverless Application Model (AWS SAM): Deklarieren Sie die -SnapStartEigenschaft in Ihrer Vorlage.
- AWS Cloud Development Kit (AWS CDK): Verwenden Sie den -SnapStartPropertyTyp.

Löschen von Snapshots

Lambda löscht Snapshots, wenn:

- Sie die Funktion oder Funktionsversion löschen.
- Sie die Funktionsversion 14 Tage lang nicht aufrufen. Wenn nach 14 Tagen ohne Aufruf die Funktionsversion in den Status Inaktiv übergeht. Wenn Sie die Funktionsversion nach 14 Tagen aufrufen, gibt Lambda eine `SnapStartNotReadyException`-Antwort zurück und beginnt mit der Initialisierung eines neuen Snapshots. Warten Sie, bis die Funktionsversion den Status Aktiv erreicht hat, und rufen Sie es dann erneut auf.

Lambda entfernt alle Ressourcen, die mit gelöschten Snapshots verknüpft sind, gemäß der Allgemeinen Datenschutzverordnung (DSGVO).

Umgang mit Eindeutigkeit mit Lambda SnapStart

Wenn Aufrufe für eine SnapStart Funktion hochskaliert werden, verwendet Lambda einen einzelnen initialisierten Snapshot, um mehrere Ausführungsumgebungen fortzusetzen. Wenn Ihr Initialisierungscode eindeutigen Inhalt generiert, der im Snapshot enthalten ist, ist der Inhalt möglicherweise nicht eindeutig, wenn er in Ausführungsumgebungen wiederverwendet wird. Um die Eindeutigkeit bei der Verwendung von zu wahren SnapStart, müssen Sie nach der Initialisierung eindeutige Inhalte generieren. Dazu gehören eindeutige IDs, eindeutige Geheimnisse und Entropie, die zum Generieren von Pseudozufälligkeiten verwendet wird.

Im Folgenden finden Sie einige bewährte Methoden für die Aufrechterhaltung der Eindeutigkeit Ihres Codes. Lambda bietet auch ein Open-Source-SnapStart Scan-Tool, um nach Code zu suchen, der Eindeutigkeit voraussetzt. Wenn Sie während der Initialisierungsphase eindeutige Daten generieren, können Sie eine Laufzeit-Hook verwenden, um die Eindeutigkeit wiederherzustellen. Mit Laufzeit-Hooks können Sie bestimmten Code ausführen, unmittelbar bevor Lambda einen Snapshot aufnimmt oder unmittelbar nachdem Lambda eine Funktion aus einem Snapshot fortsetzt.

Vermeiden des Speicherns eines Zustands, der von der Eindeutigkeit während der Initialisierung abhängt

Vermeiden Sie während der Initialisierungsphase Ihrer Funktion das Zwischenspeichern von Daten, die eindeutig sein sollen, z. B. das Generieren einer eindeutigen ID für die Protokollierung. Stattdessen empfehlen wir Ihnen, eindeutige Daten in Ihrem Funktionshandler zu generieren oder einen Laufzeit-Hook zu verwenden.

Example – Generierung einer eindeutigen ID im Funktionshandler

Das folgende Beispiel zeigt, wie eine UUID im Funktionshandler generiert wird.

```
import java.util.UUID;
  public class Handler implements RequestHandler<String, String> {
    private static UUID uniqueSandboxId = null;
    @Override
    public String handleRequest(String event, Context context) {
      if (uniqueSandboxId == null)
        uniqueSandboxId = UUID.randomUUID();
      System.out.println("Unique Sandbox Id: " + uniqueSandboxId);
      return "Hello, World!";
    }
  }
```

Kryptografisch sichere Pseudozufallszahlengeneratoren (CSPRNGs) verwenden

Wenn Ihre Anwendung von Zufälligkeit abhängt, empfehlen wir Ihnen, kryptographisch sichere Zufallszahlengeneratoren (CSPRNGs) zu verwenden. Die von Lambda verwaltete Laufzeit für Java enthält zwei integrierte CSPRNGs (OpenSSL 1.0.2 und `java.security.SecureRandom`), die automatisch die Zufälligkeit mit aufrechterhalten SnapStart. Software, die immer Zufallszahlen von erhält `/dev/random` oder `/dev/urandom` auch die Zufälligkeit mit beibehält SnapStart.

Example – java.security.SecureRandom

Das folgende Beispiel verwendet `java.security.SecureRandom`, das eindeutige Nummernfolgen erzeugt, auch wenn die Funktion aus einem Snapshot wiederhergestellt wird.

```
import java.security.SecureRandom;
  public class Handler implements RequestHandler<String, String> {
    private static SecureRandom rng = new SecureRandom();
    @Override
    public String handleRequest(String event, Context context) {
      for (int i = 0; i < 10; i++) {
        System.out.println(rng.next());
      }
      return "Hello, World!";
    }
  }
```

SnapStart Scan-Tool

Lambda bietet ein Scan-Tool an, um nach Code zu suchen, der Eindeutigkeit voraussetzt. Das SnapStart Scan-Tool ist ein Open-Source-SpotBugsPlugin, das eine statische Analyse anhand einer Reihe von Regeln durchführt. Das Scan-Tool hilft dabei, potenzielle Codeimplementierungen zu identifizieren, die Annahmen bezüglich der Eindeutigkeit widerlegen könnten. Installationsanweisungen und eine Liste der Prüfungen, die das Scan-Tool durchführt, finden Sie im aws-lambda-snapstart-java-Regeln-Repository auf GitHub.

Weitere Informationen zum Umgang mit Eindeutigkeit mit SnapStartfinden Sie unter Schneller starten mit AWS Lambda SnapStart im AWS Compute Blog.

Implementieren Sie Code vor oder nach Lambda-Funktions-Snapshots

Sie können Laufzeit-Hooks verwenden, um Code zu implementieren, bevor Lambda einen Snapshot erstellt oder nachdem Lambda eine Funktion aus einem Snapshot fortsetzt. aufzeit-Hooks sind als Teil des Open-Source-Projekts Coordinated Restore at Checkpoint (CRaC) verfügbar. CRaC wird für das Open-Java-Entwicklungs-Kit (OpenJDK) entwickelt. Ein Beispiel für die Verwendung von cRAC mit einer Referenzanwendung finden Sie im cRAC-Repository unter. GitHub CRaC verwendet drei Hauptelemente:

- `Resource` – Eine Schnittstelle mit zwei Methoden, `beforeCheckpoint()` und `afterRestore()`. Verwenden Sie diese Methoden, um den Code zu implementieren, den Sie vor einem Snapshot und nach einer Wiederherstellung ausführen möchten.
- `Context <R extends Resource>` – Um Benachrichtigungen für Prüfpunkte und Wiederherstellungen zu erhalten, muss eine `Resource` mit einem `Context` registriert sein.
- `Core` – Der Koordinationsservice, der das standardmäßige globale `Context` über die statische Methode `Core.getGlobalContext()` bereitstellt.

Weitere Informationen zum `Context` und `Resource` finden Sie unter Paket org.crac in der CRaC-Dokumentation.

Gehen Sie wie folgt vor, um Laufzeit-Hooks mit dem Paket org.crac zu implementieren. Die Lambda-Laufzeit enthält eine angepasste CRaC-Kontextimplementierung, die Ihre Laufzeit-Hooks vor dem Checkpointing und nach der Wiederherstellung aufruft.

Schritt 1: Aktualisieren der Entwicklungskonfiguration

Fügen Sie die `org.crac`-Abhängigkeit zur Entwicklungskonfiguration hinzu. Im folgenden Beispiel wird Gradle verwendet. Beispiele für andere Entwicklungssysteme finden Sie in der Apache-Maven-Dokumentation.

```
dependencies {
    compile group: 'com.amazonaws', name: 'aws-lambda-java-core', version: '1.2.1'
    # All other project dependecies go here:
    # ...
    # Then, add the org.crac dependency:
 implementation group: 'org.crac', name: 'crac', version: '1.4.0'
}
```

Schritt 2: Aktualisieren des Lambda-Handlers

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Weitere Informationen finden Sie unter Definieren Sie den Lambda-Funktionshandler in Java.

Der folgende Beispielhandler zeigt, wie Code vor Checkpointing (`beforeCheckpoint()`) und nach der Wiederherstellung (`afterRestore()`) ausgeführt wird. Dieser Handler registriert auch die `Resource` im Laufzeit-verwalteten globalen `Context`.

> **Note**
>
> Wenn Lambda einen Snapshot erstellt, kann Ihr Initialisierungscode bis zu 15 Minuten lang ausgeführt werden. Das Zeitlimit beträgt 130 Sekunden oder das konfigurierte Funktions-Timeout (maximal 900 Sekunden), je nachdem, welcher Wert höher ist. Ihre `beforeCheckpoint()`-Laufzeit-Hooks werden auf das Zeitlimit des Initialisierungscodes angerechnet. Wenn Lambda einen Snapshot wiederherstellt, muss die Laufzeit (JVM) geladen werden und `afterRestore()`-Laufzeit-Hooks müssen innerhalb des Timeout-Limits (10 Sekunden) abgeschlossen werden. Andernfalls erhalten Sie eine. SnapStartTimeoutException

```
...
  import org.crac.Resource;
  import org.crac.Core;
  ...
public class CRaCDemo implements RequestStreamHandler, Resource {
    public CRaCDemo() {
      Core.getGlobalContext().register(this);
    }
    public String handleRequest(String name, Context context) throws IOException {
      System.out.println("Handler execution");
      return "Hello " + name;
    }
    @Override
    public void beforeCheckpoint(org.crac.Context<? extends Resource> context)
        throws Exception {
      System.out.println("Before checkpoint");
```

```
    }
    @Override
    public void afterRestore(org.crac.Context<? extends Resource> context)
        throws Exception {
      System.out.println("After restore");
```

Der `Context` verwaltet nur ein `WeakReference` auf dem registrierten Objekt. Wenn für eine `Resource` eine Garbage Collection durchgeführt wird, werden Laufzeit-Hooks nicht ausgeführt. Ihr Code muss einen starken Verweis auf die `Resource` beibehalten, um sicherzustellen, dass der Laufzeit-Hook ausgeführt wird.

Hier sind zwei Beispiele für zu vermeidende Muster:

Example – Objekt ohne starke Referenz

```
Core.getGlobalContext().register( new MyResource() );
```

Example – Objekte anonymer Klassen

```
Core.getGlobalContext().register( new Resource() {

   @Override
   public void afterRestore(Context<? extends Resource> context) throws Exception {
    // ...
   }

   @Override
   public void beforeCheckpoint(Context<? extends Resource> context) throws Exception {
    // ...
   }

} );
```

Behalten Sie stattdessen eine starke Referenz bei. Im folgenden Beispiel wird die registrierte Ressource nicht von der Garbage Collection erfasst und Laufzeit-Hooks werden konsistent ausgeführt.

Example – Objekt mit starker Referenz

```
Resource myResource = new MyResource(); // This reference must be maintained to prevent
 the registered resource from being garbage collected
```

```
Core.getGlobalContext().register( myResource );
```

Überwachung für Lambda SnapStart

Sie können Ihre Lambda- SnapStart Funktionen mit Amazon CloudWatch, AWS X-Rayund überwachenLambda-Telemetrie-API.

> **Note**
>
> Die `AWS_LAMBDA_LOG_STREAM_NAME` Umgebungsvariablen `AWS_LAMBDA_LOG_GROUP_NAME` und sind in Lambda- SnapStart Funktionen nicht verfügbar.

CloudWatch für SnapStart

Es gibt einige Unterschiede im CloudWatch Protokollstream-Format für - SnapStart Funktionen:

- Initialisierungsprotokolle – Wenn eine neue Ausführungsumgebung erstellt wird, enthält `REPORT` das Feld `Init Duration` nicht. Das liegt daran, dass Lambda SnapStart Funktionen initialisiert, wenn Sie eine Version erstellen und nicht während des Funktionsaufrufs. Bei - SnapStart Funktionen befindet sich das -`Init Duration`Feld im -`INIT_REPORT`Datensatz. Dieser Datensatz zeigt die Dauer von Init-Phase, einschließlich der Dauer aller `beforeCheckpoint`-Laufizeit-Hooks an.
- Aufrufprotokolle – Wenn eine neue Ausführungsumgebung erstellt wird, enthält `REPORT` die Felder `Restore Duration` und `Billed Restore Duration`:
  - `Restore Duration`: Die Zeit, die Lambda benötigt, um einen Snapshot wiederherzustellen, die Laufzeit (JVM) zu laden und alle `afterRestore`-Laufzeit-Hooks auszuführen. Der Prozess der Wiederherstellung von Snapshots kann Zeit beinhalten, die für Aktivitäten außerhalb der MicroVM aufgewendet wird. Diese Zeit wird in `Restore Duration` erfasst.
  - `Billed Restore Duration`: Die Zeit, die Lambda benötigt, um die Laufzeit (JVM) zu laden und alle `afterRestore`-Hooks auszuführen. Die Zeit, die für die Wiederherstellung eines Snapshots benötigt wird, wird Ihnen nicht in Rechnung gestellt.

> **Note**
>
> Die Gebühren für die Dauer gelten für Code, der im Funktions-Handler ausgeführt wird, Initialisierungscode, der außerhalb des Handlers deklariert ist, die Zeit, die zum Laden der

Laufzeit (JVM) benötigt wird, und Code, der in einem Laufzeit-Hook ausgeführt wird. Weitere Informationen finden Sie unter SnapStart Preisgestaltung.

Die Kaltstartdauer ist die Summe von `Restore Duration` + `Duration`.

Das folgende Beispiel ist eine Lambda-Insights-Abfrage, die die Latenzperzentile für SnapStart Funktionen zurückgibt. Weitere Informationen zu Lambda-Insights-Abfragen finden Sie unter Beispiel-Workflow mit Abfragen zur Fehlerbehebung einer Funktion.

```
filter @type = "REPORT"
  | parse @log /\d+:\/aws\/lambda\/(?<function>.*)/
  | parse @message /Restore Duration: (?<restoreDuration>.*?) ms/
  | stats
count(*) as invocations,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 50) as p50,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 90) as p90,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99) as p99,
pct(@duration+coalesce(@initDuration,0)+coalesce(restoreDuration,0), 99.9) as p99.9
group by function, (ispresent(@initDuration) or ispresent(restoreDuration)) as
 coldstart
  | sort by coldstart desc
```

Aktives X-Ray-Tracing für SnapStart

Sie können X-Ray verwenden, um Anfragen an Lambda- SnapStart Funktionen zu verfolgen. Es gibt einige Unterschiede bei den X-Ray-Teilsegmenten für SnapStart Funktionen:

- Es gibt kein `Initialization` Untersegment für - SnapStart Funktionen.
- Das Teilsegment `Restore` zeigt die Zeit an, die Lambda benötigt, um einen Snapshot wiederherzustellen, die Laufzeit (JVM) zu laden und vorhandene `afterRestore`-Laufzeit-Hooks auszuführen. Der Prozess der Wiederherstellung von Snapshots kann Zeit beinhalten, die für Aktivitäten außerhalb der MicroVM aufgewendet wird. Diese Zeit wird im `Restore`-Untersegment erfasst. Die Zeit, die Sie außerhalb der microVM für die Wiederherstellung eines Snapshots aufwenden, wird Ihnen nicht in Rechnung gestellt.

Telemetrie-API-Ereignisse für SnapStart

Lambda sendet die folgenden SnapStart Ereignisse an Telemetrie-API:

- `platform.restoreStart` – Zeigt die Zeit an, zu der die `Restore`-Phase gestartet wurde.
- `platform.restoreRuntimeDone` – Zeigt an, ob die `Restore`-Phase erfolgreich war. Lambda sendet diese Nachricht, wenn die Laufzeit eine `restore/next`-Laufzeit-API-Anfrage sendet. Es gibt drei mögliche Status: erfolgreich, fehlgeschlagen und Timeout.
- `platform.restoreReport` – Zeigt an, wie lange die `Restore`-Phase gedauert hat und wie viele Millisekunden Ihnen während dieser Phase in Rechnung gestellt wurden.

Amazon-API-Gateway- und Funktions-URL-Metriken

Wenn Sie eine Web-API mit API Gateway erstellen, können Sie die -IntegrationLatencyMetrik verwenden, um die end-to-end Latenz zu messen (die Zeit zwischen dem Zeitpunkt, an dem API Gateway eine Anfrage an das Backend weiterleitet, und dem Zeitpunkt, an dem es eine Antwort vom Backend erhält).

Wenn Sie eine Lambda-Funktions-URL verwenden, können Sie die -UrlRequestLatencyMetrik verwenden, um die end-to-end Latenz zu messen (die Zeit zwischen dem Empfang einer Anforderung durch die Funktions-URL und dem Zeitpunkt, an dem die Funktions-URL eine Antwort zurückgibt).

Sicherheitsmodell für Lambda SnapStart

Lambda SnapStart unterstützt die Verschlüsselung im Ruhezustand. Lambda verschlüsselt Snapshots mit einem AWS KMS key. Standardmäßig verwendet Lambda einen Von AWS verwalteter Schlüssel. Wenn dieses Standardverhalten für Ihren Workflow geeignet ist, müssen Sie nichts weiter einrichten. Andernfalls können Sie die `--kms-key-arn` Option in der create-function oder dem update-function-configuration Befehl verwenden, um einen vom AWS KMS Kunden verwalteten Schlüssel bereitzustellen. Sie können dies tun, um die Rotation des KMS-Schlüssels zu steuern oder um die Anforderungen Ihrer Organisation für die Verwaltung von KMS-Schlüsseln zu erfüllen. Für vom Kunden verwaltete Schlüssel fallen Standard-AWS KMS-Gebühren an. Weitere Informationen finden Sie unter AWS Key Management Service Preise.

Wenn Sie eine SnapStart Funktion oder Funktionsversion löschen, schlagen alle `Invoke` Anforderungen an diese Funktion oder Funktionsversion fehl. Lambda löscht automatisch Snapshots, die 14 Tage lang nicht aufgerufen wurden. Lambda entfernt alle Ressourcen, die mit gelöschten Snapshots verknüpft sind, gemäß der Allgemeinen Datenschutzverordnung (DSGVO).

Maximieren Sie die Lambda-Leistung SnapStart

Themen

Leistungsoptimierung

> **Note**
>
> SnapStart funktioniert am besten, wenn es mit Funktionsaufrufen in großem Maßstab verwendet wird. Funktionen, die selten aufgerufen werden, weisen möglicherweise nicht dieselben Leistungsverbesserungen auf.

Um die Vorteile von zu maximieren SnapStart, empfehlen wir, Klassen, die zur Startlatenz beitragen, in Ihrem Initialisierungscode und nicht im Funktionshandler vorab zu laden. Dadurch wird die Latenz, die mit dem starken Laden von Klassen verbunden ist, aus dem Aufrufpfad entfernt, wodurch die Startleistung mit optimiert wird. SnapStart

Wenn Sie Klassen während der Initialisierung nicht vorab laden können, empfehlen wir, dass Sie Klassen mit Dummy-Aufrufen vorab laden. Aktualisieren Sie dazu den Code des Funktionshandlers, wie im folgenden Beispiel aus der Funktion pet store im AWS GitHub Labs-Repository gezeigt.

```
private static SpringLambdaContainerHandler<AwsProxyRequest, AwsProxyResponse> handler;
  static {
      try {
          handler =
 SpringLambdaContainerHandler.getAwsProxyHandler(PetStoreSpringAppConfig.class);

          // Use the onStartup method of the handler to register the custom filter
          handler.onStartup(servletContext -> {
              FilterRegistration.Dynamic registration =
 servletContext.addFilter("CognitoIdentityFilter", CognitoIdentityFilter.class);
              registration.addMappingForUrlPatterns(EnumSet.of(DispatcherType.REQUEST),
 false, "/*");
          });
```

```
            // Send a fake Amazon API Gateway request to the handler to load classes
    ahead of time
            ApiGatewayRequestIdentity identity = new ApiGatewayRequestIdentity();
            identity.setApiKey("foo");
            identity.setAccountId("foo");
            identity.setAccessKey("foo");

            AwsProxyRequestContext reqCtx = new AwsProxyRequestContext();
            reqCtx.setPath("/pets");
            reqCtx.setStage("default");
            reqCtx.setAuthorizer(null);
            reqCtx.setIdentity(identity);

            AwsProxyRequest req = new AwsProxyRequest();
            req.setHttpMethod("GET");
            req.setPath("/pets");
            req.setBody("");
            req.setRequestContext(reqCtx);

            Context ctx = new TestContext();
            handler.proxy(req, ctx);


        } catch (ContainerInitializationException e) {
            // if we fail here. We re-throw the exception to force another cold start
            e.printStackTrace();
            throw new RuntimeException("Could not initialize Spring framework", e);
        }
    }
```

Bewährte Methoden für Netzwerke

Der Zustand der Verbindungen, die Ihre Funktion während der Initialisierungsphase erstellt, wird nicht garantiert, wenn Lambda Ihre Funktion aus einem Snapshot wieder aufnimmt. In den meisten Fällen werden Netzwerkverbindungen, die ein AWS SDK herstellt, automatisch wieder aufgenommen. Für andere Verbindungen empfehlen wir die folgenden bewährten Methoden.

Wiederherstellen von Netzwerkverbindungen

Stellen Sie Ihre Netzwerkverbindungen immer wieder her, wenn Ihre Funktion von einem Snapshot fortgesetzt wird. Wir empfehlen, dass Sie die Netzwerkverbindungen im Funktionshandler wiederherstellen. Alternativ können Sie ein `afterRestore`-Laufzeit-Hook verwenden.

Verwenden Sie den Hostnamen nicht als eindeutige ID der Ausführungsumgebung

Wir raten davon ab, `hostname` zu verwenden, um Ihre Ausführungsumgebung als eindeutigen Knoten oder Container in Ihren Anwendungen zu identifizieren. Bei SnapStart wird ein einzelner Snapshot als Ausgangszustand für mehrere Ausführungsumgebungen verwendet, und alle Ausführungsumgebungen geben denselben `hostname` Wert für zurück`InetAddress.getLocalHost()`. Für Anwendungen, die eine eindeutige Identität oder einen eindeutigen `hostname`-Wert der Ausführungsumgebung erfordern, empfehlen wir, im Funktionshandler eine eindeutige ID zu generieren. Oder verwenden Sie einen `afterRestore`-Laufzeit-Hook, um eine eindeutige ID zu generieren, und verwenden Sie dann die eindeutige ID für die Ausführungsumgebung.

Vermeiden der Bindung von Verbindungen an feste Quellports

Wir empfehlen, Netzwerkverbindungen nicht an feste Quellports zu binden. Wenn eine Funktion nach einem Snapshot wieder aufgenommen wird, werden die Verbindungen neu aufgebaut, und Netzwerkverbindungen, die an einen festen Quellport gebunden sind, können fehlschlagen.

Vermeiden Sie die Verwendung von Java-DNS-Cache

Lambda-Funktionen speichern DNS-Antworten bereits im Cache. Wenn Sie einen anderen DNS-Cache mit verwenden SnapStart, kann es zu Verbindungstimeouts kommen, wenn die Funktion von einem Snapshot aus wieder aufgenommen wird.

Die `java.util.logging.Logger` Klasse kann den JVM-DNS-Cache indirekt aktivieren. Um die Standardeinstellungen zu überschreiben, setzen Sie networkaddress.cache.ttl vor der Initialisierung auf 0. `logger` Beispiel:

```
public class MyHandler {
  // first set TTL property
  static{
   java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
  }
 // then instantiate logger
  var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
}
```

Um `UnknownHostException` Ausfälle zu vermeiden, empfehlen wir, den Wert auf 0 zu setzen. `networkaddress.cache.negative.ttl` Sie können diese Eigenschaft für eine Lambda-Funktion mit der `AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0` Umgebungsvariablen festlegen.

Durch die Deaktivierung des JVM-DNS-Caches wird das verwaltete DNS-Caching von Lambda nicht deaktiviert.

Einstellungen für die Java-Lambda-Funktionsanpassung

Auf dieser Seite werden spezifische Einstellungen für Java-Funktionen in beschrieben AWS Lambda. Sie können diese Einstellungen verwenden, um das Startup-Verhalten der Java-Laufzeit anzupassen. Dies kann die allgemeine Funktionslatenz reduzieren und die Gesamtleistung der Funktionen verbessern, ohne dass Code geändert werden muss.

Sections

JAVA_TOOL_OPTIONS Umgebungsvariable

In Java unterstützt Lambda die Umgebungsvariable `JAVA_TOOL_OPTIONS`, um zusätzliche Befehlszeilenvariablen in Lambda festzulegen. Sie können diese Umgebungsvariable auf verschiedene Arten verwenden, z. B. um die Einstellungen für die gestufte Kompilierung anzupassen. Im nächsten Beispiel wird gezeigt, wie die Umgebungsvariable `JAVA_TOOL_OPTIONS` für diesen Anwendungsfall verwendet wird.

Beispiel: Einstellungen für die gestufte Kompilierung anpassen

Die gestaffelte Kompilierung ist ein Feature der Java Virtual Machine (JVM). Sie können bestimmte Einstellungen für die gestaffelte Kompilierung verwenden, um die JVM-Compiler just-in-time (JIT) optimal zu nutzen. In der Regel ist der C1-Compiler für eine schnelle Startzeit optimiert. Der C2-Compiler ist für die beste Gesamtleistung optimiert, benötigt aber auch mehr Speicher und es dauert länger, bis er erreicht ist.

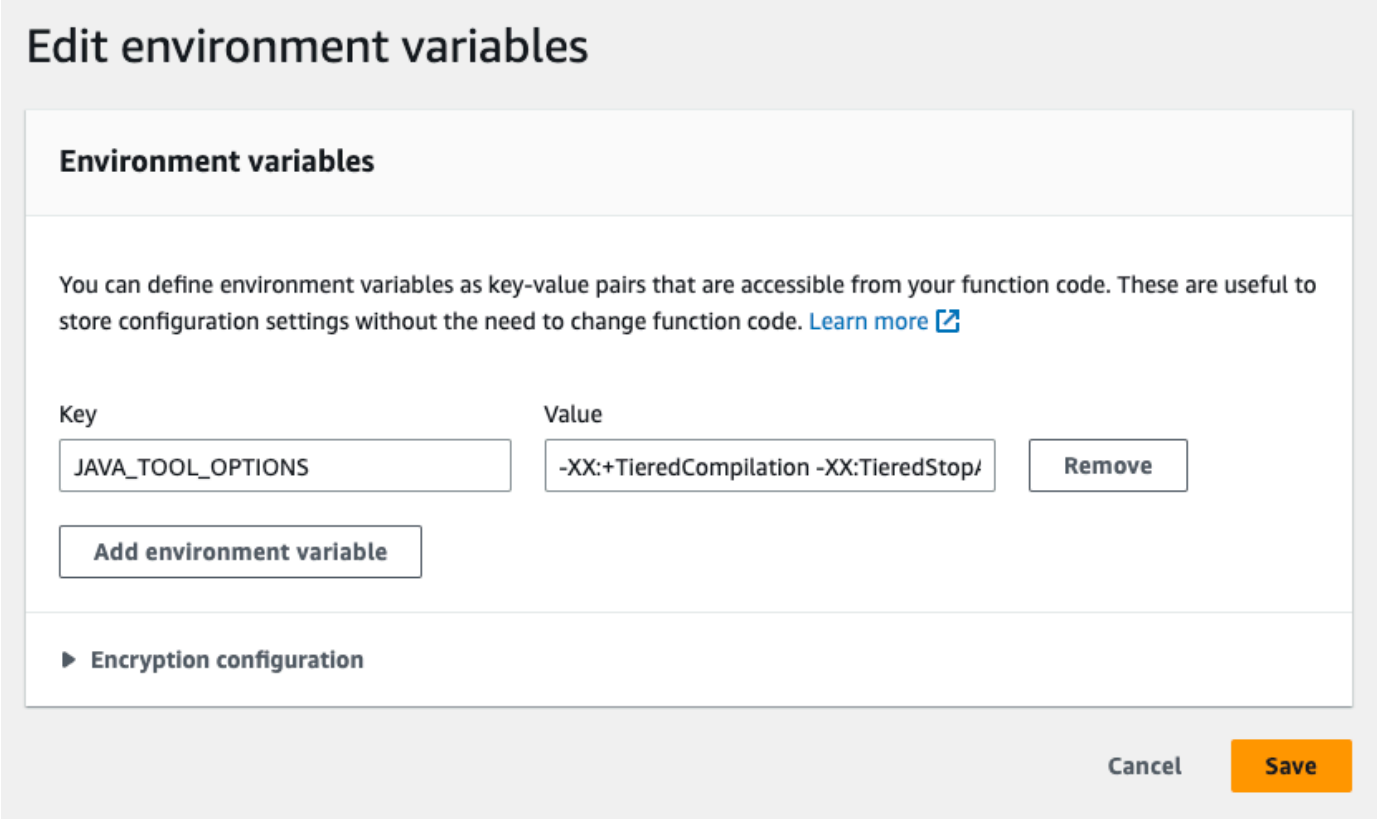
Die gestufte Kompilierung umfasst 5 verschiedene Stufen. Auf Stufe 0 interpretiert die JVM Java-Bytecode. Auf Stufe 4 verwendet die JVM den C2-Compiler, um die beim Startup der Anwendung gesammelten Profildaten zu analysieren. Im Laufe der Zeit überwacht sie die Code-Nutzung, um die besten Optimierungen zu identifizieren.

Durch die Anpassung der Stufe der gestuften Kompilierung können Sie die Kaltstartlatenz von Java-Funktionen reduzieren. Legen Sie beispielsweise die Stufe der gestaffelten Kompilierung auf 1 fest, damit die JVM den C1-Compiler verwendet. Dieser Compiler erzeugt schnell optimierten nativen Code, generiert jedoch keine Profildaten und verwendet niemals den C2-Compiler.

In der Java-17-Laufzeit ist das JVM-Flag für die mehrstufige Kompilierung standardmäßig so eingestellt, dass es bei Stufe 1 stoppt. Bis zur Java-11-Laufzeit können Sie die gestufte Kompilierungsstufe auf 1 setzen, indem Sie die folgenden Schritte ausführen:

Anpassen der Einstellungen für die gestufte Kompilierung (Konsole)

1. Öffnen Sie die Seite Funktionen in der Lambda-Konsole.
2. Wählen Sie eine Java-Funktion, für die Sie die gestufte Kompilierung anpassen möchten.
3. Wählen Sie die Registerkarte Konfiguration und dann im linken Menü die Option Umgebungsvariablen aus.
4. Wählen Sie Bearbeiten aus.
5. Wählen Sie Umgebungsvariablen hinzufügen aus.
6. Geben Sie `JAVA_TOOL_OPTIONS` als Schlüssel ein. Geben Sie `-XX:+TieredCompilation -XX:TieredStopAtLevel=1` als Wert ein.



7. Wählen Sie Speichern.

> **Note**
>
> Sie können Lambda auch verwenden SnapStart , um Kaltstartprobleme zu beheben. SnapStart verwendet zwischengespeicherte Snapshots Ihrer Ausführungsumgebung, um die Startleistung erheblich zu verbessern. Weitere Informationen zu SnapStart

Funktionen, Einschränkungen und unterstützten Regionen finden Sie unter Verbesserung der Startleistung mit Lambda SnapStart.

Beispiel: Anpassen des GC-Verhaltens mit JAVA_TOOL_OPTIONS

Java-11-Laufzeiten verwenden den Serial Garbage Collector (GC) für Garbage Collection. Standardmäßig verwenden Java-17-Laufzeiten auch den Serial GC. Mit Java 17 können Sie jedoch auch die Umgebungsvariable `JAVA_TOOL_OPTIONS` verwenden, um den Standard-GC zu ändern. Sie können zwischen dem Parallel GC und dem Shenandoah GC wählen.

Wenn Ihre Workload beispielsweise mehr Arbeitsspeicher und mehrere CPUs benötigt, sollten Sie erwägen, den Parallel GC zu verwenden, um eine bessere Leistung zu erzielen. Hängen Sie dazu Folgendes an den Wert Ihrer Umgebungsvariablen `JAVA_TOOL_OPTIONS` an:

```
-XX:+UseParallelGC
```

AWS Lambda Kontextobjekt in Java

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Methoden

- `getRemainingTimeInMillis()` – Gibt die Anzahl der verbleibenden Millisekunden zurück, bevor die Ausführung das Zeitlimit überschreitet.
- `getFunctionName()` – Gibt den Namen der Lambda-Funktion zurück.
- `getFunctionVersion()` – Gibt die Version der Funktion zurück.
- `getInvokedFunctionArn()` – Gibt den Amazon-Ressourcennamen (ARN) zurück, der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `getMemoryLimitInMB()` – Gibt die Menge an Arbeitsspeicher zurück, die der Funktion zugewiesen ist.
- `getAwsRequestId()` – Gibt den Bezeichner der Aufrufanforderung zurück.
- `getLogGroupName()` – Gibt die Protokollgruppe für die Funktion zurück.
- `getLogStreamName()` – Gibt den Protokollstrom für die Funktionsinstance zurück.
- `getIdentity()` – Gibt Informationen zur Amazon-Cognito-Identität zurück, die die Anforderung autorisiert hat.
- `getClientContext()` – (mobile Apps) Gibt Clientkontext zurück, der Lambda von der Clientanwendung bereitgestellt wird.
- `getLogger()` – Gibt das Logger-Objekt für die Funktion zurück.

Das folgende Beispiel zeigt eine Funktion, die das Kontextobjekt verwendet, um auf den Lambda-Logger zuzugreifen.

Example handler.java

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
```

```
import com.amazonaws.services.lambda.runtime.RequestHandler;

import java.util.Map;

// Handler value: example.Handler
public class Handler implements RequestHandler<Map<String,String>, Void>{

  @Override
  public Void handleRequest(Map<String,String> event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    logger.log("EVENT TYPE: " + event.getClass());
    return null;
  }
}
```

Die Funktion protokolliert den Klassentyp des eingehenden Ereignisses, bevor sie zurückkehrt`null`.

Example Protokollausgabe

```
EVENT TYPE: class java.util.LinkedHashMap
```

Die Schnittstelle für das Kontextobjekt ist in der aws-lambda-java-core-Bibliothek verfügbar. Sie können diese Schnittstelle implementieren, um eine Kontextklasse zum Testen zu erstellen. Das folgende Beispiel zeigt eine Kontextklasse, die Dummy-Werte für die meisten Eigenschaften und einen funktionierenden Testlogger zurückgibt.

Example src/test/java/example/ .java TestContext

```
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.CognitoIdentity;
import com.amazonaws.services.lambda.runtime.ClientContext;
import com.amazonaws.services.lambda.runtime.LambdaLogger;

public class TestContext implements Context{

  public TestContext() {}
  public String getAwsRequestId(){
    return new String("495b12a8-xmpl-4eca-8168-160484189f99");
  }
```

```
  public String getLogGroupName(){
    return new String("/aws/lambda/my-function");
  }
  public String getLogStreamName(){
    return new String("2020/02/26/[$LATEST]704f8dxmpla04097b9134246b8438f1a");
  }
  public String getFunctionName(){
    return new String("my-function");
  }
  public String getFunctionVersion(){
    return new String("$LATEST");
  }
  public String getInvokedFunctionArn(){
    return new String("arn:aws:lambda:us-east-2:123456789012:function:my-function");
  }
  public CognitoIdentity getIdentity(){
    return null;
  }
  public ClientContext getClientContext(){
    return null;
  }
  public int getRemainingTimeInMillis(){
    return 300000;
  }
  public int getMemoryLimitInMB(){
    return 512;
  }
  public LambdaLogger getLogger(){
    return new TestLogger();
  }

}
```

Weitere Informationen zu Protokollierung finden Sie unter AWS Lambda Funktionsprotokollierung in Java.

Kontext in Beispielanwendungen

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung des Kontextobjekts demonstrieren. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS Serverless Application Model (AWS SAM) -Vorlage und unterstützende Ressourcen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

AWS Lambda Funktionsprotokollierung in Java

AWS Lambda überwacht automatisch Lambda-Funktionen und sendet Protokolleinträge an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen zu CloudWatch Logs finden Sie unterVerwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Um Protokolle aus Ihrem Funktionscode auszugeben, können Sie Methoden von java.lang.System oder jedes Protokollierungsmodul verwenden, das nach stdout oder stderr schreibt.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus dem Code Ihrer Funktion auszugeben, können Sie Methoden für java.lang.System verwenden oder ein beliebiges Protokollierungsmodul, das in `stdout` oder `stderr` schreibt. Die aws-lambda-java-core-Bibliothek stellt eine Logger-Klasse mit dem Namen `LambdaLogger` bereit, auf die Sie vom Kontextobjekt zugreifen können. Die Logger-Klasse unterstützt mehrzeilige Protokolle.

Im folgenden Beispiel wird der `LambdaLogger`-Logger verwendet, der vom Kontextobjekt bereitgestellt wird.

Example handler.java

```
// Handler value: example.Handler
public class Handler implements RequestHandler<Object, String>{
  Gson gson = new GsonBuilder().setPrettyPrinting().create();
  @Override
  public String handleRequest(Object event, Context context)
  {
    LambdaLogger logger = context.getLogger();
    String response = new String("SUCCESS");
    // log execution details
    logger.log("ENVIRONMENT VARIABLES: " + gson.toJson(System.getenv()));
    logger.log("CONTEXT: " + gson.toJson(context));
    // process event
    logger.log("EVENT: " + gson.toJson(event));
    return response;
  }
}
```

Example Protokollformat

```
START RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Version: $LATEST
ENVIRONMENT VARIABLES:
{
    "_HANDLER": "example.Handler",
    "AWS_EXECUTION_ENV": "AWS_Lambda_java8",
    "AWS_LAMBDA_FUNCTION_MEMORY_SIZE": "512",
    ...
}
CONTEXT:
{
    "memoryLimit": 512,
    "awsRequestId": "6bc28136-xmpl-4365-b021-0ce6b2e64ab0",
    "functionName": "java-console",
    ...
}
EVENT:
{
  "records": [
    {
      "messageId": "19dd0b57-xmpl-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
```

```
        ...
    }
  ]
}
END RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0
REPORT RequestId: 6bc28136-xmpl-4365-b021-0ce6b2e64ab0 Duration: 198.50 ms Billed
 Duration: 200 ms Memory Size: 512 MB Max Memory Used: 90 MB Init Duration: 524.75 ms
```

Die Java-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die Berichtszeile enthält die folgenden Details:

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.
- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Verwenden von Lambda-Optionen für die erweiterte Protokollierung mit Java

Um Ihnen mehr Kontrolle darüber zu geben, wie die Protokolle Ihrer Funktionen erfasst, verarbeitet und verwendet werden, können Sie die folgenden Protokollierungsoptionen für unterstützte Java-Laufzeiten konfigurieren:

- Protokollformat – Wählen Sie zwischen Klartext und einem strukturierten JSON-Format für die Protokolle Ihrer Funktion aus.
- Protokollebene — für Logs im JSON-Format wählen Sie die Detailebene der Logs, an die Lambda sendet CloudWatch, wie ERROR, DEBUG oder INFO

- Protokollgruppe — wählen Sie die CloudWatch Protokollgruppe aus, an die Ihre Funktion Logs sendet

Weitere Informationen zu diesen Protokollierungsoptionen und Anweisungen zur Konfiguration Ihrer Funktion für deren Verwendung finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.

Informationen zur Verwendung der Optionen für das Protokollformat und die Protokollebene mit Ihren Java-Lambda-Funktionen finden Sie in den folgenden Abschnitten.

Verwenden des strukturierten JSON-Protokollformats mit Java

Wenn Sie JSON für das Protokollformat Ihrer Funktion auswählen, sendet Lambda die Protokollausgabe unter Verwendung der `LambdaLogger`-Klasse als strukturiertes JSON. Jedes JSON-Protokollobjekt enthält mindestens vier Schlüssel-Wert-Paare mit den folgenden Schlüsseln:

- `"timestamp"` – die Uhrzeit, zu der die Protokollmeldung generiert wurde
- `"level"` – die der Meldung zugewiesene Protokollebene
- `"message"` – der Inhalt der Protokollmeldung
- `"AWSrequestId"` – die eindeutige Anforderungs-ID für den Funktionsaufruf

Abhängig von der verwendeten Protokollierungsmethode können die im JSON-Format erfassten Protokollausgaben Ihrer Funktion auch zusätzliche Schlüssel-Wert-Paare enthalten.

Um Protokollen, die Sie mit dem `LambdaLogger`-Logger erstellen, eine Ebene zuzuweisen, müssen Sie in Ihrem Protokollierungsbefehl ein `LogLevel`-Argument angeben, wie im folgenden Beispiel gezeigt.

Example Protokollierungscode für Java

```
LambdaLogger logger = context.getLogger();
logger.log("This is a debug log", LogLevel.DEBUG);
```

Diese Protokollausgabe mit diesem Beispielcode würde wie folgt in CloudWatch Logs erfasst werden:

Example JSON-Protokolldatensatz

```
{
```

```
    "timestamp":"2023-11-01T00:21:51.358Z",
    "level":"DEBUG",
    "message":"This is a debug log",
    "AWSrequestId":"93f25699-2cbf-4976-8f94-336a0aa98c6f"
}
```

Wenn Sie Ihrer Protokollausgabe keine Ebene zuweisen, weist Lambda ihr automatisch die Ebene INFO zu.

Wenn Ihr Code bereits eine andere Protokollierungsbibliothek verwendet, um strukturierte JSON-Protokolle zu erstellen, müssen Sie keine Änderungen vornehmen. Lambda codiert Protokolle, die bereits JSON-codiert sind, nicht doppelt. Selbst wenn Sie Ihre Funktion so konfigurieren, dass sie das JSON-Protokollformat verwendet, erscheinen Ihre Logging-Ausgaben CloudWatch in der von Ihnen definierten JSON-Struktur.

Verwenden der Filterung auf Protokollebene mit Java

AWS Lambda Um Ihre Anwendungsprotokolle nach ihrer Protokollebene zu filtern, muss Ihre Funktion Protokolle im JSON-Format verwenden. Sie können dies auf zwei Arten erreichen:

- Erstellen Sie Protokollausgaben mithilfe der Standard-`LambdaLogger` und konfigurieren Sie Ihre Funktion so, dass sie die JSON-Protokollformatierung verwendet. Lambda filtert dann Ihre Protokollausgaben mithilfe des Schlüssel-Wert-Paars „level“ im JSON-Objekt, wie unter the section called “Verwenden des strukturierten JSON-Protokollformats mit Java” beschrieben. Informationen zur Konfiguration des Protokollformats Ihrer Funktion finden Sie unter the section called “Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion”.
- Verwenden Sie eine andere Protokollierungsbibliothek oder Methode, um strukturierte JSON-Protokolle in Ihrem Code zu erstellen, die ein „level“-Schlüssel-Wert-Paar enthalten, das die Ebene der Protokollausgabe definiert. Sie können auch eine beliebige Protokollierungsbibliothek verwenden, die JSON-Protokolle in `stdout` oder `stderr` schreibt. Sie können beispielsweise Powertools for AWS Lambda oder das Paket Log4J2 verwenden, um strukturierte JSON-Protokollausgaben aus Ihrem Code zu generieren. Weitere Informationen dazu finden Sie unter the section called “Verwendung von Powertools für AWS Lambda (Java) und für strukturiertes Logging AWS SAM” und the section called “Erweiterte Protokollierung mit Log4j2 und SLF4J”.

Wenn Sie Ihre Funktion so konfigurieren, dass sie Filterung auf Protokollebene verwendet, müssen Sie aus den folgenden Optionen für die Protokollebene auswählen, die Lambda an Logs senden soll: CloudWatch

Protokollebene	Standardnutzung
TRACE (am detailliertesten)	Die detailliertesten Informationen, die verwendet werden, um den Ausführungspfad Ihres Codes nachzuverfolgen
DEBUG	Detaillierte Informationen für das System-De bugging
INFO	Meldungen, die den normalen Betrieb Ihrer Funktion erfassen
WARN	Meldungen über mögliche Fehler, die zu unerwartetem Verhalten führen können, wenn sie nicht behoben werden
ERROR	Meldungen über Probleme, die verhindern, dass der Code wie erwartet funktioniert
FATAL (am wenigsten Details)	Meldungen über schwerwiegende Fehler, die dazu führen, dass die Anwendung nicht mehr funktioniert

Damit Lambda die Protokolle Ihrer Funktion filtern kann, müssen Sie auch ein `"timestamp"`-Schlüssel-Wert-Paar in Ihre JSON-Protokollausgabe aufnehmen. Die Uhrzeit muss im gültigen RFC 3339-Zeitstempelformat angegeben werden. Wenn Sie keinen gültigen Zeitstempel angeben, weist Lambda dem Protokoll die Stufe INFO zu und fügt einen Zeitstempel für Sie hinzu.

Lambda sendet Protokolle der ausgewählten Stufe und niedriger bis CloudWatch. Wenn Sie beispielsweise die Protokollebene WARN konfigurieren, sendet Lambda Protokolle, die den Stufen WARN, ERROR und FATAL entsprechen.

Erweiterte Protokollierung mit Log4j2 und SLF4J

> **Note**
>
> AWS Lambda nimmt Log4j2 nicht in seine verwalteten Laufzeiten oder Basis-Container-Images auf. Diese sind daher von den in CVE-2021-44228, CVE-2021-45046 und CVE-2021-45105 beschriebenen Problemen nicht betroffen.
> Für Fälle, in denen eine Kundenfunktion eine betroffene Log4j2-Version enthält, haben wir eine Änderung an den verwalteten Lambda-Java-Laufzeiten und Basis-Container-Images vorgenommen, die dazu beiträgt, die Probleme in CVE-2021-44228, CVE-2021-45046 und CVE-2021-45105 zu entschärfen. Infolge dieser Änderung sehen Kunden, die Log4J2 verwenden, möglicherweise einen zusätzlichen Protokolleintrag ähnlich wie „`Transforming org/apache/logging/log4j/core/lookup/JndiLookup (java.net.URLClassLoader@...)`“. Alle Log-Strings, die in der Log4J2-Ausgabe auf den jndi-Mapper verweisen, werden durch „`Patched JndiLookup::lookup()`“ ersetzt.
> Unabhängig von dieser Änderung empfehlen wir allen Kunden, deren Funktionen Log4j2 enthalten, nachdrücklich, auf die neueste Version zu aktualisieren. Insbesondere Kunden, die die aws-lambda-java-log 4j2-Bibliothek in ihren Funktionen verwenden, sollten auf Version 1.5.0 (oder höher) aktualisieren und ihre Funktionen erneut bereitstellen. Diese Version aktualisiert die zugrunde liegenden Abhängigkeiten des Log4j2-Dienstprogramms auf Version 2.17.0 (oder höher). Die aktualisierte aws-lambda-java-log 4j2-Binärdatei ist im Maven-Repository verfügbar und der Quellcode ist auf Github verfügbar.
> Beachten Sie abschließend, dass Bibliotheken, die sich auf aws-lambda-java-log4j (v1.0.0 oder 1.0.1) beziehen, unter keinen Umständen verwendet werden sollten. Diese Bibliotheken beziehen sich auf Version 1.x von log4j, deren Nutzungsdauer 2015 abgelaufen ist. Die Bibliotheken werden nicht unterstützt, nicht gewartet, nicht gepatcht und haben bekannte Sicherheitslücken.

Verwenden Sie Apache Log4j2 mit SLF4J, um die Protokollausgabe anzupassen, die Protokollierung bei Komponententests zu unterstützen und AWS SDK-Aufrufe zu protokollieren. Log4j ist eine Protokollierungsbibliothek für Java-Programme, mit der Sie Protokollstufen konfigurieren und Appender-Bibliotheken verwenden können. SLF4J ist eine Fassadenbibliothek, mit der Sie ändern können, welche Bibliothek Sie verwenden, ohne Ihren Funktionscode zu ändern.

Um die Anforderungs-ID zu den Protokollen Ihrer Funktion hinzuzufügen, verwenden Sie den Appender in der Bibliothek aws-lambda-java-log4j2 .

Example src/main/resources/log4j2.xml -Appender-Konfiguration

```
<Configuration>
  <Appenders>
    <Lambda name="Lambda" format="${env:AWS_LAMBDA_LOG_FORMAT:-TEXT}">
       <LambdaTextFormat>
         <PatternLayout>
             <pattern>%d{yyyy-MM-dd HH:mm:ss} %X{AWSRequestId} %-5p %c{1} - %m%n </
pattern>
         </PatternLayout>
       </LambdaTextFormat>
       <LambdaJSONFormat>
         <JsonTemplateLayout eventTemplateUri="classpath:LambdaLayout.json" />
       </LambdaJSONFormat>
     </Lambda>
   </Appenders>
   <Loggers>
     <Root level="${env:AWS_LAMBDA_LOG_LEVEL:-INFO}">
       <AppenderRef ref="Lambda"/>
     </Root>
     <Logger name="software.amazon.awssdk" level="WARN" />
     <Logger name="software.amazon.awssdk.request" level="DEBUG" />
   </Loggers>
 </Configuration>
```

Sie können entscheiden, wie Ihre Log4j2-Protokolle entweder für Klartext- oder JSON-Ausgaben konfiguriert werden sollen, indem Sie unter den Tags `<LambdaTextFormat>` und `<LambdaJSONFormat>` ein Layout angeben.

In diesem Beispiel wird im Textmodus jeder Zeile das Datum, die Uhrzeit, die Anforderungs-ID, die Protokollstufe und der Klassenname vorangestellt. Im JSON-Modus wird das `<JsonTemplateLayout>` mit einer Konfiguration verwendet, die zusammen mit der `aws-lambda-java-log4j2`-Bibliothek geliefert wird.

SLF4J ist eine Fassadenbibliothek zum Protokollieren in Java-Code. In Ihrem Funktionscode verwenden Sie die SLF4J-Logger-Factory, um einen Logger mit Methoden für Protokollstufen wie `info()` und `warn()` abzurufen. Bei Ihrer Build-Konfiguration schließen Sie die Protokollierungsbibliothek und den SLF4J-Adapter in den Klassenpfad ein. Durch Ändern der Bibliotheken in der Build-Konfiguration können Sie den Logger-Typ ändern, ohne den Funktionscode zu ändern. SLF4J ist erforderlich, um Protokolle aus SDK for Java zu erfassen.

Im folgenden Beispielcode verwendet die Handler-Klasse SLF4J, um einen Logger abzurufen.

Example src/main/java/example/HandlerS3.java – Protokollierung mit SLF4J

```
package example;

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;

import static org.apache.logging.log4j.CloseableThreadContext.put;


public class HandlerS3 implements RequestHandler<S3Event, String>{
    private static final Logger logger = LoggerFactory.getLogger(HandlerS3.class);

    @Override
    public String handleRequest(S3Event event, Context context) {
        for(var record : event.getRecords()) {
            try (var loggingCtx = put("awsRegion", record.getAwsRegion())) {
                loggingCtx.put("eventName", record.getEventName());
                loggingCtx.put("bucket", record.getS3().getBucket().getName());
                loggingCtx.put("key", record.getS3().getObject().getKey());

                logger.info("Handling s3 event");
            }
        }

        return "Ok";
    }
}
```

Es wird eine ähnliche Protokollausgabe wie die folgende erstellt:

Example Protokollformat

```
{
    "timestamp": "2023-11-15T16:56:00.815Z",
    "level": "INFO",
    "message": "Handling s3 event",
    "logger": "example.HandlerS3",
    "AWSRequestId": "0bced576-3936-4e5a-9dcd-db9477b77f97",
```

```
    "awsRegion": "eu-south-1",
    "bucket": "java-logging-test-input-bucket",
    "eventName": "ObjectCreated:Put",
    "key": "test-folder/"
}
```

Die Build-Konfiguration nimmt Laufzeitabhängigkeiten auf dem Lambda-Appender sowie SLF4J-Adapter und Implementierungsabhängigkeiten auf Log4j2 an.

Example build.gradle – Protokollierungsabhängigkeiten

```
dependencies {
    ...
    'com.amazonaws:aws-lambda-java-log4j2:[1.6.0,)',
    'com.amazonaws:aws-lambda-java-events:[3.11.3,)',
    'org.apache.logging.log4j:log4j-layout-template-json:[2.17.1,)',
    'org.apache.logging.log4j:log4j-slf4j2-impl:[2.19.0,)',
    ...
}
```

Wenn Sie Ihren Code vor Ort für Tests ausführen, ist das Kontextobjekt mit dem Lambda-Logger nicht verfügbar, und es gibt keine Anforderungs-ID, die der Lambda-Appender verwenden kann. Beispiele für Testkonfigurationen finden Sie in den Beispielanwendungen im nächsten Abschnitt.

Andere Tools und Bibliotheken

Powertools for AWS Lambda (Java) ist ein Entwickler-Toolkit zur Implementierung von Best Practices für Serverless und zur Steigerung der Entwicklergeschwindigkeit. Das Logging-Serviceprogramm bietet einen für Lambda optimierten Logger, der zusätzliche Informationen zum Funktionskontext all Ihrer Funktionen enthält, wobei die Ausgabe als JSON strukturiert ist. Mit diesem Serviceprogramm können Sie Folgendes tun:

- Erfassung von Schlüsselfeldern aus dem Lambda-Kontext, Kaltstart und Strukturen der Protokollierungsausgabe als JSON
- Protokollieren Sie Ereignisse von Lambda-Aufrufen, wenn Sie dazu aufgefordert werden (standardmäßig deaktiviert)
- Alle Protokolle nur für einen bestimmten Prozentsatz der Aufrufe über Protokollstichproben drucken (standardmäßig deaktiviert)
- Fügen Sie dem strukturierten Protokoll zu einem beliebigen Zeitpunkt zusätzliche Schlüssel hinzu

- Verwenden Sie einen benutzerdefinierten Protokollformatierer (Bring Your Own Formatter), um Protokolle in einer Struktur auszugeben, die mit dem Logging RFC Ihres Unternehmens kompatibel ist

Verwendung von Powertools für AWS Lambda (Java) und für strukturiertes Logging AWS SAM

Gehen Sie wie folgt vor, um eine Hello World Java-Beispielanwendung mit integrierten Powertools for AWS Lambda (Java) ~-Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu die. AWS SAM Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Java 11
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mit der Hello World Java-Vorlage.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type
 Zip --runtime java11 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name sam-app
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.095000
 INIT_START Runtime Version: java:11.v15    Runtime Version ARN: arn:aws:lambda:eu-
central-1::runtime:0a25e3e7a1cc9ce404bc435eeb2ad358d8fa64338e618d0c224fe509403583ca
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.114000
 Picked up JAVA_TOOL_OPTIONS: -XX:+TieredCompilation -XX:TieredStopAtLevel=1
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:34.793000
 Transforming org/apache/logging/log4j/core/lookup/JndiLookup
 (lambdainternal.CustomerClassLoader@1a6c5a9e)
```

```
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:35.252000
 START RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765 Version: $LATEST
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.531000 {
  "_aws": {
    "Timestamp": 1675416276051,
    "CloudWatchMetrics": [
      {
        "Namespace": "sam-app-powerools-java",
        "Metrics": [
          {
            "Name": "ColdStart",
            "Unit": "Count"
          }
        ],
        "Dimensions": [
          [
            "Service",
            "FunctionName"
          ]
        ]
      }
    ]
  },
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
 "Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "FunctionName": "sam-app-HelloWorldFunction-y9Iu1FLJJBGD",
  "functionVersion": "$LATEST",
  "ColdStart": 1.0,
  "Service": "service_undefined",
  "logStreamId": "2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81",
  "executionEnvironment": "AWS_Lambda_java11"
}
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.974000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.AWSXRayRecorder <init>
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000 Feb
 03, 2023 9:24:36 AM com.amazonaws.xray.config.DaemonConfiguration <init>
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:36.993000
 INFO: Environment variable AWS_XRAY_DAEMON_ADDRESS is set. Emitting to daemon on
 address XXXX.XXXX.XXXX.XXXX:2000.
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.331000
 09:24:37.294 [main] INFO  helloworld.App - {"version":null,"resource":"/
hello","path":"/hello/","httpMethod":"GET","headers":{"Accept":"*/
*","CloudFront-Forwarded-Proto":"https","CloudFront-Is-Desktop-
```

```
Viewer":"true","CloudFront-Is-Mobile-Viewer":"false","CloudFront-Is-
SmartTV-Viewer":"false","CloudFront-Is-Tablet-Viewer":"false","CloudFront-
Viewer-ASN":"16509","CloudFront-Viewer-Country":"IE","Host":"XXXX.execute-
api.eu-central-1.amazonaws.com","User-Agent":"curl/7.86.0","Via":"2.0
 f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)","X-Amz-
Cf-Id":"t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtiwV1Q==","X-
Amzn-Trace-Id":"Root=1-63dcd2d1-25f90b9d1c753a783547f4dd","X-Forwarded-
For":"XX.XXX.XXX.XX, XX.XXX.XXX.XX","X-Forwarded-Port":"443","X-
Forwarded-Proto":"https"},"multiValueHeaders":{"Accept":["*/
*"],"CloudFront-Forwarded-Proto":["https"],"CloudFront-Is-Desktop-Viewer":
["true"],"CloudFront-Is-Mobile-Viewer":["false"],"CloudFront-Is-SmartTV-
Viewer":["false"],"CloudFront-Is-Tablet-Viewer":["false"],"CloudFront-Viewer-
ASN":["16509"],"CloudFront-Viewer-Country":["IE"],"Host":["XXXX.execute-
api.eu-central-1.amazonaws.com"],"User-Agent":["curl/7.86.0"],"Via":["2.0
 f0300a9921a99446a44423d996042050.cloudfront.net (CloudFront)"],"X-Amz-
Cf-Id":["t9W5ByT11HaY33NM8YioKECn_4eMpNsOMPfEVRczD7T1RdhbtiwV1Q=="],"X-
Amzn-Trace-Id":["Root=1-63dcd2d1-25f90b9d1c753a783547f4dd"],"X-Forwarded-
For":["XXX, XXX"],"X-Forwarded-Port":["443"],"X-Forwarded-Proto":
["https"]},"queryStringParameters":null,"multiValueQueryStringParameters":null,"pathParamet
{"accountId":"XXX","stage":"Prod","resourceId":"at73a1","requestId":"ba09ecd2-
acf3-40f6-89af-fad32df67597","operationName":null,"identity":
{"cognitoIdentityPoolId":null,"accountId":null,"cognitoIdentityId":null,"caller":null,"apiK
hello","httpMethod":"GET","apiId":"XXX","path":"/Prod/
hello/","authorizer":null},"body":null,"isBase64Encoded":false}
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:37.351000
 09:24:37.351 [main] INFO  helloworld.App - Retrieving https://
checkip.amazonaws.com
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.313000 {
  "function_request_id": "7fcf1548-d2d4-41cd-a9a8-6ae47c51f765",
  "traceId":
 "Root=1-63dcd2d1-25f90b9d1c753a783547f4dd;Parent=e29684c1be352ce4;Sampled=1",
  "xray_trace_id": "1-63dcd2d1-25f90b9d1c753a783547f4dd",
  "functionVersion": "$LATEST",
  "Service": "service_undefined",
  "logStreamId": "2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81",
  "executionEnvironment": "AWS_Lambda_java11"
}
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.371000 END
 RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765
2023/02/03/[$LATEST]851411a899b545eea2cffeba4cfbec81 2023-02-03T09:24:39.371000
 REPORT RequestId: 7fcf1548-d2d4-41cd-a9a8-6ae47c51f765    Duration: 4118.98 ms
 Billed Duration: 4119 ms    Memory Size: 512 MB    Max Memory Used: 152 MB    Init
 Duration: 1155.47 ms
```

```
XRAY TraceId: 1-63dcd2d1-25f90b9d1c753a783547f4dd    SegmentId: 3a028fee19b895cb
 Sampled: true
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwalten der Protokollaufbewahrung

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um zu vermeiden, dass Protokolle auf unbestimmte Zeit gespeichert werden, löschen Sie die Protokollgruppe oder konfigurieren Sie einen Aufbewahrungszeitraum, nach dessen Ablauf die Protokolle CloudWatch automatisch gelöscht werden. Um die Aufbewahrung von Protokollen einzurichten, fügen Sie Ihrer AWS SAM Vorlage Folgendes hinzu:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der CloudWatch Konsole

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um

Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
```

```
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Beispielprotokolliercode

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung verschiedener Protokollierungskonfigurationen demonstrieren. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS SAM Vorlage und unterstützende Ressourcen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Die `java-basic`-Beispielanwendung zeigt eine minimale Protokollierungskonfiguration, die Protokollierungstests unterstützt. Der Handler-Code verwendet den `LambdaLogger`-Logger, der vom Kontextobjekt bereitgestellt wird. Für Tests verwendet die Anwendung eine benutzerdefinierte `TestLogger`-Klasse, die die `LambdaLogger`-Schnittstelle mit einem Log4j2-Logger implementiert. Es verwendet SLF4J als Fassade für die Kompatibilität mit dem SDK. AWS Protokollbibliotheken werden von der Build-Ausgabe ausgeschlossen, um das Bereitstellungspaket klein zu halten.

Instrumentierung von Java-Code in AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS -Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von zwei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) — Eine sichere, produktionsbereite und AWS unterstützte Distribution des (OTel) SDK. OpenTelemetry
- AWS X-Ray SDK for Java – Ein SDK zum Generieren und Senden von Nachverfolgungsdaten an X-Ray.
- Powertools for AWS Lambda (Java) — Ein Entwickler-Toolkit zur Implementierung von Best Practices für Serverless und zur Steigerung der Entwicklergeschwindigkeit.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda SDKs sind Teil einer eng integrierten Instrumentierungslösung von. AWS Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Ablaufverfolgung in X-Ray mit beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS -Distro für Open Telemetry und X-Ray-SDKs.

Sections

- Verwendung von Powertools für AWS Lambda (Java) und AWS SAM für die Ablaufverfolgung
- Verwendung von Powertools für AWS Lambda (Java) und AWS CDK für die Ablaufverfolgung
- Verwenden von ADOT zur Instrumentierung Ihrer Java-Funktionen

- Instrumentieren Sie mit dem X-Ray-SDK Ihre Java-Funktionen
- Aktivieren der Nachverfolgung mit der Lambda-Konsole
- Aktivieren der Nachverfolgung mit der Lambda-API
- Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation
- Interpretieren einer X-Ray-Nachverfolgung
- Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)
- X-Ray-Nachverfolgung in Beispielanwendungen (X-Ray-SDK)

Verwendung von Powertools für AWS Lambda (Java) und AWS SAM für die Ablaufverfolgung

Gehen Sie wie folgt vor, um eine Hello World Java-Beispielanwendung mit integrierten Powertools für AWS Lambda (Java) -Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu den. AWS SAM Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API Gateway Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Java 11
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mit der Hello World Java-Vorlage.

```
sam init --app-template hello-world-powertools-java --name sam-app --package-type
 Zip --runtime java11 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
New XRay Service Graph
  Start time: 2023-02-03 14:31:48+01:00
  End time: 2023-02-03 14:31:48+01:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-y9Iu1FLJJBGD -
 Edges: []
```

```
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 5.587
  Reference Id: 1 - client - sam-app-HelloWorldFunction-y9Iu1FLJJBGD - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 3] at (2023-02-03T14:31:48.500000) with id
 (1-63dd0cc4-3c869dec72a586875da39777) and duration (5.603s)
 - 5.587s - sam-app-HelloWorldFunction-y9Iu1FLJJBGD [HTTP: 200]
 - 4.053s - sam-app-HelloWorldFunction-y9Iu1FLJJBGD
   - 1.181s - Initialization
   - 4.037s - Invocation
     - 1.981s - ## handleRequest
       - 1.840s - ## getPageContents
   - 0.000s - Overhead
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwendung von Powertools für AWS Lambda (Java) und AWS CDK für die Ablaufverfolgung

Gehen Sie wie folgt vor, um eine Hello World Java-Beispielanwendung mit integrierten Powertools for AWS Lambda (Java) -Modulen herunterzuladen, zu erstellen und bereitzustellen. Verwenden Sie dazu den. AWS CDK Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API Gateway Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine Hello-World-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Java 11
- AWS CLI Version 2
- AWS CDK Ausführung 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS CDK Beispielanwendung bereit

1. Erstellen Sie ein Projektverzeichnis für Ihre neue Anwendung.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie die App.

```
cdk init app --language java
```

3. Erstellen Sie ein Maven-Projekt mit dem folgenden Befehl:

```
mkdir app
cd app
mvn archetype:generate -DgroupId=helloworld -DartifactId=Function -
DarchetypeArtifactId=maven-archetype-quickstart -DinteractiveMode=false
```

4. Öffnen Sie `pom.xml` im `hello-world\app\Function`-Verzeichnis und ersetzen Sie den vorhandenen Code durch den folgenden Code, der Abhängigkeiten und Maven-Plugins für Powertools enthält.

```
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/
maven-v4_0_0.xsd">
  <modelVersion>4.0.0</modelVersion>
  <groupId>helloworld</groupId>
  <artifactId>Function</artifactId>
  <packaging>jar</packaging>
```

```
  <version>1.0-SNAPSHOT</version>
  <name>Function</name>
  <url>http://maven.apache.org</url>
<properties>
    <maven.compiler.source>11</maven.compiler.source>
    <maven.compiler.target>11</maven.compiler.target>
    <log4j.version>2.17.2</log4j.version>
</properties>
    <dependencies>
        <dependency>
            <groupId>junit</groupId>
            <artifactId>junit</artifactId>
            <version>3.8.1</version>
            <scope>test</scope>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-tracing</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-metrics</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.lambda</groupId>
            <artifactId>powertools-logging</artifactId>
            <version>1.3.0</version>
        </dependency>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-core</artifactId>
            <version>1.2.2</version>
        </dependency>
        <dependency>
            <groupId>com.amazonaws</groupId>
            <artifactId>aws-lambda-java-events</artifactId>
            <version>3.11.1</version>
        </dependency>
  </dependencies>
<build>
    <plugins>
        <plugin>
```

```
            <groupId>org.codehaus.mojo</groupId>
            <artifactId>aspectj-maven-plugin</artifactId>
            <version>1.14.0</version>
            <configuration>
                <source>${maven.compiler.source}</source>
                <target>${maven.compiler.target}</target>
                <complianceLevel>${maven.compiler.target}</complianceLevel>
                <aspectLibraries>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-tracing</artifactId>
                    </aspectLibrary>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-metrics</artifactId>
                    </aspectLibrary>
                    <aspectLibrary>
                        <groupId>software.amazon.lambda</groupId>
                        <artifactId>powertools-logging</artifactId>
                    </aspectLibrary>
                </aspectLibraries>
            </configuration>
            <executions>
                <execution>
                    <goals>
                        <goal>compile</goal>
                    </goals>
                </execution>
            </executions>
        </plugin>
        <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-shade-plugin</artifactId>
                <version>3.4.1</version>
                <executions>
                    <execution>
                        <phase>package</phase>
                        <goals>
                            <goal>shade</goal>
                        </goals>
                        <configuration>
                            <transformers>
                                <transformer
```

```
 implementation="com.github.edwgiz.maven_shade_plugin.log4j2_cache_transformer.PluginsCache
                                </transformer>
                            </transformers>
                            <createDependencyReducedPom>false</
createDependencyReducedPom>
                            <finalName>function</finalName>

                        </configuration>
                    </execution>
                </executions>
                <dependencies>
                    <dependency>
                        <groupId>com.github.edwgiz</groupId>
                        <artifactId>maven-shade-plugin.log4j2-cachefile-
transformer</artifactId>
                        <version>2.15</version>
                    </dependency>
                </dependencies>
        </plugin>
    </plugins>
</build>
</project>
```

5. Erstellen Sie das `hello-world\app\src\main\resource`-Verzeichnis und erstellen Sie `log4j.xml` für die Protokollkonfiguration.

```
mkdir -p src/main/resource
cd src/main/resource
touch log4j.xml
```

6. Öffnen Sie `log4j.xml` und fügen Sie den folgenden Code hinzu.

```
<?xml version="1.0" encoding="UTF-8"?>
<Configuration>
    <Appenders>
        <Console name="JsonAppender" target="SYSTEM_OUT">
            <JsonTemplateLayout
 eventTemplateUri="classpath:LambdaJsonLayout.json" />
        </Console>
    </Appenders>
    <Loggers>
        <Logger name="JsonLogger" level="INFO" additivity="false">
```

```
            <AppenderRef ref="JsonAppender"/>
        </Logger>
        <Root level="info">
            <AppenderRef ref="JsonAppender"/>
        </Root>
    </Loggers>
</Configuration>
```

7. Öffnen Sie `App.java` aus dem `hello-world\app\Function\src\main\java\helloworld`-Verzeichnis und ersetzen Sie den vorhandenen Code durch den folgenden Code. Dies ist der Code für die Lambda-Funktion.

```
package helloworld;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.URL;
import java.util.HashMap;
import java.util.Map;
import java.util.stream.Collectors;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyRequestEvent;
import com.amazonaws.services.lambda.runtime.events.APIGatewayProxyResponseEvent;
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;
import software.amazon.lambda.powertools.logging.Logging;
import software.amazon.lambda.powertools.metrics.Metrics;
import software.amazon.lambda.powertools.tracing.CaptureMode;
import software.amazon.lambda.powertools.tracing.Tracing;

import static software.amazon.lambda.powertools.tracing.CaptureMode.*;

/**
 * Handler for requests to Lambda function.
 */
public class App implements RequestHandler<APIGatewayProxyRequestEvent,
 APIGatewayProxyResponseEvent> {
    Logger log = LogManager.getLogger(App.class);
```

```
    @Logging(logEvent = true)
    @Tracing(captureMode = DISABLED)
    @Metrics(captureColdStart = true)
    public APIGatewayProxyResponseEvent handleRequest(final
 APIGatewayProxyRequestEvent input, final Context context) {
        Map<String, String> headers = new HashMap<>();
        headers.put("Content-Type", "application/json");
        headers.put("X-Custom-Header", "application/json");

        APIGatewayProxyResponseEvent response = new APIGatewayProxyResponseEvent()
                .withHeaders(headers);
        try {
            final String pageContents = this.getPageContents("https://
checkip.amazonaws.com");
            String output = String.format("{ \"message\": \"hello world\",
 \"location\": \"%s\" }", pageContents);

            return response
                    .withStatusCode(200)
                    .withBody(output);
        } catch (IOException e) {
            return response
                    .withBody("{}")
                    .withStatusCode(500);
        }
    }
    @Tracing(namespace = "getPageContents")
    private String getPageContents(String address) throws IOException {
        log.info("Retrieving {}", address);
        URL url = new URL(address);
        try (BufferedReader br = new BufferedReader(new
 InputStreamReader(url.openStream()))) {
            return br.lines().collect(Collectors.joining(System.lineSeparator()));
        }
    }
}
```

8. Öffnen Sie `HelloWorldStack.java` aus dem `hello-world\src\main\java\com\myorg`-Verzeichnis und ersetzen Sie den vorhandenen Code durch den folgenden Code. Dieser Code verwendet Lambda Constructor und den ApiGatewayv2 Constructor, um eine REST-API und eine Lambda-Funktion zu erstellen.

```
package com.myorg;
```

```
import software.amazon.awscdk.*;
import software.amazon.awscdk.services.apigatewayv2.alpha.*;
import
 software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegration;
import
 software.amazon.awscdk.services.apigatewayv2.integrations.alpha.HttpLambdaIntegrationProps
import software.amazon.awscdk.services.lambda.Code;
import software.amazon.awscdk.services.lambda.Function;
import software.amazon.awscdk.services.lambda.FunctionProps;
import software.amazon.awscdk.services.lambda.Runtime;
import software.amazon.awscdk.services.lambda.Tracing;
import software.amazon.awscdk.services.logs.RetentionDays;
import software.amazon.awscdk.services.s3.assets.AssetOptions;
import software.constructs.Construct;

import java.util.Arrays;
import java.util.List;

import static java.util.Collections.singletonList;
import static software.amazon.awscdk.BundlingOutput.ARCHIVED;

public class HelloWorldStack extends Stack {
    public HelloWorldStack(final Construct scope, final String id) {
        this(scope, id, null);
    }

    public HelloWorldStack(final Construct scope, final String id, final StackProps
 props) {
        super(scope, id, props);

        List<String> functionPackagingInstructions = Arrays.asList(
                "/bin/sh",
                "-c",
                "cd Function " +
                        "&& mvn clean install " +
                        "&& cp /asset-input/Function/target/function.jar /asset-
output/"
        );
        BundlingOptions.Builder builderOptions = BundlingOptions.builder()
                .command(functionPackagingInstructions)
                .image(Runtime.JAVA_11.getBundlingImage())
                .volumes(singletonList(
```

```
                        // Mount local .m2 repo to avoid download all the
dependencies again inside the container
                        DockerVolume.builder()
                                .hostPath(System.getProperty("user.home") +
"/.m2/")
                                .containerPath("/root/.m2/")
                                .build()
                ))
                .user("root")
                .outputType(ARCHIVED);

        Function function = new Function(this, "Function", FunctionProps.builder()
                .runtime(Runtime.JAVA_11)
                .code(Code.fromAsset("app", AssetOptions.builder()
                        .bundling(builderOptions
                                .command(functionPackagingInstructions)
                                .build())
                        .build()))
                .handler("helloworld.App::handleRequest")
                .memorySize(1024)
                .tracing(Tracing.ACTIVE)
                .timeout(Duration.seconds(10))
                .logRetention(RetentionDays.ONE_WEEK)
                .build());

        HttpApi httpApi = new HttpApi(this, "sample-api", HttpApiProps.builder()
                .apiName("sample-api")
                .build());

        httpApi.addRoutes(AddRoutesOptions.builder()
                .path("/")
                .methods(singletonList(HttpMethod.GET))
                .integration(new HttpLambdaIntegration("function", function,
HttpLambdaIntegrationProps.builder()
                        .payloadFormatVersion(PayloadFormatVersion.VERSION_2_0)
                        .build()))
                .build());

        new CfnOutput(this, "HttpApi", CfnOutputProps.builder()
                .description("Url for Http Api")
                .value(httpApi.getApiEndpoint())
                .build());
    }
```

```
}
```

9. Öffnen Sie `pom.xml` aus dem `hello-world`-Verzeichnis und ersetzen Sie den vorhandenen Code durch den folgenden Code.

```
<?xml version="1.0" encoding="UTF-8"?>
<project xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://
maven.apache.org/xsd/maven-4.0.0.xsd"
         xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <modelVersion>4.0.0</modelVersion>

    <groupId>com.myorg</groupId>
    <artifactId>hello-world</artifactId>
    <version>0.1</version>

    <properties>
        <project.build.sourceEncoding>UTF-8</project.build.sourceEncoding>
        <cdk.version>2.70.0</cdk.version>
        <constructs.version>[10.0.0,11.0.0)</constructs.version>
        <junit.version>5.7.1</junit.version>
    </properties>

    <build>
        <plugins>
            <plugin>
                <groupId>org.apache.maven.plugins</groupId>
                <artifactId>maven-compiler-plugin</artifactId>
                <version>3.8.1</version>
                <configuration>
                    <source>1.8</source>
                    <target>1.8</target>
                </configuration>
            </plugin>

            <plugin>
                <groupId>org.codehaus.mojo</groupId>
                <artifactId>exec-maven-plugin</artifactId>
                <version>3.0.0</version>
                <configuration>
                    <mainClass>com.myorg.HelloWorldApp</mainClass>
                </configuration>
            </plugin>
```

```
        </plugins>
    </build>

    <dependencies>
        <!-- AWS Cloud Development Kit -->
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>aws-cdk-lib</artifactId>
            <version>${cdk.version}</version>
        </dependency>
        <dependency>
            <groupId>software.constructs</groupId>
            <artifactId>constructs</artifactId>
            <version>${constructs.version}</version>
        </dependency>
        <dependency>
          <groupId>org.junit.jupiter</groupId>
          <artifactId>junit-jupiter</artifactId>
          <version>${junit.version}</version>
          <scope>test</scope>
        </dependency>
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>apigatewayv2-alpha</artifactId>
            <version>${cdk.version}-alpha.0</version>
        </dependency>
        <dependency>
            <groupId>software.amazon.awscdk</groupId>
            <artifactId>apigatewayv2-integrations-alpha</artifactId>
            <version>${cdk.version}-alpha.0</version>
        </dependency>
    </dependencies>
</project>
```

10. Stellen Sie sicher, dass Sie sich im `hello-world`-Verzeichnis befinden, und stellen Sie Ihre Anwendung bereit.

```
cdk deploy
```

11. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name HelloWorldStack --query
 'Stacks[0].Outputs[?OutputKey==`HttpApi`].OutputValue' --output text
```

12. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

13. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
New XRay Service Graph
  Start time: 2023-02-03 14:59:50+00:00
  End time: 2023-02-03 14:59:50+00:00
  Reference Id: 0 - (Root) AWS::Lambda - sam-app-HelloWorldFunction-YBg8yfYtOc9j -
 Edges: [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.924
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-YBg8yfYtOc9j
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0.016
  Reference Id: 2 - client - sam-app-HelloWorldFunction-YBg8yfYtOc9j - Edges: [0]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0
```

```
XRay Event [revision 1] at (2023-02-03T14:59:50.204000) with id
 (1-63dd2166-434a12c22e1307ff2114f299) and duration (0.924s)
 - 0.924s - sam-app-HelloWorldFunction-YBg8yfYtOc9j [HTTP: 200]
 - 0.016s - sam-app-HelloWorldFunction-YBg8yfYtOc9j
   - 0.739s - Initialization
   - 0.016s - Invocation
     - 0.013s - ## lambda_handler
       - 0.000s - ## app.hello
   - 0.000s - Overhead
```

14. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
cdk destroy
```

Verwenden von ADOT zur Instrumentierung Ihrer Java-Funktionen

ADOT bietet vollständig verwaltete Lambda-Ebenen, die alles packen, was Sie zum Sammeln von Telemetriedaten mit dem OTel-SDK benötigen. Indem Sie diese Ebene verwenden, können Sie Ihre Lambda-Funktionen instrumentieren, ohne einen Funktionscode ändern zu müssen. Sie können Ihren Ebenen auch für die benutzerdefinierte Initialisierung von OTel konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Konfiguration für den ADOT Collector auf Lambda in der ADOT-Dokumentation.

Für Java-Laufzeiten können Sie zwischen zwei Ebenen wählen, die verbraucht werden sollen:

- AWS verwaltete Lambda-Schicht für ADOT Java (Auto-Instrumentation Agent) — Diese Schicht transformiert Ihren Funktionscode beim Start automatisch, um Tracing-Daten zu sammeln. Detaillierte Anweisungen, wie Sie diese Ebene zusammen mit dem ADOT-Java-Agenten verwenden können, finden Sie in der ADOT-Dokumentation unter AWS Distro for OpenTelemetry Lambda Support for Java (Auto-Instrumentation Agent).
- AWS verwaltete Lambda-Schicht für ADOT Java — Diese Schicht bietet auch eine integrierte Instrumentierung für Lambda-Funktionen, erfordert jedoch einige manuelle Codeänderungen, um das OTel SDK zu initialisieren. Eine ausführliche Anleitung zur Nutzung dieser Ebene finden Sie unter AWS Distro for OpenTelemetry Lambda Support for Java in der ADOT-Dokumentation.

Instrumentieren Sie mit dem X-Ray-SDK Ihre Java-Funktionen

Um Daten über Aufrufe Ihrer Funktion an andere Ressourcen und Services in Ihrer Anwendung aufzuzeichnen, können Sie Ihrer Build-Konfiguration das X-Ray-SDK für Java hinzufügen. Das folgende Beispiel zeigt eine Gradle-Build-Konfiguration, die die Bibliotheken enthält, die die automatische Instrumentierung von Clients aktivieren. AWS SDK for Java 2.x

Example build.gradle – Ablaufverfolgung von Abhängigkeiten

```
dependencies {
    implementation platform('software.amazon.awssdk:bom:2.16.1')
    implementation platform('com.amazonaws:aws-xray-recorder-sdk-bom:2.11.0')
    ...
    implementation 'com.amazonaws:aws-xray-recorder-sdk-core'
    implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk'
    implementation 'com.amazonaws:aws-xray-recorder-sdk-aws-sdk-v2-instrumentor'
    ...
}
```

Aktivieren Sie nach Hinzufügen der richtigen Abhängigkeiten die Nachverfolgung in der Konfiguration Ihrer Funktion über die Lambda-Konsole oder die API.

Aktivieren der Nachverfolgung mit der Lambda-Konsole

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

Aktivieren der Nachverfolgung mit der Lambda-API

Konfigurieren Sie die Ablaufverfolgung für Ihre Lambda-Funktion mit dem AWS CLI oder AWS SDK und verwenden Sie die folgenden API-Operationen:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Interpretieren einer X-Ray-Nachverfolgung

Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray. Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

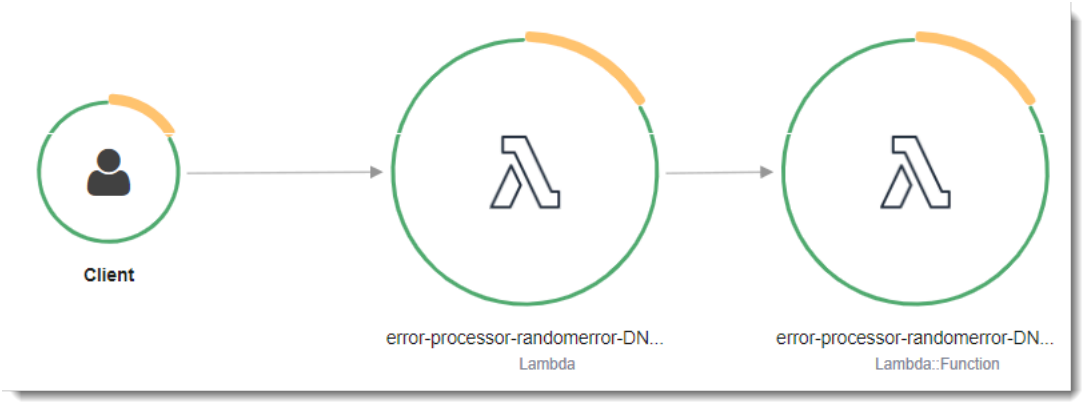
Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein

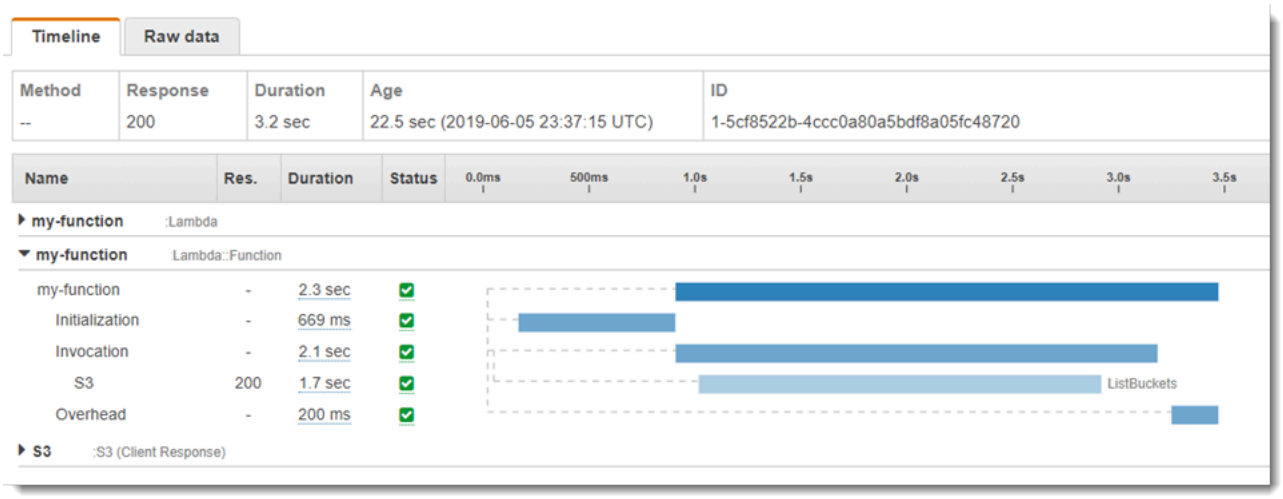
repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.
- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

> **Note**
>
> Zu den Lambda SnapStart-Funktionen gehört auch ein `Restore`-Teilsegment. Das Teilsegment `Restore` zeigt die Zeit an, die Lambda benötigt, um einen Snapshot wiederherzustellen, die Laufzeit (JVM) zu laden und vorhandene `afterRestore`-Laufzeit-Hooks auszuführen. Der Prozess der Wiederherstellung von Snapshots kann Zeit beinhalten, die für Aktivitäten außerhalb der MicroVM aufgewendet wird. Diese Zeit wird im `Restore`-Untersegment erfasst. Die Zeit, die Sie außerhalb der microVM für die Wiederherstellung eines Snapshots aufwenden, wird Ihnen nicht in Rechnung gestellt.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter AWS X-Ray SDK for Java im AWS X-Ray -Entwicklerhandbuch.

> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Laufzeitabhängigkeiten in einer Ebene speichern (X-Ray-SDK)

Wenn Sie das X-Ray-SDK verwenden, um AWS SDK-Clients Ihren Funktionscode zu instrumentieren, kann Ihr Bereitstellungspaket ziemlich umfangreich werden. Um Laufzeitabhängigkeiten bei jeder Aktualisierung des Funktionscodes zu vermeiden, verpacken Sie das X-Ray-SDK in einer Lambda-Ebene.

Das folgende Beispiel zeigt eine `AWS::Serverless::LayerVersion`-Ressource, die AWS SDK for Java und das X-Ray-SDK für Java speichert.

Example template.yml – Abhängigkeitenebene

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: build/distributions/blank-java.zip
      Tracing: Active
      Layers:
        - !Ref libs
      ...
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-java-lib
      Description: Dependencies for the blank-java sample app.
      ContentUri: build/blank-java-lib.zip
      CompatibleRuntimes:
        - java21
```

Bei dieser Konfiguration aktualisieren Sie die Bibliotheksebene nur, wenn Sie Ihre Laufzeitabhängigkeiten ändern. Da das Funktionsbereitstellungspaket nur Ihren Code enthält, kann dies dazu beitragen, die Upload-Zeiten zu reduzieren.

Das Erstellen einer Ebene für Abhängigkeiten erfordert Build-Konfigurationsänderungen, um das Layer-Archiv vor der Bereitstellung zu generieren. Ein funktionierendes Beispiel finden Sie in der Java-Basic-Beispielanwendung unter. GitHub

X-Ray-Nachverfolgung in Beispielanwendungen (X-Ray-SDK)

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung von X-Ray Tracing demonstrieren. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS SAM Vorlage und unterstützende Ressourcen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Für alle Beispielanwendungen ist die aktive Ablaufverfolgung für Lambda-Funktionen aktiviert. Die `s3-java` Anwendung zeigt beispielsweise die automatische Instrumentierung von AWS SDK for Java 2.x Clients, Segmentmanagement für Tests, benutzerdefinierte Untersegmente und die Verwendung von Lambda-Schichten zum Speichern von Laufzeitabhängigkeiten.

Java-Beispielanwendungen für AWS Lambda

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung von Java in demonstrieren AWS Lambda. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS CloudFormation Vorlage und unterstützende Ressourcen.

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Ausführen beliebter Java-Frameworks auf Lambda

- spring-cloud-function-samples — Ein Beispiel aus Spring, das zeigt, wie das Spring Cloud Function-Framework zur Erstellung von Lambda-Funktionen verwendet wird. AWS
- Serverlose Spring Boot-Anwendungsdemo — Ein Beispiel, das zeigt, wie eine typische Spring Boot-Anwendung in einer verwalteten Java-Laufzeit mit und ohne SnapStart oder als natives GraalVM-Image mit einer benutzerdefinierten Laufzeit eingerichtet wird.
- Serverlose Micronaut-Anwendungsdemo — Ein Beispiel, das zeigt, wie Micronaut in einer verwalteten Java-Laufzeit mit und ohne oder als natives SnapStart GraalVM-Image mit einer

benutzerdefinierten Laufzeit verwendet wird. Erfahren Sie mehr in den Micronaut/Lambda-Leitfäden.

- Serverlose Quarkus-Anwendungsdemo — Ein Beispiel, das zeigt, wie Quarkus in einer verwalteten Java-Laufzeit mit und ohne oder als natives GraalVM-Image mit einer SnapStart benutzerdefinierten Laufzeit verwendet werden kann. Weitere Informationen finden Sie im Quarkus/Lambda-Leitfaden und im Quarkus/-Leitfaden. SnapStart

Wenn Lambda-Funktionen in Java für Sie neu sind, beginnen mit den `java-basic`-Beispielen. Für erste Schritte mit Lambda-Ereignisquellen schauen Sie sich die `java-events`-Beispiele an. Beide Beispielsätze zeigen die Verwendung der Java-Bibliotheken, Umgebungsvariablen, des SDK und des SDK von Lambda. AWS AWS X-Ray Diese Beispiele erfordern nur eine minimale Einrichtung. Sie können sie in weniger als einer Minute von der Befehlszeile aus bereitstellen.

Erstellen von Lambda-Funktionen mit Go

Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie eine reine Betriebssystemlaufzeit (die `provided` Runtime-Familie), um Go-Funktionen für Lambda bereitzustellen.

Themen

Unterstützte Go-Laufzeiten

Die verwaltete Go 1.x-Laufzeit für Lambda ist veraltet. Wenn Sie Funktionen haben, die die Go 1.x-Laufzeit verwenden, müssen Sie Ihre Funktionen zu oder migrieren. `provided.al2023` `provided.al2` Die `provided.al2023` `provided.al2` Runtimes bieten mehrere Vorteile gegenüber`go1.x`, darunter Unterstützung für die Arm64-Architektur (AWS Graviton2-Prozessoren), kleinere Binärdateien und etwas schnellere Aufrufzeiten.

Für diese Migration sind keine Codeänderungen erforderlich. Die einzigen erforderlichen Änderungen betreffen die Erstellung Ihres Bereitstellungspakets sowie die Laufzeit, die Sie zur Erstellung Ihrer Funktion verwenden. Weitere Informationen finden Sie im Compute-Blog unter AWS Lambda Funktionen von der GO1.x-Laufzeit zur benutzerdefinierten Laufzeit auf Amazon Linux 2 migrieren.AWS

Nur OS

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Reine OS-Laufzeit	`provided.al2023`	Amazon Linux 2023			
Reine OS-Laufzeit	`provided.al2`	Amazon Linux 2			

Tools und Bibliotheken

Lambda stellt die folgenden Tools und Bibliotheken für die Go-Laufzeit bereit:

- AWS SDK for Go: Das offizielle AWS SDK für die Go-Programmiersprache.
- github.com/aws/aws-lambda-go/lambda: Die Implementierung des Lambda-Programmiermodells für Go. Dieses Paket wird von verwendet AWS Lambda , um Ihren Handler aufzurufen.
- github.com/aws/aws-lambda-go/lambdacontext: Hilfsprogramme für den Zugriff auf Informationen zum Kontext aus dem Kontext-Objekt.
- github.com/aws/aws-lambda-go/events: Diese Bibliothek bietet Typdefinitionen für gängige Integrationen von Ereignisquellen.
- github.com/aws/aws-lambda-go/cmd/build-lambda-zip: Mit diesem Tool kann unter Windows ein ZIP-Dateiarchiv erstellt werden.

Weitere Informationen finden Sie unter aws-lambda-go on. GitHub

Lambda stellt die folgenden Beispielanwendungen für die Go-Laufzeit bereit:

Lambda-Beispielanwendungen in Go

- go-al2: Eine Hello World-Funktion, die die öffentliche IP-Adresse zurückgibt. Diese App verwendet die benutzerdefinierte Laufzeit `provided.al2`.
- blank-go — Eine Go-Funktion, die die Verwendung der Go-Bibliotheken, der Protokollierung, der Umgebungsvariablen und des SDK von Lambda zeigt. AWS Diese App verwendet die Laufzeit `go1.x`.

Definieren Sie den Lambda-Funktionshandler in Go

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Eine Lambda-Funktion in Go wird als ausführbare Go-Datei erstellt. Ihr Lambda-Funktionscode muss das github.com/aws/aws-lambda-go/lambda-Paket umfassen, mit dem das Lambda-Programmiermodell für Go implementiert wird. Darüber hinaus müssen Sie Handler-Funktionscode und eine `main()`-Funktion implementieren.

Example Go-Lambda-Funktion

```
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/lambda"
)

type MyEvent struct {
 Name string `json:"name"`
}

func HandleRequest(ctx context.Context, event *MyEvent) (*string, error) {
 if event == nil {
  return nil, fmt.Errorf("received nil event")
 }
 message := fmt.Sprintf("Hello %s!", event.Name)
 return &message, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Hier ist eine Beispieleingabe für diese Funktion:

```
{
  "name": "Jane"
```

```
}
```

Beachten Sie Folgendes:

- Paket „main“: In Go muss das Paket mit `func main()` stets den Namen `main` haben.
- Importieren: Damit können Sie die Bibliotheken einschließen, die Ihre Lambda-Funktion erfordert. In diesem Fall sind dies:
  - context: AWS Lambda-Context-Objekt in Go.
  - Fmt: Das Formatierungs-Objekt in Go, das zur Formatierung des Rückgabewerts Ihrer Funktion verwendet wird.
  - github.com/aws/aws-lambda-go/lambda: Dies implementiert, wie zuvor erwähnt, das Lambda-Programmiermodell für Go.
- func HandleRequest (ctx context.Context, event *MyEvent) (*string, error): Dies ist die Signatur Ihres Lambda-Handlers. Es ist der Einstiegspunkt für Ihre Lambda-Funktion und enthält die Logik, die ausgeführt wird, wenn Ihre Funktion aufgerufen wird. Darüber hinaus geben die enthalten Parameter Folgendes an:
  - ctx context.Context: Stellt Laufzeitinformationen für Ihren Lambda-Funktionsaufruf bereit. `ctx` ist die Variable, die Sie deklarieren, um die verfügbaren Informationen über AWS Lambda-Context-Objekt in Go zu nutzen.
  - event * MyEvent: Dies ist ein Parameter mit dem Namen, auf den verweist. `event` `MyEvent` Es stellt die Eingabe für die Lambda-Funktion dar.
  - *string, error: Der Handler gibt zwei Werte zurück. Der erste ist ein Zeiger auf eine Zeichenfolge, die das Ergebnis der Lambda-Funktion enthält. Der zweite ist ein Fehlertyp, der `nil` ist, wenn kein Fehler vorliegt, und der standardmäßige Fehlerinformationen enthält, falls etwas schief geht.
  - return &message, nil: Gibt zwei Werte zurück. Der erste ist ein Zeiger auf eine Zeichenfolgennachricht, bei der es sich um eine Begrüßung handelt, die anhand des `Name`-Felds aus dem Eingabeereignis erstellt wurde. Der zweite Wert, `nil`, gibt an, dass bei der Funktion keine Fehler aufgetreten sind.
- func main(): Der Eintrittspunkt, von dem aus Ihr Lambda-Funktionscode ausgeführt wird. Diese Information ist erforderlich.

  Indem Sie `lambda.Start(HandleRequest)` zwischen den `func main(){}`-Code-Klammern hinzufügen, wird Ihre Lambda-Funktion ausgeführt. Laut den Standards der Go-Sprache muss sich die offene Klammer `{` direkt am Ende der `main`-Funktionssignatur befinden.

Benennung

provided.al2 and provided.al2023 Laufzeiten

Bei Go-Funktionen, die die Laufzeit `provided.al2` oder `provided.al2023` in einem ZIP-Bereitstellungspaket verwenden, muss die ausführbare Datei, die Ihren Funktionscode enthält, `bootstrap` heißen. Wenn Sie eine Funktion über eine ZIP-Datei bereitstellen, muss sich die `bootstrap`-Datei im Stammverzeichnis der ZIP-Datei befinden. Bei Go-Funktionen, die die Laufzeit `provided.al2` oder `provided.al2023` in einem Container-Image verwenden, kann die ausführbare Datei einen beliebigen Namen haben.

Für den Handler kann ein beliebiger Name verwendet werden. Sie können die Umgebungsvariable `_HANDLER` verwenden, um in Ihrem Code auf den Handler-Wert zu verweisen.

Laufzeit „go1.x“

Bei Go-Funktionen, die die Laufzeit `go1.x` verwenden, können sich die ausführbare Datei und der Handler einen beliebigen Namen teilen. Wenn Sie beispielsweise den Wert des Handlers auf `Handler` setzen, ruft Lambda die Funktion `main()` in der ausführbaren Datei `Handler` auf.

Um den Namen des Funktionshandlers in der Lambda-Konsole zu ändern, wählen Sie im Bereich Laufzeiteinstellungen die Option Bearbeiten.

Lambda-Funktions-Handler mit strukturierten Typen

Im obigen Beispiel handelte es sich beim Eingabetyp um eine einfache Zeichenfolge. Sie können jedoch auch strukturierte Ereignisse an Ihren Funktions-Handler übergeben:

```
package main

import (
 "fmt"
 "github.com/aws/aws-lambda-go/lambda"
)

type MyEvent struct {
 Name string `json:"What is your name?"`
 Age  int    `json:"How old are you?"`
}
```

```
type MyResponse struct {
 Message string `json:"Answer"`
}

func HandleLambdaEvent(event *MyEvent) (*MyResponse, error) {
 if event == nil {
  return nil, fmt.Errorf("received nil event")
 }
 return &MyResponse{Message: fmt.Sprintf("%s is %d years old!", event.Name,
 event.Age)}, nil
}

func main() {
 lambda.Start(HandleLambdaEvent)
}
```

Hier ist eine Beispieleingabe für diese Funktion:

```
{
    "What is your name?": "Jim",
    "How old are you?": 33
}
```

Die Antwort schaut wie folgt aus:

```
{
    "Answer": "Jim is 33 years old!"
}
```

Um exportiert werden, müssen Feldnamen in der Ereignisstruktur großgeschrieben werden. Weitere Informationen zum Umgang mit Ereignissen aus AWS Ereignisquellen finden Sie unter aws-lambda-go/events.

Gültige Handler-Signaturen

Sie haben bei der Erstellung eines Lambda-Funktions-Handlers in Go mehrere Möglichkeiten. Allerdings müssen die folgenden Regeln beachten:

- Der Handler muss eine Funktion sein.
- Der Handler kann zwischen 0 und 2 Argumente aufnehmen. Bei zwei Argumenten muss das erste Argument implementiere `context.Context`.

- Der Handler kann zwischen 0 und 2 Argumente zurückgeben. Bei einem einzigen Rückgabewert muss er implementiere `error`. Bei zwei Rückgabewerten muss der zweite Wert implementiere `error`.

Im Folgenden werden gültige Handler-Signaturen aufgeführt. `TIn` und `TOut` stellen Typen dar, die mit der Standardbibliothek encoding/json kompatibel sind. Weitere Informationen zur Deserialisierung dieser Typen finden Sie unter func Unmarshal.

- `func ()`
- `func () error`
- `func (TIn) error`
- `func () (TOut, error)`
- `func (context.Context) error`
- `func (context.Context, TIn) error`
- `func (context.Context) (TOut, error)`
- `func (context.Context, TIn) (TOut, error)`

Verwenden des globalen Zustands

Sie können globale Variablen deklarieren und ändern, die vom Handler-Code Ihrer Lambda-Funktion unabhängig sind. Darüber hinaus deklariert Ihr Handler möglicherweise eine `init`-Funktion, die ausgeführt wird, wenn Ihr Handler geladen wird. Dies verhält sich genauso wie in AWS Lambda Standard-Go-Programmen. Eine einzelne Instance Ihrer Lambda-Funktion behandelt nie mehrere Ereignisse gleichzeitig.

Example Go-Funktion mit globalen Variablen

> **Note**
>
> Dieser Code verwendet die AWS SDK for Go V2. Weitere Informationen finden Sie unter Erste Schritte mit der AWS SDK for Go V2.

```
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "log"
)

var invokeCount int
var myObjects []types.Object

func init() {
 // Load the SDK configuration
 cfg, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  log.Fatalf("Unable to load SDK config: %v", err)
 }

 // Initialize an S3 client
 svc := s3.NewFromConfig(cfg)

 // Define the bucket name as a variable so we can take its address
 bucketName := "DOC-EXAMPLE-BUCKET"
 input := &s3.ListObjectsV2Input{
  Bucket: &bucketName,
 }

 // List objects in the bucket
 result, err := svc.ListObjectsV2(context.TODO(), input)
 if err != nil {
  log.Fatalf("Failed to list objects: %v", err)
```

```
 }
 myObjects = result.Contents
}

func LambdaHandler(ctx context.Context) (int, error) {
 invokeCount++
 for i, obj := range myObjects {
  log.Printf("object[%d] size: %d key: %s", i, obj.Size, *obj.Key)
 }
 return invokeCount, nil
}

func main() {
 lambda.Start(LambdaHandler)
}
```

AWS Lambda-Context-Objekt in Go

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler. übergeben. Dieses Objekt stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Die Lambda-Kontextbibliothek bietet die folgenden globalen Variablen, Methoden und Eigenschaften.

Globale Variablen

- `FunctionName` – Der Name der Lambda-Funktion.
- `FunctionVersion` – Die Version der Funktion.
- `MemoryLimitInMB` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `LogGroupName` – Protokollgruppe für die Funktion.
- `LogStreamName` – Der Protokollstrom für die Funktionsinstance.

Context-Methoden

- `Deadline` – Gibt das Datum zurück, an dem eine Zeitüberschreitung für die Ausführung eintritt (in Unix-Millisekunden).

Context-Eigenschaften

- `InvokedFunctionArn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `AwsRequestID` – Der Bezeichner der Aufrufanforderung.
- `Identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
- `ClientContext` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.

Zugreifen auf Aufrufkontextinformationen

Lambda-Funktionen haben Zugriff auf Metadaten über ihre Umgebung und die Aufrufanforderung. Darauf kann unter Paketkontext zugegriffen werden. Falls Ihr Handler `context.Context` als Parameter umfasst, fügt Lambda Informationen über Ihre Funktion in der `Value`-Eigenschaft des

Kontexts ein. Beachten Sie, dass Sie die `lambdacontext`-Bibliothek importieren müssen, um auf die Inhalte des `context.Context`-Objekts zuzugreifen.

```
package main

import (
        "context"
        "log"
        "github.com/aws/aws-lambda-go/lambda"
        "github.com/aws/aws-lambda-go/lambdacontext"
)

func CognitoHandler(ctx context.Context) {
        lc, _ := lambdacontext.FromContext(ctx)
        log.Print(lc.Identity.CognitoIdentityPoolID)
}

func main() {
        lambda.Start(CognitoHandler)
}
```

Im obigen Beispiel `lc` ist die Variable, die verwendet wird, um die Informationen zu verarbeiten, die das Kontextobjekt erfasst hat und diese Informationen `log.Print(lc.Identity.CognitoIdentityPoolID)`druckt, in diesem Fall die CognitoIdentityPoolID.

Das folgende Beispiel bietet eine Einführung in die Verwendung der Kontextobjekte zur Überwachung der Abschlussdauer Ihrer Lambda-Funktion. Damit können Sie die Leistungserwartungen analysieren und Ihren Funktionscode bei Bedarf entsprechend anpassen.

```
package main

import (
        "context"
        "log"
        "time"
        "github.com/aws/aws-lambda-go/lambda"
)

func LongRunningHandler(ctx context.Context) (string, error) {

        deadline, _ := ctx.Deadline()
```

```
        deadline = deadline.Add(-100 * time.Millisecond)
        timeoutChannel := time.After(time.Until(deadline))

        for {

                select {

                case <- timeoutChannel:
                        return "Finished before timing out.", nil

                default:
                        log.Print("hello!")
                        time.Sleep(50 * time.Millisecond)
                }
        }
}

func main() {
        lambda.Start(LongRunningHandler)
}
```

Bereitstellen von Lambda-Go-Funktionen mit ZIP-Dateiarchiven

Der Code Ihrer AWS Lambda Funktion besteht aus Skripten oder kompilierten Programmen und deren Abhängigkeiten. Sie verwenden ein Bereitstellungspaket, um Ihren Funktionscode in Lambda bereitzustellen. Lambda unterstützt zwei Arten von Bereitstellungspaketen: Container-Images und ZIP-Dateiarchiven.

Auf dieser Seite wird beschrieben, wie Sie eine .zip-Datei als Bereitstellungspaket für die Go-Laufzeit erstellen und dann die .zip-Datei verwenden, um Ihren Funktionscode AWS Lambda mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) und AWS Serverless Application Model (AWS SAM) bereitzustellen.

Da Lambda POSIX-Dateiberechtigungen verwendet, müssen Sie möglicherweise Berechtigungen für den Bereitstellungspaketordner festlegen, bevor Sie das ZIP-Dateiarchiv erstellen.

Sections

Erstellen einer ZIP-Datei unter macOS und Linux

Im Folgenden wird beschrieben, wie Sie Ihre ausführbare Datei mithilfe des Befehls `go build` kompilieren und ein Bereitstellungspaket in Form einer ZIP-Datei für Lambda erstellen. Stellen Sie vor dem Kompilieren Ihres Codes sicher, dass Sie das Lambda-Paket von installiert haben. GitHub Dieses Modul stellt eine Implementierung der Laufzeitschnittstelle bereit, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet. Führen Sie den folgenden Befehl aus, um diese Bibliothek herunterzuladen.

```
go get github.com/aws/aws-lambda-go/lambda
```

Wenn Ihre Funktion das verwendet AWS SDK for Go, laden Sie den Standardsatz von SDK-Modulen zusammen mit allen AWS Service-API-Clients herunter, die für Ihre Anwendung erforderlich sind. Informationen zur Installation des SDK for Go finden Sie unter Erste Schritte mit der AWS SDK for Go V2.

Verwenden der bereitgestellten Runtime-Familie

Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie eine reine Betriebssystemlaufzeit (die `provided` Runtime-Familie), um Go-Funktionen für Lambda bereitzustellen.

So erstellen Sie ein ZIP-Bereitstellungspaket (macOS/Linux)

1. Kompilieren Sie Ihre ausführbare Datei in dem Projektverzeichnis, das die Datei `main.go` Ihrer Anwendung enthält. Beachten Sie Folgendes:

   - Die ausführbare Datei muss `bootstrap` heißen. Weitere Informationen finden Sie unter Benennung.
   - Legen Sie die Befehlssatzarchitektur des Ziels fest. Reine Betriebssystem-Laufzeiten unterstützen sowohl arm64 als auch x86_64.
   - Sie können das optionale Tag `lambda.norpc` verwenden, um die RPC-Komponente (Remote Procedure Call, Remoteprozeduraufruf) der Bibliothek lambda auszuschließen. Die RPC-Komponente ist nur erforderlich, wenn Sie die veraltete Go 1.x-Laufzeit verwenden. Durch Ausschließen der RPC-Komponente verringert sich die Größe des Bereitstellungspakets.

   arm64-Architektur:

   ```
   GOOS=linux GOARCH=arm64 go build -tags lambda.norpc -o bootstrap main.go
   ```

   x86_64-Architektur:

   ```
   GOOS=linux GOARCH=amd64 go build -tags lambda.norpc -o bootstrap main.go
   ```

2. (Optional) Möglicherweise müssen Sie Pakete mit Einstellung von `CGO_ENABLED=0` in Linux kompilieren:

   ```
   GOOS=linux GOARCH=arm64 CGO_ENABLED=0 go build -o bootstrap -tags lambda.norpc
    main.go
   ```

   Dieser Befehl erstellt ein stabiles Binärpaket für Standard-C-Bibliotheksversionen (`libc`), was auf Lambda und anderen Geräten unterschiedlich sein kann.
3. Erstellen Sie ein Bereitstellungspaket, indem Sie die ausführbare Datei in eine ZIP-Datei packen.

```
zip myFunction.zip bootstrap
```

> **Note**
>
> Fügen Sie die `bootstrap`-Datei dem Stamm der ZIP-Datei hinzu.

4. Erstellen der -Funktion Beachten Sie Folgendes:

   - Die Binärdatei muss `bootstrap` benannt werden, aber der Handlername kann beliebig sein. Weitere Informationen finden Sie unter Benennung.
   - Die `--architectures`-Option ist nur bei Verwendung von „arm64“ erforderlich. Der Standardwert ist „x86_64“.
   - Geben Sie für `--role` den Amazon-Ressourcennamen (ARN) der Ausführungsrolle an.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--architectures arm64 \
--role arn:aws:iam::111122223333:role/lambda-ex \
--zip-file fileb://myFunction.zip
```

Erstellen einer ZIP-Datei unter Windows

Die folgenden Schritte zeigen, wie Sie das build-lambda-zipTool für Windows von herunterladen GitHub, Ihre ausführbare Datei kompilieren und ein ZIP-Bereitstellungspaket erstellen.

> **Note**
>
> Falls noch nicht geschehen, müssen Sie git installieren und die ausführbare `git`-Datei Ihrer Windows- %PATH%-Umgebungsvariable hinzufügen.

Stellen Sie vor dem Kompilieren Ihres Codes sicher, dass Sie die Lambda-Bibliothek von installiert haben. GitHub Führen Sie den folgenden Befehl aus, um diese Bibliothek herunterzuladen.

```
go get github.com/aws/aws-lambda-go/lambda
```

Wenn Ihre Funktion das verwendet AWS SDK for Go, laden Sie den Standardsatz von SDK-Modulen zusammen mit allen AWS Service-API-Clients herunter, die für Ihre Anwendung erforderlich sind. Informationen zur Installation des SDK for Go finden Sie unter Erste Schritte mit der AWS SDK for Go V2.

Verwenden der bereitgestellten Runtime-Familie

Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie eine reine Betriebssystemlaufzeit (die `provided` Runtime-Familie), um Go-Funktionen für Lambda bereitzustellen.

So erstellen Sie ein ZIP-Bereitstellungspaket (Windows)

1. Laden Sie das build-lambda-zipTool von herunter. GitHub

   ```
   go install github.com/aws/aws-lambda-go/cmd/build-lambda-zip@latest
   ```

2. Verwenden Sie das Tool aus Ihrer `GOPATH`, um eine ZIP-Datei zu erstellen. Bei einer Go-Standardinstallation befindet sich das Tool in der Regel unter `%USERPROFILE%\Go\bin`. Navigieren Sie andernfalls an den Installationsort der Go-Laufzeit und führen Sie einen der folgenden Schritte aus:

   cmd.exe

   Verwenden Sie in „cmd.exe“ je nach Befehlssatzarchitektur des Ziels eine der folgenden Optionen. Nur Betriebssystem-Laufzeiten unterstützen sowohl arm64 als auch x86_64.

   Sie können das optionale Tag `lambda.norpc` verwenden, um die RPC-Komponente (Remote Procedure Call, Remoteprozeduraufruf) der Bibliothek lambda auszuschließen. Die RPC-Komponente ist nur erforderlich, wenn Sie die veraltete Go 1.x-Laufzeit verwenden. Durch Ausschließen der RPC-Komponente verringert sich die Größe des Bereitstellungspakets.

   Example für die x86_64-Architektur

   ```
   set GOOS=linux
   set GOARCH=amd64
   set CGO_ENABLED=0
   go build -tags lambda.norpc -o bootstrap main.go
   ```

```
%USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

Example für die arm64-Architektur

```
set GOOS=linux
set GOARCH=arm64
set CGO_ENABLED=0
go build -tags lambda.norpc -o bootstrap main.go
%USERPROFILE%\Go\bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

PowerShell

Führen Sie in PowerShell, abhängig von Ihrer Ziel-Befehlssatzarchitektur, einen der folgenden Schritte aus. Reine Betriebssystem-Laufzeiten unterstützen sowohl arm64 als auch x86_64.

Sie können das optionale Tag `lambda.norpc` verwenden, um die RPC-Komponente (Remote Procedure Call, Remoteprozeduraufruf) der Bibliothek lambda auszuschließen. Die RPC-Komponente ist nur erforderlich, wenn Sie die veraltete Go 1.x-Laufzeit verwenden. Durch Ausschließen der RPC-Komponente verringert sich die Größe des Bereitstellungspakets.

x86_64-Architektur:

```
$env:GOOS = "linux"
$env:GOARCH = "amd64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

arm64-Architektur:

```
$env:GOOS = "linux"
$env:GOARCH = "arm64"
$env:CGO_ENABLED = "0"
go build -tags lambda.norpc -o bootstrap main.go
~\Go\Bin\build-lambda-zip.exe -o myFunction.zip bootstrap
```

3. Erstellen der -Funktion Beachten Sie Folgendes:

- Die Binärdatei muss `bootstrap` benannt werden, aber der Handlername kann beliebig sein. Weitere Informationen finden Sie unter Benennung.
- Die `--architectures`-Option ist nur bei Verwendung von „arm64“ erforderlich. Der Standardwert ist „x86_64“.
- Geben Sie für `--role` den Amazon-Ressourcennamen (ARN) der Ausführungsrolle an.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--architectures arm64 \
--role arn:aws:iam::111122223333:role/lambda-ex \
--zip-file fileb://myFunction.zip
```

Go Lambda-Funktionen mithilfe von ZIP-Dateien erstellen und aktualisieren

Nach der Erstellung Ihres ZIP-Bereitstellungspakets können Sie es verwenden, um eine neue Lambda-Funktion zu erstellen oder eine vorhandene zu aktualisieren. Sie können Ihr .zip-Paket mithilfe der Lambda-Konsole, der und der AWS Command Line Interface Lambda-API bereitstellen. Sie können Lambda-Funktionen auch mit AWS Serverless Application Model (AWS SAM) und AWS CloudFormation erstellen und aktualisieren.

Die maximale Größe eines ZIP-Bereitstellungspakets für Lambda beträgt 250 MB (entpackt). Beachten Sie, dass dieser Grenzwert für die kombinierte Größe aller hochgeladenen Dateien gilt, einschließlich aller Lambda-Ebenen.

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Schreibweise von Linux-Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen () für Verzeichnisse und ausführbare Dateien. rwxr-xr-x

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Konsole

Eine neue Funktion müssen Sie zuerst in der Konsole erstellen und dann Ihr ZIP-Archiv hochladen. Zum Aktualisieren einer bestehenden Funktion öffnen Sie die Seite für Ihre Funktion und gehen dann genauso vor, um Ihre aktualisierte ZIP-Datei hinzuzufügen.

Bei einer ZIP-Datei mit unter 50 MB können Sie eine Funktion erstellen oder aktualisieren, indem Sie die Datei direkt von Ihrem lokalen Computer hochladen. Bei ZIP-Dateien mit einer Größe von mehr als 50 MB müssen Sie Ihr Paket zuerst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3-Bucket mithilfe von finden Sie unter Erste Schritte mit Amazon S3. AWS Management Console Informationen zum Hochladen von Dateien mit dem AWS CLI finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch.

> **Note**
>
> Sie können eine vorhandene Container-Image-Funktion nicht konvertieren, um ein ZIP-Archiv zu verwenden. Sie müssen eine neue Funktion erstellen.

So erstellen Sie eine neue Funktion (Konsole)

1. Öffnen Sie die Funktionsseite der Lambda-Konsole und wählen Sie Funktion erstellen aus.
2. Wählen Sie Author from scratch aus.
3. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie als Funktionsname den Namen Ihrer Funktion ein.
   b. Wählen Sie unter Runtime (Laufzeit) `provided.al2023` aus.
4. (Optional) Erweitern Sie unter Berechtigungen die Option Standardausführungsrolle ändern. Sie können eine neue Ausführungsrolle erstellen oder eine vorhandene Rolle verwenden.
5. Wählen Sie Funktion erstellen. Lambda erstellt eine grundlegende „Hello World“-Funktion mit der von Ihnen gewählten Laufzeit.

So laden Sie ein ZIP-Archiv von Ihrem lokalen Computer hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie die ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie die ZIP-Datei aus.
5. Laden Sie die ZIP-Datei wie folgt hoch:
   a. Wählen Sie Hochladen und dann Ihre ZIP-Datei in der Dateiauswahl aus.
   b. Klicken Sie auf Open.
   c. Wählen Sie Speichern.

So laden Sie ein ZIP-Archiv aus einem Amazon-S3-Bucket hoch (Konsole)

1. Wählen Sie auf der Funktionsseite der Lambda-Konsole die Funktion aus, für die Sie eine neue ZIP-Datei hochladen möchten.
2. Wählen Sie die Registerkarte Code aus.
3. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
4. Wählen Sie den Amazon-S3-Speicherort aus.
5. Fügen Sie die Amazon-S3-Link-URL Ihrer ZIP-Datei ein und wählen Sie Speichern aus.

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien mithilfe der AWS CLI

Sie können die AWS CLI verwenden, um eine neue Funktion zu erstellen oder eine vorhandene unter Verwendung einer ZIP-Datei zu aktualisieren. Verwenden Sie die Erstellungsfunktion und die update-function-codeBefehle, um Ihr .zip-Paket bereitzustellen. Wenn Ihre ZIP-Datei kleiner als 50 MB ist, können Sie das ZIP-Paket von einem Dateispeicherort auf Ihrem lokalen Build-Computer hochladen. Bei größeren Dateien müssen Sie Ihr ZIP-Paket aus einem Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

> **Note**
>
> Wenn Sie Ihre ZIP-Datei mithilfe von aus einem Amazon S3 S3-Bucket hochladen AWS CLI, muss sich der Bucket im selben Verzeichnis befinden AWS-Region wie Ihre Funktion.

Um eine neue Funktion mithilfe einer .zip-Datei mit dem zu erstellen AWS CLI, müssen Sie Folgendes angeben:

- Den Namen Ihrer Funktion (`--function-name`)
- Die Laufzeit Ihrer Funktion (`--runtime`)
- Den Amazon-Ressourcennamen (ARN) der Ausführungsrolle der Funktion (`--role`).
- Den Namen der Handler-Methode in Ihrem Funktionscode (`--handler`)

Sie müssen auch den Speicherort Ihrer ZIP-Datei angeben. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigte `--code`-Option. Sie müssen den `S3ObjectVersion`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda create-function --function-name myFunction \
--runtime provided.al2023 --handler bootstrap \
--role arn:aws:iam::111122223333:role/service-role/my-lambda-role \
--code S3Bucket=DOC-EXAMPLE-BUCKET,S3Key=myFileName.zip,S3ObjectVersion=myObjectVersion
```

Um eine vorhandene Funktion mit der CLI zu aktualisieren, geben Sie den Namen Ihrer Funktion unter Verwendung des `--function-name`-Parameters an. Sie müssen auch den Speicherort der ZIP-Datei angeben, die Sie zum Aktualisieren Ihres Funktionscodes verwenden möchten. Befindet sich Ihre ZIP-Datei in einem Ordner auf Ihrem lokalen Build-Computer, verwenden Sie die `--zip-file`-Option, um den Dateipfad anzugeben, wie im folgenden Beispielbefehl gezeigt.

```
aws lambda update-function-code --function-name myFunction \
--zip-file fileb://myFunction.zip
```

Zur Angabe des Speicherorts der ZIP-Datei in einem Amazon-S3-Bucket verwenden Sie die im folgenden Beispielbefehl gezeigten `--s3-bucket`- und `--s3-key`-Optionen. Sie müssen den `--s3-object-version`-Parameter nur für versionierte Objekte verwenden.

```
aws lambda update-function-code --function-name myFunction \
--s3-bucket DOC-EXAMPLE-BUCKET --s3-key myFileName.zip --s3-object-version myObject
 Version
```

Erstellen und Aktualisieren von Funktionen mit ZIP-Dateien unter Verwendung der Lambda-API

Um Funktionen zu erstellen und zu konfigurieren, die ein ZIP-Dateiarchiv verwenden, verwenden Sie die folgenden API-Operationen:

- CreateFunction
- UpdateFunctionCode

Funktionen mit ZIP-Dateien erstellen und aktualisieren mit AWS SAM

Das AWS Serverless Application Model (AWS SAM) ist ein Toolkit, das dabei hilft, den Prozess der Erstellung und Ausführung serverloser Anwendungen zu optimieren. AWS Sie definieren die Ressourcen für Ihre Anwendung in einer YAML- oder JSON-Vorlage und verwenden die AWS SAM Befehlszeilenschnittstelle (AWS SAM CLI), um Ihre Anwendungen zu erstellen, zu verpacken und bereitzustellen. Wenn Sie eine Lambda-Funktion aus einer AWS SAM Vorlage erstellen, AWS SAM wird automatisch ein ZIP-Bereitstellungspaket oder ein Container-Image mit Ihrem Funktionscode und allen von Ihnen angegebenen Abhängigkeiten erstellt. Weitere Informationen zur Verwendung AWS SAM zum Erstellen und Bereitstellen von Lambda-Funktionen finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model Entwicklerhandbuch.

Sie können es auch verwenden AWS SAM , um eine Lambda-Funktion mithilfe eines vorhandenen ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion zu erstellen AWS SAM, können Sie Ihre ZIP-Datei in einem Amazon S3 S3-Bucket oder in einem lokalen Ordner auf Ihrem Build-Computer speichern. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS SAM Vorlage spezifiziert die `AWS::Serverless::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `CodeUri`- auf die Amazon S3 S3-URI, den Pfad zum lokalen Ordner oder FunctionCodeObjekt des Funktionscodes gesetzt
- `Runtime` – festlegen auf die gewünschte Laufzeit

Wenn Ihre ZIP-Datei größer als 50 MB ist, müssen Sie sie nicht zuerst in einen Amazon S3 S3-Bucket hochladen. AWS SAM AWS SAM kann .zip-Pakete bis zur maximal zulässigen Größe von 250 MB (entpackt) von einem Speicherort auf Ihrem lokalen Build-Computer hochladen.

Weitere Informationen zum Bereitstellen von Funktionen mithilfe der ZIP-Datei in finden Sie AWS::Serverless::Functionim AWS SAM Entwicklerhandbuch.AWS SAM

Beispiel: Wird verwendet AWS SAM , um eine Go-Funktion mit der bereitgestellten.al2023 zu erstellen

1. Erstellen Sie eine AWS SAM Vorlage mit den folgenden Eigenschaften:

   - BuildMethod: Gibt den Compiler für Ihre Anwendung an. Verwenden Sie `go1.x`.
   - Runtime: Verwenden Sie `provided.al2023`.
   - CodeUri: Geben Sie den Pfad zu Ihrem Code ein.
   - Architectures: Verwenden Sie `[arm64]` für die arm64-Architektur. Verwenden Sie für die x86_64-Befehlssatzarchitektur die Option `[amd64]` oder entfernen Sie die Eigenschaft `Architectures`.

   Example template.yaml

   ```
   AWSTemplateFormatVersion: '2010-09-09'
   Transform: 'AWS::Serverless-2016-10-31'
   Resources:
     HelloWorldFunction:
       Type: AWS::Serverless::Function
       Metadata:
         BuildMethod: go1.x
       Properties:
   ```

```
      CodeUri: hello-world/ # folder where your main program resides
      Handler: bootstrap
      Runtime: provided.al2023
      Architectures: [arm64]
```

2. Verwenden Sie den Befehl sam build, um die ausführbare Datei zu kompilieren.

```
sam build
```

3. Verwenden Sie den Befehl sam deploy, um die Funktion in Lambda bereitzustellen.

```
sam deploy --guided
```

Funktionen mit ZIP-Dateien erstellen und aktualisieren mit AWS CloudFormation

Sie können verwenden AWS CloudFormation , um eine Lambda-Funktion mithilfe eines ZIP-Dateiarchivs zu erstellen. Um eine Lambda-Funktion aus einer ZIP-Datei zu erstellen, müssen Sie Ihre Datei zunächst in einen Amazon-S3-Bucket hochladen. Anweisungen zum Hochladen einer Datei in einen Amazon S3 S3-Bucket mithilfe von finden Sie unter Objekte verschieben im AWS CLI Benutzerhandbuch. AWS CLI

In Ihrer AWS CloudFormation Vorlage spezifiziert die `AWS::Lambda::Function` Ressource Ihre Lambda-Funktion. Legen Sie in dieser Ressource die folgenden Eigenschaften fest, um eine Funktion zu erstellen, die als ZIP-Datei-Archiv definiert ist:

- `PackageType` – festlegen auf `Zip`
- `Code` – Geben Sie den Namen des Amazon-S3-Buckets und den ZIP-Dateinamen in die Felder `S3Bucket` und `S3Key` ein
- `Runtime` – festlegen auf die gewünschte Laufzeit

Die AWS CloudFormation generierte ZIP-Datei darf 4 MB nicht überschreiten. Weitere Informationen zur Bereitstellung von Funktionen mithilfe der ZIP-Datei finden Sie AWS::Lambda::Functionim AWS CloudFormation Benutzerhandbuch. AWS CloudFormation

Erstellen einer Go-Ebene für Ihre Abhängigkeiten

> **Note**
>
> Die Verwendung von Ebenen mit Funktionen in einer kompilierten Sprache wie Go bietet möglicherweise nicht den gleichen Nutzen wie in einer interpretierten Sprache wie Python. Da es sich bei Go um eine kompilierte Sprache handelt, müssen Ihre Funktionen während der Initialisierungsphase alle freigegebenen Baugruppen manuell in den Speicher laden, was die Kaltstartzeiten verlängern kann. Stattdessen empfehlen wir, den freigegebenen Code bei der Kompilierung einzuschließen, um die Vorteile der integrierten Compiler-Optimierungen zu nutzen.

Die Anweisungen in diesem Abschnitt zeigen Ihnen, wie Sie Ihre Abhängigkeiten in eine Ebene einschließen.

Lambda erkennt automatisch alle Bibliotheken im `/opt/lib`-Verzeichnis und alle Binärdateien im `/opt/bin`-Verzeichnis. Um sicherzustellen, dass Lambda den Inhalt Ihrer Ebene korrekt findet, erstellen Sie eine Ebene mit der folgenden Struktur:

```
custom-layer.zip
# lib
    | lib_1
    | lib_2
# bin
    | bin_1
    | bin_2
```

Nachdem Sie Ihre Ebene gebündelt haben, sehen Sie sich the section called “Erstellen und Löschen von Ebenen” und the section called “Hinzufügen von Ebenen” an, um die Einrichtung Ihrer Ebene abzuschließen.

Bereitstellen von Go-Lambda-Funktionen mit Container-Images

Es gibt zwei Möglichkeiten, ein Container-Image für eine Go Lambda-Funktion zu erstellen:

- Verwenden Sie ein reines AWS Betriebssystem-Basis-Image

  Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie ein Basis-Image nur für das Betriebssystem, um Go-Images für Lambda zu erstellen. Um das Image mit Lambda kompatibel zu machen, müssen Sie das `aws-lambda-go/lambda`-Paket in das Image aufnehmen.
- Verwenden Sie ein Image, das nicht zur Basisversion gehört AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie das `aws-lambda-go/lambda`-Paket in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

AWS Basis-Images für die Bereitstellung von Go-Funktionen

Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie ein reines Betriebssystem-Basisimage, um Go-Funktionen für Lambda bereitzustellen.

Nur OS

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
Reine OS-Laufzeit	`provided.al2023`	Amazon Linux 2023			
Reine OS-Laufzeit	`provided.al2`	Amazon Linux 2			

Öffentliche Galerie der Registry von Amazon Elastic Container: gallery.ecr.aws/lambda/provided

Laufzeitschnittstellen-Clients von Go

Das `aws-lambda-go/lambda`-Paket enthält eine Implementierung der Laufzeitschnittstelle. Beispiele für die Verwendung von `aws-lambda-go/lambda` in Ihrem Image finden Sie unter Verwenden Sie ein reines AWS Betriebssystem-Basis-Image oder Verwenden Sie ein Image, das nicht zur Basisversion gehört AWS.

Verwenden Sie ein reines AWS Betriebssystem-Basis-Image

Go wird anders implementiert als andere verwaltete Laufzeiten. Da Go nativ zu einer ausführbaren Binärdatei kompiliert wird, ist keine spezielle Sprachlaufzeit erforderlich. Verwenden Sie ein Basis-Image nur für das Betriebssystem, um Container-Images für Go-Funktionen zu erstellen.

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
al2023	Reine OS-Laufzeit	Amazon Linux 2023	Dockerfile für reine Betriebssystem-Runtime aktiviert GitHub	
al2	Reine OS-Laufzeit	Amazon Linux 2	Dockerfile für Runtime nur für Betriebssystem aktiviert GitHub	

Weitere Informationen zu diesen Basis-Images finden Sie in der öffentlichen Amazon-ECR-Galerie unter provided.

Sie müssen das Paket aws-lambda-go/lambda in Ihren Go-Handler aufnehmen. Dieses Paket implementiert das Programmiermodell für Go, einschließlich der Laufzeitschnittstelle.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Go
- Docker
- AWS Command Line Interface () Version 2 AWS CLI

Erstellen eines Images aus dem Basis-Image „provided.al2023“

So erstellen und implementieren Sie eine Go-Funktion mit dem **`provided.al2023`**-Basis-Image.

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir hello
cd hello
```

2. Initialisieren Sie ein neues Go-Modul.

```
go mod init example.com/hello-world
```

3. Fügen Sie die Lambda-Bibliothek als Abhängigkeit Ihres neuen Moduls hinzu.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Erstellen Sie eine Datei namens `main.go` und öffnen Sie diese dann in einem Text-Editor. Dies ist der Code für die Lambda-Funktion. Sie können den folgenden Beispielcode zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.

```
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
```

```
)

func handler(ctx context.Context, event events.APIGatewayProxyRequest)
 (events.APIGatewayProxyResponse, error) {
 response := events.APIGatewayProxyResponse{
  StatusCode: 200,
  Body:       "\"Hello from Lambda!\"",
 }
 return response, nil
}

func main() {
 lambda.Start(handler)
}
```

5. Verwenden Sie einen Texteditor, um ein Dockerfile in Ihrem Projektverzeichnis zu erstellen. Die folgende Beispiel-Docker-Datei verwendet eine mehrstufige Entwicklung. Dadurch können Sie in jedem Schritt ein anderes Basis-Image verwenden. Sie können ein Image verwenden, z. B. ein Go-Basis-Image, um Ihren Code zu kompilieren und die ausführbare Binärdatei zu erstellen. Sie können dann ein anderes Image verwenden, z. B. `provided.al2023` in der `FROM`-Abschlusserklärung, um das Image zu definieren, das Sie für Lambda bereitstellen. Der Build-Prozess ist vom endgültigen Bereitstellungs-Image getrennt, so dass das endgültige Image nur die Dateien enthält, die zum Ausführen der Anwendung benötigt werden.

   Sie können das optionale Tag `lambda.norpc` verwenden, um die RPC-Komponente (Remote Procedure Call, Remoteprozeduraufruf) der Bibliothek lambda auszuschließen. Die RPC-Komponente ist nur erforderlich, wenn Sie die veraltete Go 1.x-Runtime verwenden. Durch Ausschließen der RPC-Komponente verringert sich die Größe des Bereitstellungspakets.

   Example – Mehrstufige Docker-Datei

   > **Note**
   >
   > Stellen Sie sicher, dass die Version von Go, die Sie in der Docker-Datei angeben (z. B. `golang:1.20`), dieselbe Version von Go ist, mit der Sie Ihre Anwendung erstellt haben.

```
FROM golang:1.20 as build
WORKDIR /helloworld
# Copy dependencies list
```

```
COPY go.mod go.sum ./
# Build with optional lambda.norpc tag
COPY main.go .
RUN go build -tags lambda.norpc -o main main.go
# Copy artifacts to a clean image
FROM public.ecr.aws/lambda/provided:al2023
COPY --from=build /helloworld/main ./main
ENTRYPOINT [ "./main" ]
```

6. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um Ihr Image lokal zu testen. Der Laufzeit-Schnittstellen-Emulator ist im `provided.al2023`-Basis-Image enthalten.

So führen Sie den Laufzeit-Schnittstellen-Emulator auf Ihrem lokalen Computer aus

1. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.
   - `./main` ist `ENTRYPOINT` aus Ihrem Dockerfile.

```
docker run -d -p 9000:8080 \
--entrypoint /usr/local/bin/aws-lambda-rie \
docker-image:test ./main
```

Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

2. Veröffentlichen Sie in einem neuen Terminalfenster ein Ereignis mit einem curl-Befehl an den folgenden Endpunkt:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Für einige Funktionen ist möglicherweise eine JSON-Nutzlast erforderlich. Beispiel:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

3. Die Container-ID erhalten.

```
docker ps
```

4. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

```
aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

```
aws ecr create-repository --repository-name hello-world --region us-east-1 --image-scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
```

> **Note**
>
> Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

Wenn erfolgreich, sehen Sie eine Antwort wie diese:

```
{
    "repository": {
        "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-world",
        "registryId": "111122223333",
        "repositoryName": "hello-world",
        "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world",
        "createdAt": "2023-03-09T10:39:01+00:00",
        "imageTagMutability": "MUTABLE",
        "imageScanningConfiguration": {
            "scanOnPush": true
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:

   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
```

```
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

Verwenden Sie ein Image, das nicht zur Basisversion gehört AWS

Sie können ein Container-Image für Go aus einem AWS Nicht-Base-Image erstellen. Das Beispiel-Dockerfile in den folgenden Schritten verwendet ein Alpine-Basis-Image.

Sie müssen das Paket aws-lambda-go/lambda in Ihren Go-Handler aufnehmen. Dieses Paket implementiert das Programmiermodell für Go, einschließlich der Laufzeitschnittstelle.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- Go
- Docker
- AWS Command Line Interface (AWS CLI) Version 2

Erstellen eines Images aus einem alternativen Basis-Image

Erstellen und Bereitstellen einer Go-Funktion mit einem Alpine-Basis-Image

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir hello
cd hello
```

2. Initialisieren Sie ein neues Go-Modul.

```
go mod init example.com/hello-world
```

3. Fügen Sie die Lambda-Bibliothek als Abhängigkeit Ihres neuen Moduls hinzu.

```
go get github.com/aws/aws-lambda-go/lambda
```

4. Erstellen Sie eine Datei namens `main.go` und öffnen Sie diese dann in einem Text-Editor. Dies ist der Code für die Lambda-Funktion. Sie können den folgenden Beispielcode zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.

```
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, event events.APIGatewayProxyRequest)
 (events.APIGatewayProxyResponse, error) {
 response := events.APIGatewayProxyResponse{
  StatusCode: 200,
  Body:       "\"Hello from Lambda!\"",
 }
 return response, nil
}

func main() {
 lambda.Start(handler)
}
```

5. Verwenden Sie einen Texteditor, um ein Dockerfile in Ihrem Projektverzeichnis zu erstellen. Das folgende Beispiel-Dockerfile verwendet ein Alpine-Basis-Image.

Example Dockerfile

> **Note**
>
> Stellen Sie sicher, dass die Version von Go, die Sie in der Docker-Datei angeben (z. B. `golang:1.20`), dieselbe Version von Go ist, mit der Sie Ihre Anwendung erstellt haben.

```
FROM golang:1.20.2-alpine3.16 as build
WORKDIR /helloworld
# Copy dependencies list
COPY go.mod go.sum ./
# Build
COPY main.go .
RUN go build -o main main.go
# Copy artifacts to a clean image
FROM alpine:3.16
COPY --from=build /helloworld/main /main
ENTRYPOINT [ "/main" ]
```

6. Erstellen Sie Ihr Docker-Image mit dem docker build-Befehl. Das folgende Beispiel benennt das Bild in `docker-image` und gibt ihm den `test` Tag.

```
docker build --platform linux/amd64 -t docker-image:test .
```

> **Note**
>
> Der Befehl gibt die `--platform linux/amd64`-Option an, um sicherzustellen, dass Ihr Container mit der Lambda-Ausführungsumgebung kompatibel ist, unabhängig von der Architektur des Entwicklungsrechners. Wenn Sie beabsichtigen, eine Lambda-Funktion mithilfe der ARM64-Befehlssatzarchitektur zu erstellen, müssen Sie den Befehl unbedingt so ändern, dass stattdessen die `--platform linux/arm64`-Option verwendet wird.

(Optional) Testen Sie das Image lokal

Verwenden Sie den Laufzeit-Schnittstellen-Emulator, um das Image lokal zu testen. Sie können den Emulator in Ihr Image einbauen oder ihn mit dem folgenden Verfahren auf Ihrem lokalen Computer installieren.

Installieren des Laufzeitschnittstellen-Emulators auf Ihrem lokalen Computer

1. Führen Sie in Ihrem Projektverzeichnis den folgenden Befehl aus, um den Runtime-Interface-Emulator (x86-64-Architektur) herunterzuladen GitHub und auf Ihrem lokalen Computer zu installieren.

   Linux/macOS

   ```
   mkdir -p ~/.aws-lambda-rie && \
       curl -Lo ~/.aws-lambda-rie/aws-lambda-rie https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie && \
       chmod +x ~/.aws-lambda-rie/aws-lambda-rie
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie die GitHub Repository-URL im vorherigen Befehl durch Folgendes:

   ```
   https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie-arm64
   ```

   PowerShell

   ```
   $dirPath = "$HOME\.aws-lambda-rie"
   if (-not (Test-Path $dirPath)) {
       New-Item -Path $dirPath -ItemType Directory
   }

   $downloadLink = "https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/download/aws-lambda-rie"
   $destinationPath = "$HOME\.aws-lambda-rie\aws-lambda-rie"
   Invoke-WebRequest -Uri $downloadLink -OutFile $destinationPath
   ```

   Um den arm64-Emulator zu installieren, ersetzen Sie das `$downloadLink` durch Folgendes:

```
https://github.com/aws/aws-lambda-runtime-interface-emulator/releases/latest/
download/aws-lambda-rie-arm64
```

2. Starten Sie Ihr Docker-Image mit dem docker run-Befehl. Beachten Sie Folgendes:

   - `docker-image` ist der Image-Name und `test` ist das Tag.
   - `/main` ist `ENTRYPOINT` aus Ihrem Dockerfile.

   Linux/macOS

   ```
   docker run --platform linux/amd64 -d -v ~/.aws-lambda-rie:/aws-lambda -p
    9000:8080 \
       --entrypoint /aws-lambda/aws-lambda-rie \
       docker-image:test \
           /main
   ```

   PowerShell

   ```
   docker run --platform linux/amd64 -d -v "$HOME\.aws-lambda-rie:/aws-lambda" -p
    9000:8080 `
   --entrypoint /aws-lambda/aws-lambda-rie `
   docker-image:test `
       /main
   ```

   Dieser Befehl führt das Image als Container aus und erstellt einen lokalen Endpunkt bei `localhost:9000/2015-03-31/functions/function/invocations`.

   > **Note**
   >
   > Wenn Sie das Docker-Image für die ARM64-Befehlssatz-Architektur erstellt haben, müssen Sie die Option `--platform linux/arm64` statt `--platform linux/amd64` verwenden.

3. Veröffentlichen Sie ein Ereignis auf dem lokalen Endpunkt.

   Linux/macOS

   Führen Sie unter Linux oder macOS den folgenden `curl`-Befehl aus:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d '{}'
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
curl "http://localhost:9000/2015-03-31/functions/function/invocations" -d
 '{"payload":"hello world!"}'
```

PowerShell

Führen Sie in PowerShell den folgenden `Invoke-WebRequest` Befehl aus:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{}' -ContentType "application/json"
```

Dieser Befehl ruft die Funktion mit einem leeren Ereignis auf und gibt eine Antwort zurück. Wenn Sie Ihren eigenen Funktionscode anstelle des Beispielfunktionscodes verwenden, wird empfohlen, die Funktion mit einer JSON-Nutzlast aufzurufen. Beispiel:

```
Invoke-WebRequest -Uri "http://localhost:9000/2015-03-31/functions/function/
invocations" -Method Post -Body '{"payload":"hello world!"}' -ContentType
 "application/json"
```

4. Die Container-ID erhalten.

```
docker ps
```

5. Verwenden Sie den Befehl docker kill, um den Container zu anzuhalten. Ersetzen Sie in diesem Befehl `3766c4ab331c` durch die Container-ID aus dem vorherigen Schritt.

```
docker kill 3766c4ab331c
```

Das Image bereitstellen

Um das Image in Amazon ECR hochzuladen und die Lambda-Funktion zu erstellen

1. Führen Sie den Befehl get-login-password aus, um die Docker-CLI bei Ihrem Amazon-ECR-Registry zu authentifizieren.

   - Setzen Sie den `--region` Wert auf den AWS-Region Ort, an dem Sie das Amazon ECR-Repository erstellen möchten.
   - Ersetzen Sie es `111122223333` durch Ihre AWS-Konto ID.

   ```
   aws ecr get-login-password --region us-east-1 | docker login --username AWS --
   password-stdin 111122223333.dkr.ecr.us-east-1.amazonaws.com
   ```

2. Erstellen Sie ein Repository in Amazon ECR mithilfe des Befehls create-repository.

   ```
   aws ecr create-repository --repository-name hello-world --region us-east-1 --image-
   scanning-configuration scanOnPush=true --image-tag-mutability MUTABLE
   ```

   > **Note**
   >
   > Das Amazon ECR-Repository muss sich im selben Format AWS-Region wie die Lambda-Funktion befinden.

   Wenn erfolgreich, sehen Sie eine Antwort wie diese:

   ```
   {
       "repository": {
           "repositoryArn": "arn:aws:ecr:us-east-1:111122223333:repository/hello-
   world",
           "registryId": "111122223333",
           "repositoryName": "hello-world",
           "repositoryUri": "111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-
   world",
           "createdAt": "2023-03-09T10:39:01+00:00",
           "imageTagMutability": "MUTABLE",
           "imageScanningConfiguration": {
               "scanOnPush": true
   ```

```
        },
        "encryptionConfiguration": {
            "encryptionType": "AES256"
        }
    }
}
```

3. Kopieren Sie das `repositoryUri` aus der Ausgabe im vorherigen Schritt.
4. Führen Sie den Befehl docker tag aus, um Ihr lokales Image als neueste Version in Ihrem Amazon-ECR-Repository zu markieren. In diesem Befehl gilt Folgendes:
   - Ersetzen Sie `docker-image:test` durch den Namen und das Tag Ihres Docker-Images.
   - Ersetzen Sie `<ECRrepositoryUri>` durch den `repositoryUri`, den Sie kopiert haben. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
docker tag docker-image:test <ECRrepositoryUri>:latest
```

   Beispiel:

```
docker tag docker-image:test 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

5. Führen Sie den Befehl docker push aus, um Ihr lokales Image im Amazon-ECR-Repository bereitzustellen. Stellen Sie sicher, dass Sie `:latest` am Ende der Repository-URI angeben.

```
docker push 111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest
```

6. Erstellen Sie eine Ausführungsrolle für die Funktion, wenn Sie noch keine haben. Sie benötigen den Amazon-Ressourcennamen (ARN) der Rolle im nächsten Schritt.
7. So erstellen Sie die Lambda-Funktion: Geben Sie für `ImageUri` die Repository-URI von zuvor an. Stellen Sie sicher, dass Sie `:latest` am Ende der URI angeben.

```
aws lambda create-function \
  --function-name hello-world \
  --package-type Image \
  --code ImageUri=111122223333.dkr.ecr.us-east-1.amazonaws.com/hello-world:latest \
  --role arn:aws:iam::111122223333:role/lambda-ex
```

> **Note**
>
> Sie können eine Funktion mit einem Bild in einem anderen AWS Konto erstellen, sofern sich das Bild in derselben Region wie die Lambda-Funktion befindet. Weitere Informationen finden Sie unter Kontoübergreifende Berechtigungen von Amazon ECR.

8. Die Funktion aufrufen.

```
aws lambda invoke --function-name hello-world response.json
```

Das Ergebnis sollte ungefähr wie folgt aussehen:

```
{
  "ExecutedVersion": "$LATEST",
  "StatusCode": 200
}
```

9. Um die Ausgabe der Funktion zu sehen, überprüfen Sie die `response.json`-Datei.

Um den Funktionscode zu aktualisieren, müssen Sie das Image erneut erstellen, das neue Image in das Amazon-ECR-Repository hochladen und dann den Befehl update-function-code verwenden, um das Image für die Lambda-Funktion bereitzustellen.

Lambda löst das Image-Tag in einen bestimmten Image-Digest auf. Das heißt, wenn Sie das Image-Tag, das zur Bereitstellung der Funktion verwendet wurde, auf ein neues Image in Amazon ECR verweisen, aktualisiert Lambda die Funktion nicht automatisch, um das neue Image zu verwenden. Um das neue Image für dieselbe Lambda-Funktion bereitzustellen, müssen Sie den `update-function-code` Befehl verwenden, auch wenn das Image-Tag in Amazon ECR gleich bleibt.

AWS Lambda Funktion protokollieren in Go

AWS Lambda überwacht automatisch Lambda-Funktionen in Ihrem Namen und sendet Protokolle an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Auf dieser Seite wird beschrieben, wie Sie eine Protokollausgabe aus dem Code Ihrer Lambda-Funktion erstellen oder mit der AWS Command Line Interface Lambda-Konsole oder der CloudWatch Konsole auf Logs zugreifen.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus dem Code Ihrer Funktion auszugeben, können Sie Methoden für das Fmt-Paket verwenden oder eine Protokollierungsbibliothek, die zu `stdout` oder `stderr` schreibt. Im folgenden Beispiel wird das Protokollpaket verwendet.

Example main.go – Protokollierung

```
func handleRequest(ctx context.Context, event events.SQSEvent) (string, error) {
  // event
  eventJson, _ := json.MarshalIndent(event, "", "  ")
  log.Printf("EVENT: %s", eventJson)
  // environment variables
  log.Printf("REGION: %s", os.Getenv("AWS_REGION"))
  log.Println("ALL ENV VARS:")
  for _, element := range os.Environ() {
    log.Println(element)
  }
```

Example Protokollformat

```
START RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Version: $LATEST
2020/03/27 03:40:05 EVENT: {
  "Records": [
    {
      "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
      "receiptHandle": "MessageReceiptHandle",
      "body": "Hello from SQS!",
      "md5OfBody": "7b27xmplb47ff90a553787216d55d91d",
      "md5OfMessageAttributes": "",
      "attributes": {
        "ApproximateFirstReceiveTimestamp": "1523232000001",
        "ApproximateReceiveCount": "1",
        "SenderId": "123456789012",
        "SentTimestamp": "1523232000000"
      },
      ...
2020/03/27 03:40:05 AWS_LAMBDA_LOG_STREAM_NAME=2020/03/27/
[$LATEST]569cxmplc3c34c7489e6a97ad08b4419
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_NAME=blank-go-function-9DV3XMPL6XBC
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
2020/03/27 03:40:05 AWS_LAMBDA_FUNCTION_VERSION=$LATEST
2020/03/27 03:40:05 AWS_EXECUTION_ENV=AWS_Lambda_go1.x
END RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71
REPORT RequestId: dbda340c-xmpl-4031-8810-11bb609b4c71 Duration: 38.66 ms Billed
 Duration: 39 ms Memory Size: 128 MB Max Memory Used: 54 MB Init Duration: 203.69 ms
XRAY TraceId: 1-5e7d7595-212fxmpl9ee07c4884191322 SegmentId: 42ffxmpl0645f474 Sampled:
 true
```

Die Go-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die Berichtszeile enthält die folgenden Details.

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.

- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der Konsole CloudWatch

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
```

```
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Go-Code instrumentieren AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS -Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von zwei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) — Eine sichere, produktionsbereite und AWS unterstützte Distribution des (OTel) SDK. OpenTelemetry
- AWS X-Ray SDK for Go — Ein SDK zum Generieren und Senden von Trace-Daten an X-Ray.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda SDKs sind Teil einer eng integrierten Instrumentierungslösung von. AWS Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Ablaufverfolgung in X-Ray mit beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS -Distro für Open Telemetry und X-Ray-SDKs.

Sections

Verwenden von ADOT zur Instrumentierung Ihrer Go-Funktionen

ADOT bietet vollständig verwaltete Lambda-Ebenen, die alles packen, was Sie zum Sammeln von Telemetriedaten mit dem OTel-SDK benötigen. Indem Sie diese Ebene verwenden, können Sie Ihre Lambda-Funktionen instrumentieren, ohne einen Funktionscode ändern zu müssen. Sie können Ihren Ebenen auch für die benutzerdefinierte Initialisierung von OTel konfigurieren. Weitere Informationen finden Sie unter Benutzerdefinierte Konfiguration für den ADOT Collector auf Lambda in der ADOT-Dokumentation.

Für Go-Laufzeiten können Sie den AWS -verwaltete Lambda-Ebene für ADOT Go hinzufügen, um Ihre Funktionen automatisch zu instrumentieren. Eine ausführliche Anleitung zum Hinzufügen dieser Ebene finden Sie unter AWS Distro for OpenTelemetry Lambda Support for Go in der ADOT-Dokumentation.

Instrumentierung Ihrer Go-Funktionen mithilfe von X-Ray-SDK

Um Details zu Aufrufen aufzuzeichnen, die Ihre Lambda-Funktion an andere Ressourcen in Ihrer Anwendung tätigt, können Sie auch das AWS X-Ray SDK for Go verwenden. Um das SDK zu erhalten, laden Sie das SDK aus seinem GitHub Repository herunter mit`go get`:

```
go get github.com/aws/aws-xray-sdk-go
```

Um AWS SDK-Clients zu instrumentieren, übergeben Sie den Client an die `xray.AWS()` Methode. Anschließend können Sie Aufrufe verfolgen, indem Sie die `WithContext`-Version der Methode verwenden.

```
svc := s3.New(session.New())
xray.AWS(svc.Client)
...
svc.ListBucketsWithContext(ctx aws.Context, input *ListBucketsInput)
```

Aktivieren Sie nach Hinzufügen der richtigen Abhängigkeiten die Nachverfolgung in der Konfiguration Ihrer Funktion über die Lambda-Konsole oder die API.

Aktivieren der Nachverfolgung mit der Lambda-Konsole

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

Aktivieren der Nachverfolgung mit der Lambda-API

Konfigurieren Sie die Ablaufverfolgung für Ihre Lambda-Funktion mit dem AWS CLI oder AWS SDK und verwenden Sie die folgenden API-Operationen:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Interpretieren einer X-Ray-Nachverfolgung

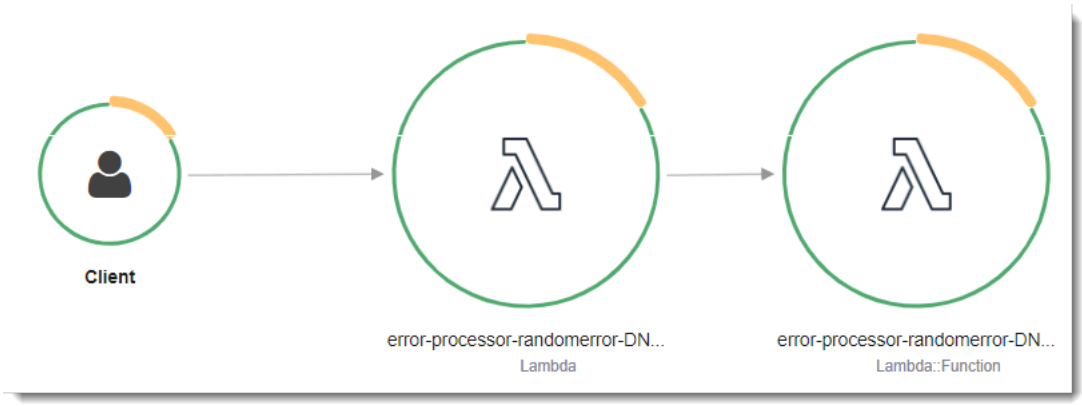
Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray.
Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

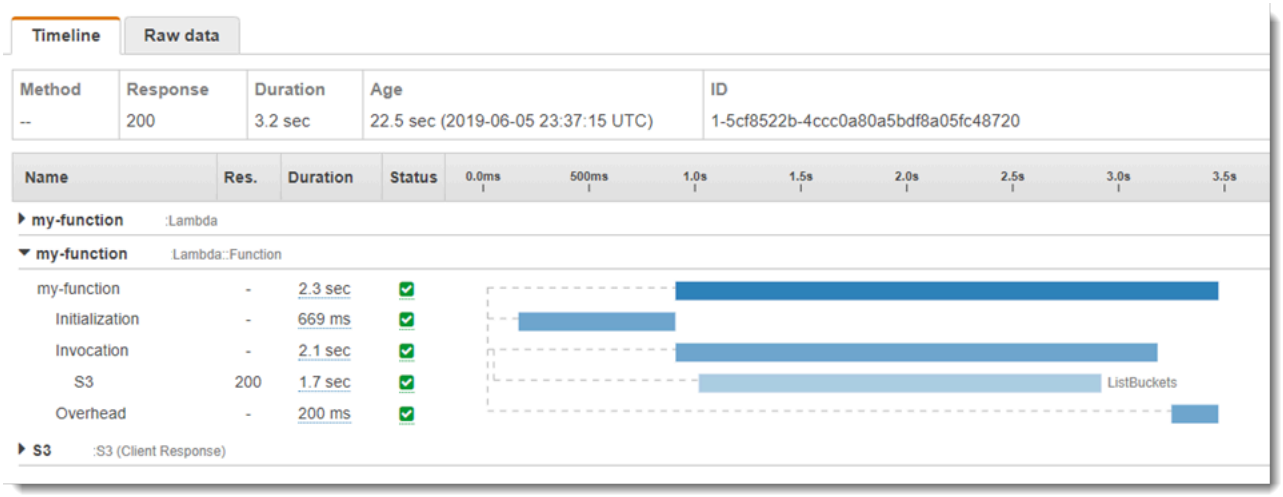
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.
- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter AWS X-Ray -SDK für Go im AWS X-Ray -Entwicklerhandbuch.

> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-

Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Verwenden von -Umgebungsvariablen

Um auf Umgebungsvariablen in Go zuzugreifen, verwenden Sie die Getenv-Funktion.

Im Folgenden wird das Verfahren erläutert. Beachten Sie, dass von der Funktion das Fmt-Paket importiert wird, um die gedruckten Ergebnisse zu formatieren. Außerdem wird das os-Paket importiert. Dies ist eine plattformunabhängige Systemschnittstelle, über die Sie auf Umgebungsvariablen zugreifen können.

```
package main

import (
 "fmt"
 "os"
 "github.com/aws/aws-lambda-go/lambda"
)

func main() {
 fmt.Printf("%s is %s. years old\n", os.Getenv("NAME"), os.Getenv("AGE"))

}
```

Eine Liste der Umgebungsvariablen, die von der Lambda-Laufzeit festgelegt werden, finden Sie unter Definierte Laufzeitumgebungsvariablen.

Erstellen von Lambda-Funktionen mit C#

Sie können Ihre .NET-Anwendung in Lambda mit den verwalteten .NET 6- oder .NET 8-Laufzeiten, einer benutzerdefinierten Laufzeit oder einem Container-Image ausführen. Nachdem Ihr Anwendungscode kompiliert wurde, können Sie ihn entweder als ZIP-Datei oder als Container-Image für Lambda bereitstellen. Lambda stellt die folgenden Laufzeiten für .NET-Sprachen bereit:

.NET

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
.NET 8	`dotnet8`	Amazon Linux 2023			
.NET 6	`dotnet6`	Amazon Linux 2	12. November 2	28. Februar 2025	31. März 2025

Einrichten der .NET-Entwicklungsumgebung

Um Ihre Lambda-Funktionen zu entwickeln und zu erstellen, können Sie jede der allgemein verfügbaren.NET-Integrated Development Environments (IDEs) verwenden, einschließlich Microsoft Visual Studio, Visual Studio Code und JetBrains Rider. Zur Vereinfachung Ihrer Entwicklungserfahrung AWS bietet es eine Reihe von .NET-Projektvorlagen sowie die `Amazon.Lambda.Tools` Befehlszeilenschnittstelle (CLI).

Führen Sie die folgenden .NET-CLI-Befehle aus, um diese Projektvorlagen und Befehlszeilentools zu installieren.

Installation der .NET-Projektvorlagen

So installieren Sie die Projektvorlagen (.NET 8):

```
dotnet new install Amazon.Lambda.Templates
```

So installieren Sie die Projektvorlagen (.NET 6):

```
dotnet new --install Amazon.Lambda.Templates
```

> **Note**
>
> Wenn Sie die verwaltete Lambda-Laufzeit von .NET 6 verwenden, empfehlen wir Ihnen, ein Upgrade auf .NET 8 durchzuführen. Weitere Informationen finden Sie unter AWS Lambda Runtime-Upgrades verwalten und Einführung in das.NET 8-Runtime for AWS Lambda im AWS Compute-Blog.

Installation und Aktualisierung der CLI-Tools

Führen Sie die folgenden Befehle aus, um die `Amazon.Lambda.Tools` CLI zu installieren, zu aktualisieren und zu deinstallieren.

Installieren der Befehlszeilen-Tools:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Um die Befehlszeilentools zu aktualisieren:

```
dotnet tool update -g Amazon.Lambda.Tools
```

Um die Befehlszeilentools zu deinstallieren:

```
dotnet tool uninstall -g Amazon.Lambda.Tools
```

Definieren Sie den Lambda-Funktionshandler in C#

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Wenn Ihre Funktion aufgerufen wird und Lambda die Handler-Methode Ihrer Funktion ausführt, übergibt es zwei Argumente an Ihre Funktion. Das erste Argument ist das `event`-Objekt. Wenn eine andere Funktion Ihre Funktion AWS-Service aufruft, enthält das `event` Objekt Daten über das Ereignis, das den Aufruf Ihrer Funktion verursacht hat. Ein `event`-Objekt von API Gateway enthält beispielsweise Informationen über den Pfad, die HTTP-Methode und HTTP-Header. Die genaue Ereignisstruktur hängt davon ab, wie Ihre Funktion AWS-Service aufgerufen wird. Weitere Informationen zu Veranstaltungsformaten für einzelne Dienste finden Sie unter Integration anderer Services.

Lambda übergibt auch ein `context`-Objekt an Ihre Funktion. Dieses Objekt enthält Informationen über den Aufruf, die Funktion und die Ausführungsumgebung. Weitere Informationen finden Sie unter the section called “Context”.

Das native Format für alle Lambda-Ereignisse sind Bytestreams, die das Ereignis im JSON-Format darstellen. Wenn Ihre Funktionseingabe- und Ausgabeparameter nicht vom Typ `System.IO.Stream` sind, müssen Sie sie serialisieren. Geben Sie den zu verwendenden Serialisierer an, indem Sie das Assembly-Attribut `LambdaSerializer` setzen. Weitere Informationen finden Sie unter the section called “Serialisieren von Lambda-Funktionen”.

Themen

- .NET-Ausführungsmodelle für Lambda
- Handler für Klassenbibliotheken
- Ausführbare Assembly-Handler
- Serialisieren von Lambda-Funktionen
- Vereinfachen Sie den Funktionscode mit dem Lambda Annotations Framework
- Einschränkungen des Lambda-Funktionshandlers

.NET-Ausführungsmodelle für Lambda

Es gibt zwei verschiedene Ausführungsmodelle für die Ausführung von Lambda-Funktionen in .NET: den Klassenbibliotheksansatz und den Ansatz für ausführbare Assemblys.

Beim Ansatz der Klassenbibliothek übermitteln Sie Lambda eine Zeichenfolge mit den Angaben `AssemblyName`, `ClassName`, und `Method` der aufzurufenden Funktion. Weitere Informationen über das Format dieser Zeichenfolge finden Sie unter the section called “Handler für Klassenbibliotheken”. Während der Initialisierungsphase der Funktion wird die Klasse Ihrer Funktion initialisiert und der gesamte Code im Konstruktor wird ausgeführt.

Beim Ansatz für ausführbare Assemblys verwenden Sie das Feature für Anweisungen der obersten Ebene von C# 9. Dieser Ansatz generiert eine ausführbare Assembly, die Lambda immer dann ausführt, wenn sie einen Aufrufbefehl für Ihre Funktion empfängt. Sie geben Lambda nur den Namen der ausführbaren Assembly an, die ausgeführt werden soll.

Die folgenden Abschnitte enthalten Beispielfunktionscode für diese beiden Ansätze.

Handler für Klassenbibliotheken

Der folgende Lambda-Funktionscode zeigt ein Beispiel für eine Handler-Methode (`FunctionHandler`) für eine Lambda-Funktion, die den Klassenbibliotheksansatz verwendet. In dieser Beispielfunktion empfängt Lambda ein Ereignis von API Gateway, das die Funktion aufruft. Die Funktion liest einen Datensatz aus einer Datenbank und gibt den Datensatz als Teil der API-Gateway-Antwort zurück.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);
```

```
        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Wenn Sie eine Lambda-Funktion erstellen, müssen Sie Lambda Informationen über den Handler Ihrer Funktion in Form eines Handler-Strings zur Verfügung stellen. Dadurch wird Lambda mitgeteilt, welche Methode in Ihrem Code ausgeführt werden soll, wenn Ihre Funktion aufgerufen wird. In C# lautet das Format der Handlerzeichenfolge bei Verwendung des Klassenbibliotheksansatzes wie folgt:

`ASSEMBLY::TYPE::METHOD`, wobei:

- `ASSEMBLY` ist der Name der .NET-Assembly-Datei für Ihre Anwendung. Wenn Sie die `Amazon.Lambda.Tools` CLI zur Erstellung Ihrer Anwendung verwenden und den Assembly-Namen nicht über die Eigenschaft `AssemblyName` in der .csproj-Datei festlegen, ist `ASSEMBLY` einfach der Name Ihrer .csproj-Datei.
- `TYPE` ist der vollständige Name des Handler-Typs, der aus `Namespace` und `ClassName` besteht.
- `METHOD` ist der Name der Funktionshandlermethode in Ihrem Code.

Wenn die Baugruppe im Beispielcode den Namen `GetProductHandler` trägt, lautet die Zeichenfolge für den Handler `GetProductHandler::GetProductHandler.Function::FunctionHandler`.

Ausführbare Assembly-Handler

Im folgenden Beispiel ist die Lambda-Funktion als ausführbare Assembly definiert. Die Handler-Methode in diesem Code heißt `Handler`. Bei der Verwendung ausführbarer Assemblys muss die Lambda-Laufzeit gebootet werden. Dazu verwenden Sie die `LambdaBootstrapBuilder.Create`-Methode. Diese Methode nimmt als Eingaben die Methode, die Ihre Funktion als Handler verwendet, und den zu verwendenden Lambda-Serializer entgegen.

Weitere Informationen zur Verwendung von Anweisungen auf oberster Ebene finden Sie unter Einführung in die .NET 6-Laufzeit für AWS Lambda im AWS Compute-Blog.

```
namespace GetProductHandler;

IDatabaseRepository repo = new DatabaseRepository();

await LambdaBootstrapBuilder.Create<APIGatewayProxyRequest>(Handler, new
 DefaultLambdaJsonSerializer())
    .Build()
    .RunAsync();

async Task<APIGatewayProxyResponse> Handler(APIGatewayProxyRequest apigProxyEvent,
 ILambdaContext context)
{
    var id = input.PathParameters["id"];

    var databaseRecord = await this.repo.GetById(id);

    return new APIGatewayProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = JsonSerializer.Serialize(databaseRecord)
    };
};
```

Bei der Verwendung von ausführbaren Assemblys ist der Handler-String, der Lambda mitteilt, wie Ihr Code ausgeführt werden soll, der Name der Assembly. In diesem Beispiel wäre das `GetProductHandler`.

Serialisieren von Lambda-Funktionen

Wenn Ihre Lambda-Funktion andere Eingabe- oder Ausgabetypen als ein `Stream`-Objekt verwendet, müssen Sie eine Serialisierungsbibliothek zu Ihrer Anwendung hinzufügen. Sie können die Serialisierung entweder mit der standardmäßigen reflexionsbasierten Serialisierung implementieren, die von `System.Text.Json` und `Newtonsoft.Json` bereitgestellt wird, oder mit der quellgenerierten Serialisierung.

Verwenden Sie die durch die Quelle generierte Serialisierung

Die durch Quellen generierte Serialisierung ist eine Funktion von.NET-Versionen 6 und höher, mit der Serialisierungscode während der Kompilierung generiert werden kann. Sie macht Reflexionen überflüssig und kann die Leistung Ihrer Funktion verbessern. Gehen Sie wie folgt vor, um die quellgenerierte Serialisierung in Ihrer Funktion zu verwenden:

- Erstellen Sie eine neue Teilklasse, die von `JsonSerializerContext` erbt, und fügen Sie `JsonSerializable`-Attribute für alle Typen hinzu, die serialisiert oder deserialisiert werden müssen.
- Konfigurieren Sie das `LambdaSerializer` so, dass es ein `SourceGeneratorLambdaJsonSerializer<T>` verwendet.
- Aktualisieren Sie alle manuellen Serialisierungen oder Deserialisierungen in Ihrem Anwendungscode, um die neu erstellte Klasse zu verwenden.

Eine Beispielfunktion, die quellgenerierte Serialisierung verwendet, wird im folgenden Code gezeigt.

```
[assembly:
 LambdaSerializer(typeof(SourceGeneratorLambdaJsonSerializer<CustomSerializer>))]

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord,
 CustomSerializer.Default.Product)
        };
    }
}

[JsonSerializable(typeof(APIGatewayProxyRequest))]
[JsonSerializable(typeof(APIGatewayProxyResponse))]
[JsonSerializable(typeof(Product))]
```

```
public partial class CustomSerializer : JsonSerializerContext
{

}
```

> **Note**
>
> Wenn Sie die native Ahead-of-Time-Compilation (AOT) mit Lambda verwenden möchten, müssen Sie die quellgenerierte Serialisierung verwenden.

Verwenden Sie die reflektionsbasierte Serialisierung

AWS stellt vorgefertigte Bibliotheken bereit, mit denen Sie Ihrer Anwendung schnell Serialisierung hinzufügen können. Sie konfigurieren dies entweder mit den Paketen `Amazon.Lambda.Serialization.SystemTextJson` oder `Amazon.Lambda.Serialization.Json` NuGet . Hinter den Kulissen verwendet `Amazon.Lambda.Serialization.SystemTextJson` `System.Text.Json`, um Serialisierungsaufgaben durchzuführen, und `Amazon.Lambda.Serialization.Json` verwendet das Paket `Newtonsoft.Json`.

Sie können auch Ihre eigene Serialisierungsbibliothek erstellen, indem Sie die `ILambdaSerializer`-Schnittstelle implementieren; diese ist als Teil der `Amazon.Lambda.Core`-Bibliothek verfügbar. Diese Schnittstelle definiert zwei Methoden:

- `T Deserialize<T>(Stream requestStream);`

  Sie implementieren diese Methode für die Deserialisierung der Anfragenutzlast von der `Invoke`-API in das Objekt, das Ihrem Lambda-Funktions-Handler übergeben wird.
- `T Serialize<T>(T response, Stream responseStream);`

  Sie implementieren diese Methode, um das von Ihrem Lambda-Funktions-Handler zurückgegebene Ergebnis in die Antwort-Nutzlast zu serialisieren, die der `Invoke`-API-Vorgang zurückgibt.

Vereinfachen Sie den Funktionscode mit dem Lambda Annotations Framework

Lambda Annotations ist ein Framework für .NET 6 und .NET 8, das das Schreiben von Lambda-Funktionen mit C# vereinfacht. Mit dem Annotations-Framework können Sie einen Großteil des Codes in einer Lambda-Funktion ersetzen, die mit dem regulären Programmiermodell geschrieben wurde. Code, der mit dem Framework geschrieben wurde, verwendet einfachere Ausdrücke, sodass Sie sich auf Ihre Geschäftslogik konzentrieren können.

Der folgende Beispielcode zeigt, wie die Verwendung des Annotations-Frameworks das Schreiben von Lambda-Funktionen vereinfachen kann. Das erste Beispiel zeigt Code, der mit dem regulären Lambda-Programmmodell geschrieben wurde, und das zweite zeigt das Äquivalent unter Verwendung des Annotations-Frameworks.

```
public APIGatewayHttpApiV2ProxyResponse LambdaMathAdd(APIGatewayHttpApiV2ProxyRequest
 request, ILambdaContext context)
{
    if (!request.PathParameters.TryGetValue("x", out var xs))
    {
        return new APIGatewayHttpApiV2ProxyResponse
        {
            StatusCode = (int)HttpStatusCode.BadRequest
        };
    }
    if (!request.PathParameters.TryGetValue("y", out var ys))
    {
        return new APIGatewayHttpApiV2ProxyResponse
        {
            StatusCode = (int)HttpStatusCode.BadRequest
        };
    }
    var x = int.Parse(xs);
    var y = int.Parse(ys);
    return new APIGatewayHttpApiV2ProxyResponse
    {
        StatusCode = (int)HttpStatusCode.OK,
        Body = (x + y).ToString(),
        Headers = new Dictionary#string, string> { { "Content-Type", "text/plain" } }
    };
}
```

```
[LambdaFunction]
[HttpApi(LambdaHttpMethod.Get, "/add/{x}/{y}")]
public int Add(int x, int y)
{
    return x + y;
}
```

Ein weiteres Beispiel dafür, wie die Verwendung von Lambda-Anmerkungen Ihren Code vereinfachen kann, finden Sie in dieser serviceübergreifenden Beispielanwendung im Repository. `awsdocs/aws-doc-sdk-examples` GitHub Der Ordner `PamApiAnnotations` verwendet Lambda-Anmerkungen in der `function.cs`-Hauptdatei. Zum Vergleich: Der `PamApi`-Ordner enthält äquivalente Dateien, die mit dem regulären Lambda-Programmiermodell geschrieben wurden.

Das Annotations-Framework verwendet Quellgeneratoren, um Code zu generieren, der vom Lambda-Programmiermodell in den Code aus dem zweiten Beispiel übersetzt wird.

Weitere Informationen über die Verwendung von Lambda-Annotationen für .NET finden Sie in den folgenden Ressourcen:

- Das Repository. `aws/aws-lambda-dotnet` GitHub
- Vorstellung von.NET Annotations Lambda Framework (Preview) im AWS Developer Tools Blog.
- Das `Amazon.Lambda.Annotations` NuGet Paket.

Abhängigkeitsinjektion mit dem Lambda Annotations-Framework

Sie können auch das Lambda Annotations-Framework verwenden, um Ihren Lambda-Funktionen eine Dependency Injection hinzuzufügen, indem Sie die Syntax verwenden, mit der Sie vertraut sind. Wenn Sie einer `[LambdaStartup]`-Datei ein `Startup.cs`-Attribut hinzufügen, generiert das Lambda Annotations-Framework den erforderlichen Code zur Kompilierzeit.

```
[LambdaStartup]
public class Startup
{
    public void ConfigureServices(IServiceCollection services)
    {
        services.AddSingleton<IDatabaseRepository, DatabaseRepository>();
    }
}
```

Ihre Lambda-Funktion kann Dienste entweder durch Konstruktorinjektion oder durch Injektion in einzelne Methoden unter Verwendung des `[FromServices]`-Attributs injizieren.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function(IDatabaseRepository repo)
    {
        this._repo = repo;
    }

    [LambdaFunction]
    [HttpApi(LambdaHttpMethod.Get, "/product/{id}")]
    public async Task<Product> FunctionHandler([FromServices] IDatabaseRepository
 repository, string id)
    {
        return await this._repo.GetById(id);
    }
}
```

Einschränkungen des Lambda-Funktionshandlers

Beachten Sie, dass für die Handlersignatur einige Einschränkungen bestehen.

- Möglicherweise ist es nicht `unsafe`, Pointer-Typen in der Handler-Signatur zu verwenden, Sie können jedoch `unsafe`-Kontext in der Handler-Methode und ihren Abhängigkeiten verwenden. Weitere Informationen finden Sie unter unsafe (C#-Referenz) auf der Microsoft-Docs-Website.
- Eine variable Anzahl von Parametern kann nicht mit dem Schlüsselwort `params` weitergegeben werden und `ArgIterator` kann nicht als Eingabe- oder Rückgabe-Parameter verwendet werden, der zur Unterstützung einer variablen Anzahl von Parametern verwendet wird.
- Der Handler darf keine generische Methode sein (z. B. IList<T> Sort<T>(IList<T> input)).
- Asynchrone Handler mit der Signatur `async void` werden nicht unterstützt.

Erstellen und Bereitstellen von C#-Lambda-Funktionen mit ZIP-Dateiarchiven

Ein .NET-Bereitstellungspaket (ZIP-Dateiarchiv) enthält die kompilierten Assembly Ihrer Funktion sowie aller ihrer Assembly-Abhängigkeiten. Das Paket enthält auch eine *`proj`*`.deps.json`-Datei. Dies signalisiert der .NET-Laufzeit alle Abhängigkeiten Ihrer Funktion sowie eine *`proj`*`.runtimeconfig.json`-Datei, die für die Konfiguration der Laufzeit verwendet wird.

Um einzelne Lambda-Funktionen bereitzustellen, können Sie die `Amazon.Lambda.Tools` .NET Lambda Global CLI verwenden. Mit dem `dotnet lambda deploy-function` Befehl wird automatisch ein ZIP-Bereitstellungspaket erstellt und auf Lambda bereitgestellt. Wir empfehlen jedoch, Frameworks wie das AWS Serverless Application Model (AWS SAM) oder das AWS Cloud Development Kit (AWS CDK) zu verwenden, um Ihre .NET-Anwendungen bereitzustellen AWS.

Serverlose Anwendungen bestehen normalerweise aus einer Kombination von Lambda-Funktionen und anderen verwalteten Funktionen, die AWS-Services zusammenarbeiten, um eine bestimmte Geschäftsaufgabe auszuführen. AWS SAM und AWS CDK vereinfachen Sie die Erstellung und Bereitstellung von Lambda-Funktionen mit anderen AWS-Services in großem Maßstab. Die AWS SAM Vorlagenspezifikation bietet eine einfache und übersichtliche Syntax zur Beschreibung von Lambda-Funktionen, APIs, Berechtigungen, Konfigurationen und anderen AWS Ressourcen, aus denen Ihre serverlose Anwendung besteht. Über das AWS CDK definieren Sie die Cloud-Infrastruktur als Code, mit dem Sie zuverlässige, skalierbare und kostengünstige Anwendungen in der Cloud mit modernen Programmiersprachen und Frameworks wie .NET erstellen können. AWS CDK Sowohl die als auch die AWS SAM verwenden das.NET Lambda Global CLI, um Ihre Funktionen zu verpacken.

Obwohl es möglich ist, Lambda-Ebenen mit Funktionen in C# mithilfe der .NET-Core-CLI zu verwenden, raten wir davon ab. Funktionen in C#, die Ebenen verwenden, laden die freigegebenen Baugruppen während des Init-Phase manuell in den Speicher, was die Kaltstartzeiten verlängern kann. Schließen Sie stattdessen den gesamten freigegebenen Code zur Kompilierzeit ein, um die integrierten Optimierungen des .NET-Compilers zu nutzen.

In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen und Bereitstellen von.NET-Lambda-Funktionen mit der AWS SAM AWS CDK, der und der.NET Lambda Global-CLI.

Themen

- Verwenden der.NET Lambda Global CLI
- Stellen Sie C#-Lambda-Funktionen bereit mit AWS SAM

- Stellen Sie C#-Lambda-Funktionen bereit mit AWS CDK
- ASP.NET-Anwendungen bereitstellen

Verwenden der.NET Lambda Global CLI

Die .NET-CLI und die Erweiterung .NET Lambda Global Tools (`Amazon.Lambda.Tools`) bieten eine plattformübergreifende Möglichkeit, .NET-basierte Lambda-Anwendungen zu erstellen, zu verpacken und für Lambda bereitzustellen. In diesem Abschnitt erfahren Sie, wie Sie neue Lambda .NET-Projekte mit den .NET CLI- und Amazon Lambda-Vorlagen erstellen und diese mithilfe von `Amazon.Lambda.Tools` verpacken und bereitstellen

Themen

- Voraussetzungen
- .NET-Projekte mit der .NET-CLI erstellen
- .NET-Projekte über die .NET-CLI bereitstellen
- Verwendung von Lambda-Ebenen mit der.NET-CLI

Voraussetzungen

.NET 8 SDK

Falls Sie dies noch nicht getan haben, installieren Sie das.NET 8 SDK und Runtime.

AWS Amazon.Lambda.Templates.NET-Projektvorlagen

Verwenden Sie das Amazon.Lambda.Templates NuGet Paket, um Ihren Lambda-Funktionscode zu generieren. Zur Installation dieses Vorlagenpakets führen Sie den folgenden Befehl aus:

```
dotnet new install Amazon.Lambda.Templates
```

AWS Amazon.Lambda.Tools .NET Globale CLI-Tools

Verwenden Sie zum Erstellen Ihrer Lambda-Funktionen die Amazon.Lambda.Tools-.NET Global Tools-Erweiterung. Um Amazon.Lambda.Tools zu installieren, führen Sie den folgenden Befehl aus:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Weitere Informationen zur Amazon.Lambda.Tools .NET-CLI-Erweiterung finden Sie im AWS Extensions for .NET CLI-Repository unter GitHub.

.NET-Projekte mit der .NET-CLI erstellen

Verwenden Sie in der .NET CLI den `dotnet new`-Befehl zum Erstellen von .NET-Projekten in der Befehlszeile. Lambda bietet mit dem `Amazon.Lambda.Templates` NuGet Paket zusätzliche Vorlagen an.

Nach der Installation des Pakets führen Sie den folgenden Befehl aus, um eine Liste des verfügbaren Vorlagen zu sehen.

```
dotnet new list
```

Wenn Sie Details zu einer Vorlage einsehen möchten, verwenden Sie die `help`-Option. Um beispielsweise Details über die `lambda.EmptyFunction`-Vorlage zu sehen, führen Sie den folgenden Befehl aus.

```
dotnet new lambda.EmptyFunction --help
```

Verwenden Sie die `lambda.EmptyFunction`-Vorlage, um eine Basisvorlage für eine .NET-Lambda-Funktion zu erstellen. Dadurch wird eine einfache Funktion erstellt, die eine Zeichenfolge als Eingabe verwendet und diese mithilfe der `ToUpper`-Methode in Großbuchstaben umwandelt. Diese Vorlage unterstützt die folgenden Optionen.

- `--name` – Der Name der Funktion.
- `--region`— Die AWS Region, in der die Funktion erstellt werden soll.
- `--profile`— Der Name eines Profils in Ihrer AWS SDK for .NET Anmeldeinformationsdatei. Weitere Informationen zu Anmeldeinformationsprofilen in.NET finden Sie unter Configure AWS Credentials im AWS SDK for .NET Developer Guide.

In diesem Beispiel erstellen wir eine neue leere Funktion `myDotnetFunction` mit dem Namen unter Verwendung des Standardprofils und der AWS-Region Standardeinstellungen:

```
dotnet new lambda.EmptyFunction --name myDotnetFunction
```

Mit diesem Befehl werden die folgenden Dateien und Verzeichnisse in Ihrem Projektverzeichnis erstellt.

```
### myDotnetFunction
    ### src
    #   ### myDotnetFunction
    #       ### Function.cs
    #       ### Readme.md
    #       ### aws-lambda-tools-defaults.json
    #       ### myDotnetFunction.csproj
    ### test
        ### myDotnetFunction.Tests
            ### FunctionTest.cs
            ### myDotnetFunction.Tests.csproj
```

Zeigen Sie im Verzeichnis `src/myDotnetFunction` die folgenden Dateien an:

- aws-lambda-tools-defaults.json: Hier geben Sie die Befehlszeilenoptionen an, wenn Sie Ihre Lambda-Funktion bereitstellen. Zum Beispiel:

  ```
    "profile" : "default",
    "region" : "us-east-2",
    "configuration" : "Release",
    "function-architecture": "x86_64",
    "function-runtime":"dotnet8",
    "function-memory-size" : 256,
    "function-timeout" : 30,
    "function-handler" : "myDotnetFunction::myDotnetFunction.Function::FunctionHandler"
  ```

- Function.cs: Der Funktionscode Ihres Lambda-Handlers. Dies ist eine C #-Vorlage mit der `Amazon.Lambda.Core`-Standardbibliothek und einem `LambdaSerializer`-Standardattribut. Weitere Informationen zu den Serialisierungsanforderungen und -optionen finden Sie unter Serialisieren von Lambda-Funktionen. Es ist auch eine Beispielfunktion enthalten, die Sie bearbeiten können, um Lambda-Funktionscode anzuwenden.

  ```
  using Amazon.Lambda.Core;

  // Assembly attribute to enable the Lambda function's JSON input to be converted into
   a .NET class.
  [assembly:
   LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializ
  ```

```
namespace myDotnetFunction;

public class Function
{

    /// <summary>
    /// A simple function that takes a string and does a ToUpper
    /// </summary#
    /// <param name="input"></param>
    /// <param name="context"></param>
    /// <returns></returns>
    public string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}
```

- my DotnetFunction .csproj: Eine MSBuild-Datei, die die Dateien und Assemblys auflistet, aus denen Ihre Anwendung besteht.

```
<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <ImplicitUsings>enable</ImplicitUsings>
    <Nullable>enable</Nullable>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
    <!-- This property makes the build directory similar to a publish directory and
 helps the AWS .NET Lambda Mock Test Tool find project dependencies. -->
    <CopyLocalLockFileAssemblies>true</CopyLocalLockFileAssemblies>
    <!-- Generate ready to run images during publishing to improve cold start time.
 -->
    <PublishReadyToRun>true</PublishReadyToRun>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.2.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.SystemTextJson"
 Version="2.4.0" />
  </ItemGroup>
</Project>
```

- Readme: Verwenden Sie diese Datei, um Ihre Lambda-Funktion zu dokumentieren.

Zeigen Sie im Verzeichnis `myfunction/test` die folgenden Dateien an:

- my DotnetFunction .tests.csproj: Wie bereits erwähnt, ist dies eine MSBuild-Datei, die die Dateien und Assemblys auflistet, aus denen Ihr Testprojekt besteht. Beachten Sie auch, dass die `Amazon.Lambda.Core`-Bibliothek enthalten ist. Damit können Sie nahtlos beliebige Lambda-Vorlagen integrieren, die zum Testen Ihrer Funktion erforderlich sind.

```
<Project Sdk="Microsoft.NET.Sdk">
   ...

    <PackageReference Include="Amazon.Lambda.Core" Version="2.2.0 " />
   ...
```

- FunctionTest.cs: Dieselbe C#-Code-Vorlagendatei, in der sie im Verzeichnis enthalten ist. `src` Bearbeiten Sie diese Datei, damit sie dem Produktionscode Ihrer Funktion gleicht, und testen Sie sie vor dem Hochladen Ihrer Lambda-Funktion in eine Produktionsumgebung.

```
using Xunit;
using Amazon.Lambda.Core;
using Amazon.Lambda.TestUtilities;

using MyFunction;

namespace MyFunction.Tests
{
    public class FunctionTest
    {
        [Fact]
        public void TestToUpperFunction()
        {

            // Invoke the lambda function and confirm the string was upper cased.
            var function = new Function();
            var context = new TestLambdaContext();
            var upperCase = function.FunctionHandler("hello world", context);

            Assert.Equal("HELLO WORLD", upperCase);
        }
    }
}
```

.NET-Projekte über die .NET-CLI bereitstellen

Um Ihr Bereitstellungspaket zu erstellen und es auf Lambda bereitzustellen, verwenden Sie die `Amazon.Lambda.Tools`-CLI-Tools. Um Ihre Funktion anhand der Dateien bereitzustellen, die Sie in den vorherigen Schritten erstellt haben, navigieren Sie zunächst zu dem Ordner, der die `.csproj`-Datei Ihrer Funktion enthält.

```
cd myDotnetFunction/src/myDotnetFunction
```

Führen Sie den folgenden Befehl aus, um Ihren Code als ZIP-Bereitstellungspaket für Lambda bereitzustellen. Wählen Sie Ihren eigenen Funktionsnamen.

```
dotnet lambda deploy-function myDotnetFunction
```

Während der Bereitstellung werden Sie vom Assistenten aufgefordert, eine auszuwählen. the section called “Ausführungsrolle (Berechtigungen für Funktionen zum Zugriff auf andere Ressourcen)” Wählen Sie für dieses Beispiel die `lambda_basic_role`.

Nachdem Sie Ihre Funktion bereitgestellt haben, können Sie sie mit dem `dotnet lambda invoke-function`-Befehl in der Cloud testen. Für den Beispielcode in der `lambda.EmptyFunction`-Vorlage können Sie Ihre Funktion testen, indem Sie mit der `--payload`-Option eine Zeichenfolge übergeben.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything
 is OK"
```

Wenn Ihre Funktion erfolgreich bereitgestellt wurde, sollten Sie eine Ausgabe ähnlich der folgenden sehen.

```
dotnet lambda invoke-function myDotnetFunction --payload "Just checking if everything
 is OK"
Amazon Lambda Tools for .NET Core applications (5.8.0)
Project Home: https://github.com/aws/aws-extensions-for-dotnet-cli, https://github.com/
aws/aws-lambda-dotnet

Payload:
"JUST CHECKING IF EVERYTHING IS OK"

Log Tail:
START RequestId: id Version: $LATEST
```

```
END RequestId: id
REPORT RequestId: id  Duration: 0.99 ms       Billed Duration: 1 ms         Memory
 Size: 256 MB     Max Memory Used: 12 MB
```

Verwendung von Lambda-Ebenen mit der.NET-CLI

> **Note**
>
> Die Verwendung von Ebenen mit Funktionen in einer kompilierten Sprache wie C# bietet möglicherweise nicht den gleichen Nutzen wie in einer interpretierten Sprache wie Python. Da es sich bei C# um eine kompilierte Sprache handelt, müssen Ihre Funktionen während der Initialisierungsphase immer noch alle freigegebenen Baugruppen manuell in den Speicher laden, was die Kaltstartzeiten erhöhen kann. Stattdessen empfehlen wir, den freigegebenen Code bei der Kompilierung einzuschließen, um die Vorteile der integrierten Compiler-Optimierungen zu nutzen.

Die .NET-CLI unterstützt Befehle, mit denen Sie Ebenen veröffentlichen und C#-Funktionen bereitstellen können, die Ebenen nutzen. Um eine Ebene in einem angegebenen Amazon-S3-Bucket zu veröffentlichen, führen Sie den folgenden Befehl im selben Verzeichnis wie Ihre `.csproj`-Datei aus:

```
dotnet lambda publish-layer <layer_name> --layer-type runtime-package-store --s3-
bucket <s3_bucket_name>
```

Wenn Sie dann Ihre Funktion mithilfe der .NET-CLI bereitstellen, geben Sie im folgenden Befehl den Ebenen-ARN an, den Sie verwenden wollen:

```
dotnet lambda deploy-function <function_name> --function-layers arn:aws:lambda:us-
east-1:123456789012:layer:layer-name:1
```

Ein vollständiges Beispiel für eine Hello World-Funktion finden Sie im blank-csharp-with-layerBeispiel.

Stellen Sie C#-Lambda-Funktionen bereit mit AWS SAM

The AWS Serverless Application Model (AWS SAM) ist ein Toolkit, das dabei hilft, den Prozess der Erstellung und Ausführung serverloser Anwendungen zu optimieren. AWS Sie definieren die

Ressourcen für Ihre Anwendung in einer YAML- oder JSON-Vorlage und verwenden die AWS SAM Befehlszeilenschnittstelle (AWS SAM CLI), um Ihre Anwendungen zu erstellen, zu verpacken und bereitzustellen. Wenn Sie eine Lambda-Funktion aus einer AWS SAM Vorlage erstellen, AWS SAM wird automatisch ein ZIP-Bereitstellungspaket oder ein Container-Image mit Ihrem Funktionscode und allen von Ihnen angegebenen Abhängigkeiten erstellt. AWS SAM stellt dann Ihre Funktion mithilfe eines Stacks bereit.AWS CloudFormation Weitere Informationen zur Verwendung AWS SAM zum Erstellen und Bereitstellen von Lambda-Funktionen finden Sie unter Erste Schritte mit AWS SAM im AWS Serverless Application Model Entwicklerhandbuch.

Die folgenden Schritte zeigen Ihnen, wie Sie eine .NET Hello World-Beispielanwendung mit AWS SAM herunterladen, erstellen und bereitstellen können. Diese Beispielanwendung verwendet eine Lambda-Funktion und einen Amazon API Gateway-Endpunkt, um ein grundlegendes API-Backend zu implementieren. Wenn Sie eine HTTP GET-Anforderung an Ihren API Gateway-Endpunkt senden, ruft API Gateway Ihre Lambda-Funktion auf. Die Funktion gibt eine „Hello World“ -Meldung zusammen mit der IP-Adresse der Lambda-Funktionsinstance zurück, die Ihre Anfrage verarbeitet.

Wenn Sie Ihre Anwendung erstellen und bereitstellen AWS SAM, verwendet die AWS SAM CLI im Hintergrund den `dotnet lambda package` Befehl, um die einzelnen Lambda-Funktionscodepakete zu verpacken.

Voraussetzungen

.NET 8 SDK

Installieren Sie das.NET 8 SDK und Runtime.

AWS SAM CLI Version 1.39 oder höher

Informationen zur Installation der neuesten Version der AWS SAM CLI finden Sie unter Installation der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mit der Hello World-.NET-Vorlage mit dem folgenden Befehl.

   ```
   sam init --app-template hello-world --name sam-app \
   --package-type Zip --runtime dotnet8
   ```

   Mit diesem Befehl werden die folgenden Dateien und Verzeichnisse in Ihrem Projektverzeichnis erstellt.

```
### sam-app
    ### README.md
    ### events
    #   ### event.json
    ### omnisharp.json
    ### samconfig.toml
    ### src
    #   ### HelloWorld
    #       ### Function.cs
    #       ### HelloWorld.csproj
    #       ### aws-lambda-tools-defaults.json
    ### template.yaml
    ### test
        ### HelloWorld.Test
            ### FunctionTest.cs
            ### HelloWorld.Tests.csproj
```

2. Navigieren Sie in das Verzeichnis, das die `template.yaml file` enthält. Diese Datei ist eine Vorlage, die die AWS -Ressourcen für Ihre Anwendung definiert, einschließlich Ihrer Lambda-Funktion und einer API-Gateway-API.

```
cd sam-app
```

3. Um den Quellcode Ihrer Anwendung zu erstellen, führen Sie folgenden Befehl aus.

```
sam build
```

4. Führen Sie den folgenden Befehl aus AWS, um Ihre Anwendung bereitzustellen.

```
sam deploy --guided
```

Dieser Befehl packt Ihre Anwendung und stellt sie mit der folgenden Reihe von Eingabeaufforderungen bereit. Um die Standardoptionen zu übernehmen, drücken Sie die Eingabetaste.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert, ist das in Ordnung? , geben Sie unbedingt einy.

- Stack-Name: Der Name des Stacks, der in AWS CloudFormation bereitgestellt werden soll. Dieser Name muss für Ihr AWS-Konto Land eindeutig sein AWS-Region.
- AWS-Region: Die AWS-Region , auf der Sie Ihre App bereitstellen möchten.
- Änderungen vor der Bereitstellung bestätigen: Wählen Sie Ja, um alle Änderungssätze manuell zu überprüfen, bevor AWS SAM die Anwendungsänderungen bereitstellt. Wenn Sie Nein wählen, stellt die AWS SAM CLI automatisch Anwendungsänderungen bereit.
- Erlauben Sie die Erstellung von SAM-CLI-IAM-Rollen: Viele AWS SAM Vorlagen, in diesem Beispiel die von Hello World, erstellen AWS Identity and Access Management (IAM-) Rollen, um Ihren Lambda-Funktionen Zugriff auf andere zu gewähren. AWS-Services Wählen Sie Ja aus, um die Erlaubnis zur Bereitstellung eines AWS CloudFormation Stacks zu erteilen, der IAM-Rollen erstellt oder ändert.
- Rollback deaktivieren: Wenn bei der Erstellung oder Bereitstellung Ihres Stacks ein Fehler auftritt, wird der Stack standardmäßig AWS SAM auf die vorherige Version zurückgesetzt. Wählen Sie Nein, um diese Standardeinstellung zu akzeptieren.
- HelloWorldFunction Möglicherweise ist keine Autorisierung definiert, ist das in Ordnung: Geben Sie einy.
- Argumente in samconfig.toml speichern: Wählen Sie Ja, um Ihre Konfigurationsauswahl zu speichern. In Zukunft können Sie `sam deploy` ohne Parameter erneut ausführen, um Änderungen an Ihrer Anwendung vorzunehmen.

5. Wenn die Bereitstellung Ihrer Anwendung abgeschlossen ist, gibt die CLI den Amazon Resource Name (ARN) der Hello World Lambda-Funktion und die für sie erstellte IAM-Rolle zurück. Sie zeigt auch den Endpunkt Ihrer API-Gateway-API an. Um Ihre Anwendung zu testen, öffnen Sie den Endpunkt in einem Browser. Es wird eine Antwort ähnlich der folgenden angezeigt.

   ```
   {"message":"hello world","location":"34.244.135.203"}
   ```

6. Um Ihre Ressourcen zu löschen, führen Sie den folgenden Befehl aus. Beachten Sie, dass der von Ihnen erstellte API-Endpunkt ein öffentlicher Endpunkt ist, auf den über das Internet zugegriffen werden kann. Es wird empfohlen, dass Sie diesen Endpunkt nach dem Testen löschen.

   ```
   sam delete
   ```

Nächste Schritte

Weitere Informationen AWS SAM zur Erstellung und Bereitstellung von Lambda-Funktionen mit.NET finden Sie in den folgenden Ressourcen:

- Das AWS Serverless Application Model (AWS SAM) Entwicklerhandbuch
- Serverlose .NET-Anwendungen mit AWS Lambda und der SAM-CLI CLI

Stellen Sie C#-Lambda-Funktionen bereit mit AWS CDK

Das AWS Cloud Development Kit (AWS CDK) ist ein Open-Source-Framework für die Softwareentwicklung zur Definition von Cloud-Infrastruktur als Code mit modernen Programmiersprachen und Frameworks wie.NET. AWS CDK Projekte werden ausgeführt, um AWS CloudFormation Vorlagen zu generieren, die dann zur Bereitstellung Ihres Codes verwendet werden.

Folgen Sie den Anweisungen in den folgenden Abschnitten AWS CDK, um eine Hello World-.NET-Beispielanwendung mithilfe von zu erstellen und bereitzustellen. Die Beispielanwendung implementiert ein grundlegendes API-Backend, das aus einem API-Gateway-Endpunkt und einer Lambda-Funktion besteht. API Gateway ruft die Lambda-Funktion auf, wenn Sie eine HTTP-GET-Anforderung an den Endpunkt senden. Die Funktion gibt eine Hello-World-Nachricht zusammen mit der IP-Adresse der Lambda-Instance zurück, die Ihre Anfrage verarbeitet.

Voraussetzungen

.NET 8 SDK

Installieren Sie das.NET 8 SDK und Runtime.

AWS CDK Version 2

Informationen zur Installation der neuesten Version von finden Sie AWS CDK unter Erste Schritte mit dem AWS CDK im AWS Cloud Development Kit (AWS CDK) v2-Entwicklerhandbuch.

Stellen Sie eine AWS CDK Beispielanwendung bereit

1. Erstellen Sie ein Projektverzeichnis für die Beispielanwendung und navigieren Sie dorthin.

```
mkdir hello-world
cd hello-world
```

2. Initialisieren Sie eine neue AWS CDK Anwendung, indem Sie den folgenden Befehl ausführen.

```
cdk init app --language csharp
```

Der Befehl erstellt die folgenden Dateien und Verzeichnisse in Ihrem Projektverzeichnis

```
### README.md
### cdk.json
### src
    ### HelloWorld
    #   ### GlobalSuppressions.cs
    #   ### HelloWorld.csproj
    #   ### HelloWorldStack.cs
    #   ### Program.cs
    ### HelloWorld.sln
```

3. Öffnen Sie das `src`-Verzeichnis und erstellen Sie eine neue Lambda-Funktion mit der.NET-CLI. Dies ist die Funktion, die Sie mit dem AWS CDK einsetzen werden. In diesem Beispiel erstellen Sie eine Hello world-Funktion mit dem Namen `HelloWorldLambda` unter Verwendung der `lambda.EmptyFunction`-Vorlage.

```
cd src
dotnet new lambda.EmptyFunction -n HelloWorldLambda
```

Nach diesem Schritt sollte Ihre Verzeichnisstruktur innerhalb Ihres Projektverzeichnisses wie folgt aussehen.

```
### README.md
### cdk.json
### src
    ### HelloWorld
    #   ### GlobalSuppressions.cs
    #   ### HelloWorld.csproj
    #   ### HelloWorldStack.cs
    #   ### Program.cs
    ### HelloWorld.sln
    ### HelloWorldLambda
        ### src
        #   ### HelloWorldLambda
        #       ### Function.cs
        #       ### HelloWorldLambda.csproj
```

```
        #       ### Readme.md
        #       ### aws-lambda-tools-defaults.json
        ### test
            ### HelloWorldLambda.Tests
                ### FunctionTest.cs
                ### HelloWorldLambda.Tests.csproj
```

4. Öffnen Sie die `HelloWorldStack.cs`-Datei aus dem Verzeichnis `src/HelloWorld`. Ersetzen Sie den Inhalt der Datei durch den folgenden Code.

```
using Amazon.CDK;
using Amazon.CDK.AWS.Lambda;
using Amazon.CDK.AWS.Logs;
using Constructs;

namespace CdkTest
{
    public class HelloWorldStack : Stack
    {
        internal HelloWorldStack(Construct scope, string id, IStackProps props =
 null) : base(scope, id, props)
        {
            var buildOption = new BundlingOptions()
            {
                Image = Runtime.DOTNET_8.BundlingImage,
                User = "root",
                OutputType = BundlingOutput.ARCHIVED,
                Command = new string[]{
            "/bin/sh",
                "-c",
                " dotnet tool install -g Amazon.Lambda.Tools"+
                " && dotnet build"+
                " && dotnet lambda package --output-package /asset-output/
function.zip"
                }
            };

             var helloWorldLambdaFunction = new Function(this,
 "HelloWorldFunction", new FunctionProps
            {
                Runtime = Runtime.DOTNET_8,
                MemorySize = 1024,
                LogRetention = RetentionDays.ONE_DAY,
```

```
                Handler =
 "HelloWorldLambda::HelloWorldLambda.Function::FunctionHandler",
                Code = Code.FromAsset("./src/HelloWorldLambda/src/
HelloWorldLambda", new Amazon.CDK.AWS.S3.Assets.AssetOptions
                {
                    Bundling = buildOption
                }),
            });
        }
    }
}
```

Dies ist der Code zum Kompilieren und Bündeln des Anwendungscodes sowie die Definition der Lambda-Funktion selbst. Mit dem `BundlingOptions`-Objekt kann eine Zip-Datei erstellt werden, zusammen mit einer Reihe von Befehlen, die zur Erzeugung des Inhalts der Zip-Datei verwendet werden. In diesem Fall wird der Befehl `dotnet lambda package` zum Kompilieren und Erzeugen der Zip-Datei verwendet.

5. Um Ihre Anwendung bereitzustellen, führen Sie den folgenden Befehl aus.

```
cdk deploy
```

6. Rufen Sie Ihre bereitgestellte Lambda-Funktion mit der .NET Lambda CLI auf.

```
dotnet lambda invoke-function HelloWorldFunction -p "hello world"
```

7. Nach Abschluss der Tests können Sie die erstellten Ressourcen löschen, es sei denn, Sie möchten sie beibehalten. Führen Sie den folgenden Befehl aus, um Ihre Ressourcen zu löschen.

```
cdk destroy
```

Nächste Schritte

Weitere Informationen AWS CDK zur Erstellung und Bereitstellung von Lambda-Funktionen mit.NET finden Sie in den folgenden Ressourcen:

- Arbeiten mit dem AWS CDK in C#
- Erstellen, Verpacken und Veröffentlichen von.NET C#-Lambda-Funktionen mit dem CDK AWS

ASP.NET-Anwendungen bereitstellen

Sie können nicht nur ereignisgesteuerte Funktionen hosten, sondern auch .NET mit Lambda verwenden, um leichtgewichtige ASP.NET-Anwendungen zu hosten. Mit dem Paket können Sie ASP.NET-Anwendungen erstellen und bereitstellen. `Amazon.Lambda.AspNetCoreServer` NuGet In diesem Abschnitt erfahren Sie, wie Sie eine ASP.NET-Web-API mit dem .NET Lambda CLI-Tooling in Lambda bereitstellen.

Themen

Voraussetzungen

.NET 8 SDK

Installieren Sie das.NET 8 SDK und ASP.NET Core Runtime.

Amazon.Lambda.Tools

Verwenden Sie zum Erstellen Ihrer Lambda-Funktionen die Amazon.Lambda.Tools-.NET Global Tools-Erweiterung. Um Amazon.Lambda.Tools zu installieren, führen Sie den folgenden Befehl aus:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Weitere Informationen zur Amazon.Lambda.Tools .NET-CLI-Erweiterung finden Sie im AWS Extensions for .NET CLI-Repository unter GitHub.

Amazon.Lambda.Templates

Verwenden Sie das Amazon.Lambda.Templates NuGet Paket, um Ihren Lambda-Funktionscode zu generieren. Zur Installation dieses Vorlagenpakets führen Sie den folgenden Befehl aus:

```
dotnet new --install Amazon.Lambda.Templates
```

Eine ASP.NET-Web-API für Lambda bereitstellen

Um eine Web-API mit ASP.NET bereitzustellen, können Sie die .NET-Lambda-Vorlagen verwenden, um ein neues Web-API-Projekt zu erstellen. Verwenden Sie den folgenden Befehl, um ein neues ASP.NET-Web-API-Projekt zu initialisieren. Im Beispielbefehl nennen wir das Projekt `AspNetOnLambda`.

```
dotnet new serverless.AspNetCoreWebAPI -n AspNetOnLambda
```

Mit diesem Befehl werden die folgenden Dateien und Verzeichnisse in Ihrem Projektverzeichnis erstellt.

```
.
### AspNetOnLambda
    ### src
    #   ### AspNetOnLambda
    #       ### AspNetOnLambda.csproj
    #       ### Controllers
    #       #   ### ValuesController.cs
    #       ### LambdaEntryPoint.cs
    #       ### LocalEntryPoint.cs
    #       ### Readme.md
    #       ### Startup.cs
    #       ### appsettings.Development.json
    #       ### appsettings.json
    #       ### aws-lambda-tools-defaults.json
    #       ### serverless.template
    ### test
        ### AspNetOnLambda.Tests
            ### AspNetOnLambda.Tests.csproj
            ### SampleRequests
            #   ### ValuesController-Get.json
            ### ValuesControllerTests.cs
            ### appsettings.json
```

Wenn Lambda Ihre Funktion aufruft, wird als Einstiegspunkt die Datei `LambdaEntryPoint.cs` verwendet. Die von der .NET Lambda-Vorlage erstellte Datei enthält den folgenden Code.

```
namespace AspNetOnLambda;

public class LambdaEntryPoint : Amazon.Lambda.AspNetCoreServer.APIGatewayProxyFunction
```

```
{
    protected override void Init(IWebHostBuilder builder)
    {
        builder
            .UseStartup#Startup#();
    }

    protected override void Init(IHostBuilder builder)
    {
    }
}
```

Der von Lambda verwendete Einstiegspunkt muss von einer der drei Basisklassen im Paket `Amazon.Lambda.AspNetCoreServer` erben. Diese drei Basisklassen sind:

- `APIGatewayProxyFunction`
- `APIGatewayHttpApiV2ProxyFunction`
- `ApplicationLoadBalancerFunction`

Die Standardklasse, die verwendet wird, wenn Sie Ihre `LambdaEntryPoint.cs`-Datei mit der bereitgestellten .NET Lambda-Vorlage erstellen, ist `APIGatewayProxyFunction`. Die Basisklasse, die Sie in Ihrer Funktion verwenden, hängt davon ab, welche API-Schicht vor Ihrer Lambda-Funktion steht.

Jede der drei Basisklassen enthält eine öffentliche Methode namens `FunctionHandlerAsync`. Der Name dieser Methode wird Teil der Handler-String sein, die Lambda verwendet, um Ihre Funktion aufzurufen. Die `FunctionHandlerAsync`-Methode wandelt den eingehenden Ereignis-Payload in das korrekte ASP.NET-Format und die ASP.NET-Antwort zurück in einen Lambda-Antwort-Payload um. Für das gezeigte Beispielprojekt `AspNetOnLambda` würde der Handler-String wie folgt lauten.

```
AspNetOnLambda::AspNetOnLambda.LambdaEntryPoint::FunctionHandlerAsync
```

Um die API in Lambda bereitzustellen, führen Sie die folgenden Befehle aus, um in das Verzeichnis mit Ihrer Quellcodedatei zu navigieren und Ihre Funktion mit AWS CloudFormation bereitzustellen.

```
cd AspNetOnLambda/src/AspNetOnLambda
dotnet lambda deploy-serverless
```

> **Tip**
>
> Wenn Sie eine API mithilfe des **`dotnet lambda deploy-serverless`** Befehls bereitstellen, AWS CloudFormation gibt es Ihrer Lambda-Funktion einen Namen, der auf dem Stacknamen basiert, den Sie während der Bereitstellung angeben. Um Ihrer Lambda-Funktion einen benutzerdefinierten Namen zu geben, bearbeiten Sie die `serverless.template` Datei, um der `AWS::Serverless::Function` Ressource eine `FunctionName` Eigenschaft hinzuzufügen. Weitere Informationen finden Sie unter Namenstyp im AWS CloudFormation Benutzerhandbuch.

Bereitstellung minimaler ASP.NET-APIs für Lambda

Um eine ASP.NET-Minimal-API für Lambda bereitzustellen, können Sie die .NET-Lambda-Vorlagen verwenden, um ein neues Minimal-API-Projekt zu erstellen. Verwenden Sie den folgenden Befehl, um ein neues minimales API-Projekt zu initialisieren. In diesem Beispiel nennen wir das Projekt `MinimalApiOnLambda`.

```
dotnet new serverless.AspNetCoreMinimalAPI -n MinimalApiOnLambda
```

Der Befehl erstellt die folgenden Dateien und Verzeichnisse in Ihrem Projektverzeichnis.

```
### MinimalApiOnLambda
    ### src
        ### MinimalApiOnLambda
            ### Controllers
            #   ### CalculatorController.cs
            ### MinimalApiOnLambda.csproj
            ### Program.cs
            ### Readme.md
            ### appsettings.Development.json
            ### appsettings.json
            ### aws-lambda-tools-defaults.json
            ### serverless.template
```

Die Datei `Program.cs` enthält den folgenden Code.

```
var builder = WebApplication.CreateBuilder(args);
```

```
// Add services to the container.
builder.Services.AddControllers();

// Add AWS Lambda support. When application is run in Lambda Kestrel is swapped out as
 the web server with Amazon.Lambda.AspNetCoreServer. This
// package will act as the webserver translating request and responses between the
 Lambda event source and ASP.NET Core.
builder.Services.AddAWSLambdaHosting(LambdaEventSource.RestApi);

var app = builder.Build();


app.UseHttpsRedirection();
app.UseAuthorization();
app.MapControllers();

app.MapGet("/", () => "Welcome to running ASP.NET Core Minimal API on AWS Lambda");

app.Run();
```

Um Ihre Minimal-API für die Ausführung auf Lambda zu konfigurieren, müssen Sie diesen Code möglicherweise bearbeiten, damit Anfragen und Antworten zwischen Lambda und ASP.NET Core ordnungsgemäß übersetzt werden. Standardmäßig ist die Funktion für eine REST-API-Ereignisquelle konfiguriert. Für eine HTTP-API oder einen Application Load Balancer ersetzen Sie `(LambdaEventSource.RestApi)` durch eine der folgenden Optionen:

- `(LambdaEventSource.HttpAPi)`
- `(LambdaEventSource.ApplicationLoadBalancer)`

Um Ihre Minimal-API in Lambda bereitzustellen, führen Sie die folgenden Befehle aus, um in das Verzeichnis mit Ihrer Quellcodedatei zu navigieren und Ihre Funktion mit AWS CloudFormation bereitzustellen.

```
cd MinimalApiOnLambda/src/MinimalApiOnLambda
dotnet lambda deploy-serverless
```

Bereitstellen von .NET-Lambda-Funktionen mit Container-Images

Es gibt drei Möglichkeiten, ein Container-Image für eine .NET-Lambda-Funktion zu erstellen:

- Verwenden eines AWS Basisimages für .NET

  Die AWS -Basis-Images sind mit einer Sprachlaufzeit, einem Laufzeitschnittstellen-Client zur Verwaltung der Interaktion zwischen Lambda und Ihrem Funktionscode und einem Laufzeitschnittstellen-Emulator für lokale Tests vorinstalliert.

- Es wird ein AWS reines Betriebssystem-Basis-Image verwendet

  AWS Basis-Images nur für Betriebssysteme enthalten eine Amazon Linux-Distribution und den Runtime-Interface-Emulator. Diese Images werden häufig verwendet, um Container-Images für kompilierte Sprachen wie Go und Rust sowie für eine Sprache oder Sprachversion zu erstellen, für die Lambda kein Basis-Image bereitstellt, wie Node.js 19. Sie können reine OS-Basis-Images auch verwenden, um eine benutzerdefinierte Laufzeit zu implementieren. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für .NET in das Image aufnehmen.

- Verwenden eines Nicht-Basis-Images AWS

  Sie können auch ein alternatives Basis-Image aus einer anderen Container-Registry verwenden. Sie können auch ein von Ihrer Organisation erstelltes benutzerdefiniertes Image verwenden. Um das Image mit Lambda kompatibel zu machen, müssen Sie den Laufzeitschnittstellen-Client für .NET in das Image aufnehmen.

> **Tip**
>
> Um die Zeit zu reduzieren, die benötigt wird, bis Lambda-Container-Funktionen aktiv werden, siehe die Docker-Dokumentation unter Verwenden mehrstufiger Builds. Um effiziente Container-Images zu erstellen, folgen Sie den Bewährte Methoden für das Schreiben von Dockerfiles.

Auf dieser Seite wird erklärt, wie Sie Container-Images für Lambda erstellen, testen und bereitstellen.

Themen

- Verwenden eines AWS Basisimages für .NET
- Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

AWS Basis-Images für.NET

AWS stellt die folgenden Basisimages für.NET bereit:

Tags	Laufzeit	Betriebssystem	Dockerfile	Ablehnung
8	.NET 8	Amazon Linux 2023	Dockerfile für .NET 8 auf GitHub	
6	.NET 6	Amazon Linux 2	Dockerfile für .NET 6 auf GitHub	12. November 2024

Amazon-ECR-Repository: gallery.ecr.aws/lambda/dotnet

Verwenden eines AWS Basisimages für .NET

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- .NET SDK — In den folgenden Schritten wird das.NET 8-Basisimage verwendet. Stellen Sie sicher, dass Ihre .NET-Version mit der Version des Basis-Images übereinstimmt, die Sie in Ihrer Docker-Datei angeben.
- Docker

Erstellen und Bereitstellen eines Images mithilfe eines Basis-Images

In den folgenden Schritten verwenden Sie Amazon.Lambda.Templates und Amazon.Lambda.Tools, um ein.NET-Projekt zu erstellen. Anschließend erstellen Sie ein Docker-Image, laden das Image auf Amazon ECR hoch und stellen es auf einer Lambda-Funktion bereit.

1. Installieren Sie das Amazon.Lambda.Templates-Paket. NuGet

```
dotnet new install Amazon.Lambda.Templates
```

2. Erstellen Sie ein .NET-Projekt mithilfe der `lambda.image.EmptyFunction`-Vorlage.

```
dotnet new lambda.image.EmptyFunction --name MyFunction --region us-east-1
```

3. Navigieren Sie zum *`MyFunction`*`/src/`*`MyFunction`* Verzeichnis . Hier werden die Projektdateien gespeichert. Prüfen Sie die folgenden Dateien:

   - aws-lambda-tools-defaults.json – In dieser Datei geben Sie die Befehlszeilenoptionen an, wenn Sie Ihre Lambda-Funktion bereitstellen.
   - Function.cs – Der Funktionscode Ihres Lambda-Handlers. Dies ist eine C#-Vorlage mit der `Amazon.Lambda.Core`-Standardbibliothek und einem `LambdaSerializer`-Standardattribut. Weitere Informationen über Serialisierungsanforderungen und -optionen finden Sie unter Serialisieren von Lambda-Funktionen. Sie können den bereitgestellten Code zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.
   - MyFunction.csproj — Eine .NET-Projektdatei, die die Dateien und Assemblys auflistet, aus denen Ihre Anwendung besteht.
   - Readme.md – Diese Datei enthält weitere Informationen zur Lambda-Beispielfunktion.

4. Untersuchen Sie die Docker-Datei im `src/`*`MyFunction`*-Verzeichnis. Sie können die bereitgestellte Docker-Datei zum Testen verwenden oder sie durch Ihre eigene ersetzen. Wenn Sie Ihre eigenen verwenden, stellen Sie sicher, dass Sie:

   - Setzen Sie die `FROM`-Eigenschaft auf den URI des Basis-Images. Ihre .NET-Version muss mit der Version des Basis-Images übereinstimmen.
   - Legen Sie das `CMD`-Argument auf den Lambda-Funktionshandler fest. Das sollte mit dem `image-command` in `aws-lambda-tools-defaults.json` übereinstimmen.

   Example Dockerfile

```
# You can also pull these images from DockerHub amazon/aws-lambda-dotnet:8
FROM public.ecr.aws/lambda/dotnet:8

# Copy function code to Lambda-defined environment variable
COPY publish/* ${LAMBDA_TASK_ROOT}
```

```
# Set the CMD to your handler (could also be done as a parameter override outside
 of the Dockerfile)
CMD [ "MyFunction::MyFunction.Function::FunctionHandler" ]
```

5. Installieren Sie Amazon.Lambda.Tools .NET Global Tool.

```
dotnet tool install -g Amazon.Lambda.Tools
```

Wenn Amazon.Lambda.Tools bereits installiert ist, vergewissern Sie sich, dass Sie über die neueste Version verfügen.

```
dotnet tool update -g Amazon.Lambda.Tools
```

6. Ändern Sie das Verzeichnis zu *MyFunction*/src/*MyFunction*, sofern Sie dies noch nicht getan haben.

```
cd src/MyFunction
```

7. Verwenden Sie Amazon.Lambda.Tools, um das Docker-Image zu erstellen, es in ein neues Amazon-ECR-Repository zu verschieben und die Lambda-Funktion bereitzustellen.

   Für `--function-role` geben Sie den Rollennamen – nicht den Amazon-Ressourcenname (ARN) – der Ausführungsrolle für die Funktion an. z. B. `lambda-role`.

```
dotnet lambda deploy-function MyFunction --function-role lambda-role
```

   Weitere Informationen zum Amazon.Lambda.Tools .NET Global Tool finden Sie im AWS Extensions for .NET CLI Repository unter. GitHub

8. Die Funktion aufrufen.

```
dotnet lambda invoke-function MyFunction --payload "Testing the function"
```

   Wenn alles erfolgreich ist, sehen Sie Folgendes:

```
Payload:
"TESTING THE FUNCTION"

Log Tail:
START RequestId: id Version: $LATEST
```

```
END RequestId: id
REPORT RequestId: id  Duration: 0.99 ms       Billed Duration: 1 ms         Memory
 Size: 256 MB     Max Memory Used: 12 MB
```

9. Löschen Sie die Lambda-Funktion.

```
dotnet lambda delete-function MyFunction
```

Verwenden eines alternativen Basis-Images mit dem Laufzeitschnittstellen-Client

Wenn Sie ein OS-Basis-Image oder ein alternatives Basis-Image verwenden, müssen Sie den Laufzeitschnittstellen-Client in das Image einbinden. Der Laufzeitschnittstellen-Client erweitert die Lambda-Laufzeiten-API, die die Interaktion zwischen Lambda und Ihrem Funktionscode verwaltet.

Das folgende Beispiel zeigt, wie Sie mithilfe eines AWS Nicht-Base-Images ein Container-Image für .NET erstellen und wie Sie das Amazon.Lambda hinzufügen. RuntimeSupport Paket, das der Lambda-Runtime-Interface-Client für .NET ist. Das Dockerfile-Beispiel verwendet das Microsoft.NET 8-Basisimage.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- .NET SDK — Die folgenden Schritte verwenden ein .NET 8-Basisimage. Stellen Sie sicher, dass Ihre .NET-Version mit der Version des Basis-Images übereinstimmt, die Sie in Ihrer Docker-Datei angeben.
- Docker

Erstellen und Bereitstellen eines Images mithilfe eines alternativen Basis-Images

1. Installieren Sie das Amazon.Lambda.Templates-Paket. NuGet

```
dotnet new install Amazon.Lambda.Templates
```

2. Erstellen Sie ein .NET-Projekt mithilfe der `lambda.CustomRuntimeFunction`-Vorlage. Diese Vorlage enthält das Amazon.Lambda. RuntimeSupportPaket.

```
dotnet new lambda.CustomRuntimeFunction --name MyFunction --region us-east-1
```

3. Navigieren Sie zum *MyFunction*/src/*MyFunction* Verzeichnis . Hier werden die Projektdateien gespeichert. Prüfen Sie die folgenden Dateien:

   - aws-lambda-tools-defaults.json – In dieser Datei geben Sie die Befehlszeilenoptionen an, wenn Sie Ihre Lambda-Funktion bereitstellen.
   - Function.cs – Der Code enthält eine Klasse mit einer `Main`-Methode, die die Bibliothek `Amazon.Lambda.RuntimeSupport` als Bootstrap initialisiert. Die `Main`-Methode ist der Einstiegspunkt für den Prozess der Funktion. Die `Main`-Methode verpackt den Funktionshandler in einen Wrapper, mit dem der Bootstrap arbeiten kann. Weitere Informationen finden Sie unter Amazon.Lambda verwenden. RuntimeSupport als Klassenbibliothek im Repository. GitHub
   - MyFunction.csproj — Eine.NET-Projektdatei, die die Dateien und Assemblys auflistet, aus denen Ihre Anwendung besteht.
   - Readme.md – Diese Datei enthält weitere Informationen zur Lambda-Beispielfunktion.

4. Öffnen Sie die Datei `aws-lambda-tools-defaults.json` und fügen Sie die folgenden Zeilen hinzu:

```
  "package-type": "image",
  "docker-host-build-output-dir": "./bin/Release/lambda-publish"
```

   - package-type: Definiert das Bereitstellungspaket als Container-Image.
   - docker-host-build-output-dir: Legt das Ausgabeverzeichnis für den Build-Prozess fest.

   Example aws-lambda-tools-defaults.json

```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual
 Studio and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project root directory.",
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
```

```
  "profile": "",
  "region": "us-east-1",
  "configuration": "Release",
  "function-runtime": "provided.al2023",
  "function-memory-size": 256,
  "function-timeout": 30,
  "function-handler": "bootstrap",
  "msbuild-parameters": "--self-contained true",
  "package-type": "image",
  "docker-host-build-output-dir": "./bin/Release/lambda-publish"
}
```

5. Erstellen Sie ein Dockerfile in Verzeichnis *MyFunction*/src/*MyFunction*. Das folgende Beispiel-Dockerfile verwendet ein Microsoft .NET-Basisimage anstelle eines AWS -Basis-Images.

   - Legen Sie FROM-Eigenschaft auf die Kennung des Basis-Images fest. Ihre .NET-Version muss mit der Version des Basis-Images übereinstimmen.
   - Verwenden Sie den COPY-Befehl, um die Funktion in das Verzeichnis /var/task zu kopieren.
   - Legen Sie ENTRYPOINT auf das Modul fest, das der Docker-Container beim Start ausführen soll. In diesem Fall ist das Modul der Bootstrap, der die Bibliothek Amazon.Lambda.RuntimeSupport initialisiert.

   Example Dockerfile

```
# You can also pull these images from DockerHub amazon/aws-lambda-dotnet:8
FROM mcr.microsoft.com/dotnet/runtime:8.0

# Set the image's internal work directory
WORKDIR /var/task

# Copy function code to Lambda-defined environment variable
COPY "bin/Release/net8.0/linux-x64"  .

# Set the entrypoint to the bootstrap
ENTRYPOINT ["/usr/bin/dotnet", "exec", "/var/task/bootstrap.dll"]
```

6. Installieren Sie die Amazon.Lambda.Tools .NET Global Tools-Erweiterung.

```
dotnet tool install -g Amazon.Lambda.Tools
```

Wenn Amazon.Lambda.Tools bereits installiert ist, vergewissern Sie sich, dass Sie über die neueste Version verfügen.

```
dotnet tool update -g Amazon.Lambda.Tools
```

7. Verwenden Sie Amazon.Lambda.Tools, um das Docker-Image zu erstellen, es in ein neues Amazon-ECR-Repository zu verschieben und die Lambda-Funktion bereitzustellen.

   Für `--function-role` geben Sie den Rollennamen – nicht den Amazon-Ressourcenname (ARN) – der Ausführungsrolle für die Funktion an. z. B. `lambda-role`.

   ```
   dotnet lambda deploy-function MyFunction --function-role lambda-role
   ```

   Weitere Informationen zur .NET-CLI-Erweiterung Amazon.Lambda.Tools finden Sie im AWS Extensions for .NET CLI-Repository unter. GitHub
8. Die Funktion aufrufen.

   ```
   dotnet lambda invoke-function MyFunction --payload "Testing the function"
   ```

   Wenn alles erfolgreich ist, sehen Sie Folgendes:

   ```
   Payload:
   "TESTING THE FUNCTION"

   Log Tail:
   START RequestId: id Version: $LATEST
   END RequestId: id
   REPORT RequestId: id  Duration: 0.99 ms       Billed Duration: 1 ms         Memory
    Size: 256 MB     Max Memory Used: 12 MB
   ```
9. Löschen Sie die Lambda-Funktion.

   ```
   dotnet lambda delete-function MyFunction
   ```

Kompilieren Sie.NET-Lambda-Funktionscode in ein natives Laufzeitformat

.NET 8 unterstützt die native Kompilierung ahead-of-time (AOT). Mit nativem AOT können Sie Ihren Lambda-Funktionscode in ein natives Laufzeitformat kompilieren, wodurch die Notwendigkeit entfällt, .NET-Code zur Laufzeit zu kompilieren. Die native AOT-Kompilierung kann die Kaltstartzeit für Lambda-Funktionen reduzieren, die Sie in .NET schreiben. Weitere Informationen finden Sie im AWS Compute-Blog unter Einführung in die .NET 8-Laufzeit für AWS Lambda.

Sections

Lambda-Laufzeit

Verwenden Sie die verwaltete .NET 8-Lambda-Laufzeit, um einen Lambda-Funktionsbuild mit nativer AOT-Kompilierung bereitzustellen. Diese Laufzeit unterstützt die Verwendung von x86_64- und arm64-Architekturen.

Wenn Sie eine.NET-Lambda-Funktion ohne AOT bereitstellen, wird Ihre Anwendung zunächst in Intermediate Language (IL) -Code kompiliert. Zur Laufzeit nimmt der just-in-time (JIT-) Compiler in der Lambda-Laufzeit den IL-Code und kompiliert ihn nach Bedarf in Maschinencode. Mit einer Lambda-Funktion, die im Voraus mit nativem AOT kompiliert wird, kompilieren Sie Ihren Code bei der Bereitstellung Ihrer Funktion in Maschinencode, sodass Sie nicht auf die .NET-Laufzeit oder das SDK in der Lambda-Laufzeit angewiesen sind, um Ihren Code vor der Ausführung zu kompilieren.

Eine Einschränkung von AOT besteht darin, dass Ihr Anwendungscode in einer Umgebung mit demselben Amazon Linux 2023 (AL2023) -Betriebssystem kompiliert werden muss, das von.NET 8-Runtime verwendet wird. Die.NET Lambda-CLI bietet Funktionen zum Kompilieren Ihrer Anwendung in einem Docker-Container mithilfe eines AL2023-Images.

Um mögliche Probleme mit der architekturübergreifenden Kompatibilität zu vermeiden, empfehlen wir dringend, dass Sie Ihren Code in einer Umgebung mit derselben Prozessorarchitektur kompilieren, die Sie für Ihre Funktion konfigurieren. Weitere Informationen zu den Einschränkungen der architekturübergreifenden Kompilierung finden Sie unter Cross-Compilierung in der Microsoft.NET-Dokumentation.

Voraussetzungen

Docker

Um natives AOT verwenden zu können, muss Ihr Funktionscode in einer Umgebung mit demselben AL2023-Betriebssystem kompiliert werden wie das.NET 8-Runtime. Die .NET-CLI-Befehle in den folgenden Abschnitten verwenden Docker, um Lambda-Funktionen in einer AL203-Umgebung zu entwickeln und zu erstellen.

.NET 8 SDK

Die native AOT-Kompilierung ist ein Feature von.NET 8. Sie müssen das.NET 8-SDK auf Ihrem Build-Computer installieren, nicht nur auf der Runtime.

Amazon.Lambda.Tools

Verwenden Sie zum Erstellen Ihrer Lambda-Funktionen die Amazon.Lambda.Tools-.NET Global Tools-Erweiterung. Um Amazon.Lambda.Tools zu installieren, führen Sie den folgenden Befehl aus:

```
dotnet tool install -g Amazon.Lambda.Tools
```

Weitere Informationen zur Amazon.Lambda.Tools .NET-CLI-Erweiterung finden Sie im AWS Extensions for .NET CLI-Repository unter GitHub.

Amazon.Lambda.Templates

Verwenden Sie das Amazon.Lambda.Templates NuGet Paket, um Ihren Lambda-Funktionscode zu generieren. Zur Installation dieses Vorlagenpakets führen Sie den folgenden Befehl aus:

```
dotnet new install Amazon.Lambda.Templates
```

Erste Schritte

Sowohl das.NET Global CLI als auch AWS Serverless Application Model (AWS SAM) bieten Vorlagen für erste Schritte zum Erstellen von Anwendungen mit nativem AOT. Um Ihre erste native AOT-Lambda-Funktion zu erstellen, führen Sie die Schritte in den folgenden Anweisungen aus.

Um eine native AOT-kompilierte Lambda-Funktion zu initialisieren und bereitzustellen

1. Initialisieren Sie ein neues Projekt unter Verwendung der nativen AOT-Vorlage und navigieren Sie dann in das Verzeichnis, das die erstellten `.cs`- und `.csproj`-Dateien enthält. In diesem Beispiel nennen wir unsere Funktion `NativeAotSample`.

   ```
   dotnet new lambda.NativeAOT -n NativeAotSample
   cd ./NativeAotSample/src/NativeAotSample
   ```

   Die von der nativen AOT-Vorlage erstellte `Function.cs`-Datei enthält den folgenden Funktionscode.

   ```
   using Amazon.Lambda.Core;
   using Amazon.Lambda.RuntimeSupport;
   using Amazon.Lambda.Serialization.SystemTextJson;
   using System.Text.Json.Serialization;

   namespace NativeAotSample;

   public class Function
   {
       /// <summary>
       /// The main entry point for the Lambda function. The main function is called
    once during the Lambda init phase. It
       /// initializes the .NET Lambda runtime client passing in the function handler
    to invoke for each Lambda event and
       /// the JSON serializer to use for converting Lambda JSON format to the .NET
    types.
       /// </summary>
       private static async Task Main()
       {
           Func<string, ILambdaContext, string> handler = FunctionHandler;
           await LambdaBootstrapBuilder.Create(handler, new
    SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>())
               .Build()
   ```

```
            .RunAsync();
    }

    /// <summary>
    /// A simple function that takes a string and does a ToUpper.
    ///
    /// To use this handler to respond to an AWS event, reference the appropriate
 package from
    /// https://github.com/aws/aws-lambda-dotnet#events
    /// and change the string input parameter to the desired event type. When the
 event type
    /// is changed, the handler type registered in the main method needs to be
 updated and the LambdaFunctionJsonSerializerContext
    /// defined below will need the JsonSerializable updated. If the return type
 and event type are different then the
    /// LambdaFunctionJsonSerializerContext must have two JsonSerializable
 attributes, one for each type.
    ///
    // When using Native AOT extra testing with the deployed Lambda functions is
 required to ensure
    // the libraries used in the Lambda function work correctly with Native AOT. If
 a runtime
    // error occurs about missing types or methods the most likely solution will be
 to remove references to trim-unsafe
    // code or configure trimming options. This sample defaults to partial TrimMode
 because currently the AWS
    // SDK for .NET does not support trimming. This will result in a larger
 executable size, and still does not
    // guarantee runtime trimming errors won't be hit.
    /// </summary>
    /// <param name="input"></param>
    /// <param name="context"></param>
    /// <returns></returns>
    public static string FunctionHandler(string input, ILambdaContext context)
    {
        return input.ToUpper();
    }
}

/// <summary>
/// This class is used to register the input event and return type for the
 FunctionHandler method with the System.Text.Json source generator.
/// There must be a JsonSerializable attribute for each type used as the input and
 return type or a runtime error will occur
```

```
/// from the JSON serializer unable to find the serialization information for
 unknown types.
/// </summary>
[JsonSerializable(typeof(string))]
public partial class LambdaFunctionJsonSerializerContext : JsonSerializerContext
{
    // By using this partial class derived from JsonSerializerContext, we can
 generate reflection free JSON Serializer code at compile time
    // which can deserialize our class and properties. However, we must attribute
 this class to tell it what types to generate serialization code for.
    // See https://docs.microsoft.com/en-us/dotnet/standard/serialization/system-
text-json-source-generation
```

Native AOT kompiliert Ihre Anwendung in eine einzige native Binärdatei. Der Einstiegspunkt dieser Binärdatei ist die `static Main`-Methode. Innerhalb von `static Main` wird die Lambda-Laufzeit gebootstrapped und die `FunctionHandler`-Methode eingerichtet. Als Teil des Runtime-Bootstrap wird ein quellgenerierter Serializer mit `new SourceGeneratorLambdaJsonSerializer<LambdaFunctionJsonSerializerContext>()` konfiguriert

2. Um Ihre Anwendung auf Lambda bereitzustellen, stellen Sie sicher, dass Docker in Ihrer lokalen Umgebung ausgeführt wird, und führen Sie den folgenden Befehl aus.

```
dotnet lambda deploy-function
```

Hinter den Kulissen lädt die globale.NET-CLI ein AL2023 Docker-Image herunter und kompiliert Ihren Anwendungscode in einem laufenden Container. Die kompilierte Binärdatei wird zurück in Ihr lokales Dateisystem ausgegeben, bevor sie auf Lambda bereitgestellt wird.

3. Testen Sie Ihre Funktion, indem Sie den folgenden Befehl ausführen. Ersetzen Sie `<FUNCTION_NAME>` durch den Namen, den Sie für Ihre Funktion im Bereitstellungsassistenten gewählt haben.

```
dotnet lambda invoke-function <FUNCTION_NAME> --payload "hello world"
```

Die Antwort der CLI enthält Leistungsdetails für den Kaltstart (Initialisierungsdauer) und die Gesamtlaufzeit für Ihren Funktionsaufruf.

4. Führen Sie den folgenden Befehl aus, um die AWS Ressourcen zu löschen, die Sie mit den vorherigen Schritten erstellt haben. Ersetzen Sie `<FUNCTION_NAME>` durch den Namen, den Sie für Ihre Funktion im Bereitstellungsassistenten gewählt haben. Indem Sie AWS Ressourcen

löschen, die Sie nicht mehr verwenden, verhindern Sie, dass Ihnen AWS-Konto unnötige Gebühren in Rechnung gestellt werden.

```
dotnet lambda delete-function <FUNCTION_NAME>
```

Serialisierung

Um Funktionen mithilfe von nativem AOT für Lambda bereitzustellen, muss Ihr Funktionscode die quellgenerierte Serialisierung verwenden. Anstatt mithilfe der Laufzeitreflexion die Metadaten zu sammeln, die für den Zugriff auf Objekteigenschaften für die Serialisierung erforderlich sind, generieren Quellgeneratoren C#-Quelldateien, die beim Erstellen Ihrer Anwendung kompiliert werden. Um Ihren quellgenerierten Serializer korrekt zu konfigurieren, stellen Sie sicher, dass Sie alle Eingabe- und Ausgabeobjekte, die Ihre Funktion verwendet, sowie alle benutzerdefinierten Typen einbeziehen. Beispielsweise würde eine Lambda-Funktion, die Ereignisse von einer API-Gateway-REST-API empfängt und einen benutzerdefinierten `Product`-Typ zurückgibt, einen Serializer enthalten, der wie folgt definiert ist.

```
[JsonSerializable(typeof(APIGatewayProxyRequest))]
[JsonSerializable(typeof(APIGatewayProxyResponse))]
[JsonSerializable(typeof(Product))]
public partial class CustomSerializer : JsonSerializerContext
{
}
```

Trimmen

Natives AOT kürzt Ihren Anwendungscode als Teil der Kompilierung, um sicherzustellen, dass die Binärdatei so klein wie möglich ist. .NET 8 for Lambda bietet im Vergleich zu früheren Versionen von.NET eine verbesserte Trimmunterstützung. Support wurde zu den Lambda-Laufzeitbibliotheken, AWS .NET SDK, .NET Lambda Annotations und .NET 8 selbst hinzugefügt.

Diese Verbesserungen bieten das Potenzial, Warnungen beim Trimmen während der Erstellung zu eliminieren, aber .NET wird niemals vollständig trimmsicher sein. Das bedeutet, dass Teile von Bibliotheken, auf die Ihre Funktion angewiesen ist, im Rahmen des Kompilierungsschritts entfernt werden können. Sie können dies verwalten, indem Sie es `TrimmerRootAssemblies` als Teil Ihrer `.csproj` Datei definieren, wie im folgenden Beispiel gezeigt.

```
<ItemGroup>
```

```
    <TrimmerRootAssembly Include="AWSSDK.Core" />
    <TrimmerRootAssembly Include="AWSXRayRecorder.Core" />
    <TrimmerRootAssembly Include="AWSXRayRecorder.Handlers.AwsSdk" />
    <TrimmerRootAssembly Include="Amazon.Lambda.APIGatewayEvents" />
    <TrimmerRootAssembly Include="bootstrap" />
    <TrimmerRootAssembly Include="Shared" />
</ItemGroup>
```

Beachten Sie, dass das Problem `TrimmerRootAssembly` möglicherweise nicht behoben wird, wenn Sie eine Trimmwarnung erhalten, wenn Sie die Klasse hinzufügen, die die Warnung generiert. Eine Trim-Warnung weist darauf hin, dass die Klasse versucht, auf eine andere Klasse zuzugreifen, die erst zur Laufzeit ermittelt werden kann. Um Laufzeitfehler zu vermeiden, fügen Sie diese zweite Klasse hinzu`TrimmerRootAssembly`.

Weitere Informationen zur Verwaltung von Trimmwarnungen finden Sie in der Microsoft.NET-Dokumentation unter Einführung in Trimmwarnungen.

Fehlerbehebung

Fehler: Betriebssystemübergreifende native Kompilierung wird nicht unterstützt.

> Ihre Version des globalen Amazon.Lambda.Tools-.NET-Core-Tools ist veraltet. Aktualisieren Sie auf die neueste Version und versuchen Sie es erneut.

Docker: das Image-Betriebssystem „Linux“ kann auf dieser Plattform nicht verwendet werden.

> Docker ist auf Ihrem System für die Verwendung von Windows-Containern konfiguriert. Wechseln Sie zu Linux-Containern, um die native AOT-Entwicklungsumgebung auszuführen.

Weitere Informationen zu häufigen Fehlern finden Sie im AWS NativeAOT for .NET-Repository unter. GitHub

AWS Lambda-Context-Objekt in C#

Wenn Lambda Ihre Funktion ausführt, wird ein Context-Objekt an den Handler übergeben. Dieses Objekt stellt Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Eigenschaften

- `FunctionName` – Der Name der Lambda-Funktion.
- `FunctionVersion` – Die Version der Funktion.
- `InvokedFunctionArn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `MemoryLimitInMB` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `AwsRequestId` – Der Bezeichner der Aufrufanforderung.
- `LogGroupName` – Protokollgruppe für die Funktion.
- `LogStreamName` – Der Protokollstrom für die Funktionsinstance.
- `RemainingTime` (`TimeSpan`) – Die Anzahl der Millisekunden, die vor der Zeitüberschreitung der Ausführung verbleiben.
- `Identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
- `ClientContext` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.
- `Logger` Das Logger-Objekt für die Funktion.

Sie können die Informationen im `ILambdaContext`-Objekt verwenden, um zu Überwachungszwecken Informationen über den Aufruf Ihrer Funktion auszugeben. Der folgende Code enthält ein Beispiel dafür, wie Sie einem strukturierten Logging-Framework Kontextinformationen hinzufügen können. In diesem Beispiel fügt die Funktion `AwsRequestId` zu den Protokollausgaben hinzu. Die Funktion verwendet auch die `RemainingTime`-Eigenschaft, um eine Aufgabe während des Fluges abzubrechen, wenn die Zeitüberschreitung der Lambda-Funktion bald erreicht ist.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;
```

```
public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request, ILambdaContext context)
    {
        Logger.AppendKey("AwsRequestId", context.AwsRequestId);

        var id = request.PathParameters["id"];

        using var cts = new CancellationTokenSource();

        try
        {
            cts.CancelAfter(context.RemainingTime.Add(TimeSpan.FromSeconds(-1)));

            var databaseRecord = await this._repo.GetById(id, cts.Token);

            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.OK,
                Body = JsonSerializer.Serialize(databaseRecord)
            };
        }
        finally
        {
            cts.Cancel();

            return new APIGatewayProxyResponse
            {
                StatusCode = (int)HttpStatusCode.InternalServerError,
                Body = JsonSerializer.Serialize(databaseRecord)
            };
        }
    }
}
```

Lambda-Funktionsprotokollierung in C#

AWS Lambda überwacht automatisch Lambda-Funktionen und sendet Protokolleinträge an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen zu CloudWatch Logs finden Sie unterVerwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus dem Code Ihrer Funktion auszugeben, können Sie Methoden für die Konsolenklasse verwenden oder eine Protokollierungsbibliothek, die zu `stdout` oder `stderr` schreibt.

Die .NET-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die Berichtszeile enthält die folgenden Details.

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.
- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.

- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Tools und Bibliotheken

Powertools for AWS Lambda (.NET) ist ein Entwickler-Toolkit zur Implementierung von Best Practices für Serverless und zur Steigerung der Entwicklergeschwindigkeit. Das Logging-Serviceprogramm bietet einen für Lambda optimierten Logger, der zusätzliche Informationen zum Funktionskontext all Ihrer Funktionen enthält, wobei die Ausgabe als JSON strukturiert ist. Mit diesem Serviceprogramm können Sie Folgendes tun:

- Erfassung von Schlüsselfeldern aus dem Lambda-Kontext, Kaltstart und Strukturen der Protokollierungsausgabe als JSON
- Protokollieren Sie Ereignisse von Lambda-Aufrufen, wenn Sie dazu aufgefordert werden (standardmäßig deaktiviert)
- Alle Protokolle nur für einen bestimmten Prozentsatz der Aufrufe über Protokollstichproben drucken (standardmäßig deaktiviert)
- Fügen Sie dem strukturierten Protokoll zu einem beliebigen Zeitpunkt zusätzliche Schlüssel hinzu
- Verwenden Sie einen benutzerdefinierten Protokollformatierer (Bring Your Own Formatter), um Protokolle in einer Struktur auszugeben, die mit dem Logging RFC Ihres Unternehmens kompatibel ist

Verwendung von Powertools für AWS Lambda (.NET) und für strukturiertes Logging AWS SAM

Gehen Sie wie folgt vor, um mithilfe von eine Hello World C#-Beispielanwendung mit integrierten Powertools for AWS Lambda (.NET) -Modulen herunterzuladen, zu erstellen und bereitzustellen. AWS SAM Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im

Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine `hello world`-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- .NET 6 oder .NET 8
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mithilfe der Hello TypeScript World-Vorlage.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type
 Zip --runtime dotnet6 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl -X GET <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam logs aus, um die Protokolle für die Funktion abzurufen. Weitere Informationen finden Sie unter Arbeiten mit Protokollen im AWS Serverless Application Model - Entwicklerhandbuch.

```
sam logs --stack-name sam-app
```

Das Ergebnis sieht folgendermaßen aus:

```
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8
 2023-02-20T14:15:27.988000 INIT_START Runtime Version:
 dotnet:6.v13        Runtime Version ARN: arn:aws:lambda:ap-
southeast-2::runtime:699f346a05dae24c58c45790bc4089f252bf17dae3997e79b17d939a288aa1ec
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:28.229000
 START RequestId: bed25b38-d012-42e7-ba28-f272535fb80e Version: $LATEST
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:29.259000
 2023-02-20T14:15:29.201Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
   {"_aws":{"Timestamp":1676902528962,"CloudWatchMetrics":[{"Namespace":"sam-
app-logging","Metrics":[{"Name":"ColdStart","Unit":"Count"}],"Dimensions":
[["FunctionName"],["Service"]]}]},"FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","Service":"PowertoolsHelloWorld","ColdStart":1}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.479000
 2023-02-20T14:15:30.479Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
 {"ColdStart":true,"XrayTraceId":"1-63f3807f-5dbcb9910c96f50742707542","CorrelationId":"d3d
a549-4d67b2fdc015","FunctionName":"sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionVersion":"$LATEST","FunctionMemorySize":256,"FunctionArn":"arn:aws:l
southeast-2:123456789012:function:sam-app-HelloWorldFunction-
haKIoVeose2p","FunctionRequestId":"bed25b38-d012-42e7-ba28-
f272535fb80e","Timestamp":"2023-02-20T14:15:30.4602970Z","Level":"Information","Service":"P
 world API - HTTP 200"}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.599000
 2023-02-20T14:15:30.599Z        bed25b38-d012-42e7-ba28-f272535fb80e    info
   {"_aws":{"Timestamp":1676902528922,"CloudWatchMetrics":[{"Namespace":"sam-
```

```
app-logging","Metrics":[{"Name":"ApiRequestCount","Unit":"Count"}],"Dimensions":
[["Service"]]}]},"Service":"PowertoolsHelloWorld","ApiRequestCount":1}
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.680000 END
 RequestId: bed25b38-d012-42e7-ba28-f272535fb80e
2023/02/20/[$LATEST]4eaf8445ba7a4a93b999cb17fbfbecd8 2023-02-20T14:15:30.680000
 REPORT RequestId: bed25b38-d012-42e7-ba28-f272535fb80e  Duration: 2450.99 ms
  Billed Duration: 2451 ms Memory Size: 256 MB     Max Memory Used: 74 MB  Init
 Duration: 240.05 ms
XRAY TraceId: 1-63f3807f-5dbcb9910c96f50742707542       SegmentId: 16b362cd5f52cba0
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

Verwalten der Protokollaufbewahrung

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um zu vermeiden, dass Protokolle auf unbestimmte Zeit gespeichert werden, löschen Sie die Protokollgruppe oder konfigurieren Sie einen Aufbewahrungszeitraum, nach dessen Ablauf die Protokolle CloudWatch automatisch gelöscht werden. Um die Aufbewahrung von Protokollen einzurichten, fügen Sie Ihrer AWS SAM Vorlage Folgendes hinzu:

```
Resources:
  HelloWorldFunction:
    Type: AWS::Serverless::Function
    Properties:
      # Omitting other properties

  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: !Sub "/aws/lambda/${HelloWorldFunction}"
      RetentionInDays: 7
```

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der CloudWatch Konsole

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Logs für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
```

```
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```

Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Instrumentierung von C#-Code in AWS Lambda

Lambda lässt sich integrieren AWS X-Ray , um Ihnen zu helfen, Lambda-Anwendungen zu verfolgen, zu debuggen und zu optimieren. Sie können mit X-Ray eine Anforderung verfolgen, während sie Ressourcen in Ihrer Anwendung durchläuft, die Lambda-Funktionen und andere AWS -Services enthalten können.

Um Protokollierungsdaten an X-Ray zu senden, können Sie eine von drei SDK-Bibliotheken verwenden:

- AWS Distro for OpenTelemetry (ADOT) — Eine sichere, produktionsbereite und AWS unterstützte Distribution des (OTel) SDK. OpenTelemetry
- AWS X-Ray SDK for .NET – Ein SDK zum Generieren und Senden von Nachverfolgungsdaten an X-Ray.
- Powertools for AWS Lambda (.NET) — Ein Entwickler-Toolkit zur Implementierung von Best Practices für Serverless und zur Steigerung der Entwicklergeschwindigkeit.

Jedes der SDKs bietet Möglichkeiten, Ihre Telemetriedaten an den X-Ray Service zu senden. Sie können dann mit X-Ray die Leistungsmetriken Ihrer Anwendung anzeigen, filtern und erhalten, um Probleme und Möglichkeiten zur Optimierung zu identifizieren.

> **Important**
>
> X-Ray und Powertools für AWS Lambda SDKs sind Teil einer eng integrierten Instrumentierungslösung von. AWS Die ADOT Lambda Layers sind Teil eines branchenweiten Standards für die Verfolgung von Instrumenten, die im Allgemeinen mehr Daten erfassen, aber möglicherweise nicht für alle Anwendungsfälle geeignet sind. Sie können die end-to-end Ablaufverfolgung in X-Ray mit beiden Lösungen implementieren. Weitere Informationen zur Auswahl zwischen ihnen finden Sie unter Auswählen zwischen der AWS -Distro für Open Telemetry und X-Ray-SDKs.

Sections

- Aktivieren der Nachverfolgung mit der Lambda-API
- Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation
- Interpretieren einer X-Ray-Nachverfolgung

Verwenden von Powertools für AWS Lambda (.NET) und AWS SAM für die Ablaufverfolgung

Gehen Sie wie folgt vor, um mithilfe von eine Hello World C#-Beispielanwendung mit integrierten Powertools for AWS Lambda (.NET) -Modulen herunterzuladen, zu erstellen und bereitzustellen. AWS SAM Diese Anwendung implementiert ein grundlegendes API-Backend und verwendet Powertools zum Ausgeben von Protokollen, Metriken und Traces. Es besteht aus einem Amazon-API-Gateway-Endpunkt und einer Lambda-Funktion. Wenn Sie eine GET-Anfrage an den API-Gateway-Endpunkt senden, ruft die Lambda-Funktion Logs und Metriken auf, sendet sie im Embedded Metric Format an CloudWatch und sendet Traces an. AWS X-Ray Die Funktion gibt eine Hello-World-Nachricht zurück.

Voraussetzungen

Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- .NET 6 oder .NET 8
- AWS CLI Version 2
- AWS SAM CLI Version 1.75 oder höher. Wenn Sie eine ältere Version der AWS SAM CLI haben, finden Sie weitere Informationen unter Upgrade der AWS SAM CLI.

Stellen Sie eine AWS SAM Beispielanwendung bereit

1. Initialisieren Sie die Anwendung mithilfe der Hello TypeScript World-Vorlage.

```
sam init --app-template hello-world-powertools-dotnet --name sam-app --package-type
 Zip --runtime dotnet6 --no-tracing
```

2. Entwickeln Sie die App.

```
cd sam-app && sam build
```

3. Stellen Sie die Anwendung bereit.

```
sam deploy --guided
```

4. Folgen Sie den Anweisungen auf dem Bildschirm. Um die im interaktiven Erlebnis bereitgestellten Standardoptionen zu akzeptieren, drücken Sie `Enter`.

> **Note**
>
> Für ist HelloWorldFunction möglicherweise keine Autorisierung definiert. Ist das in Ordnung? , stellen Sie sicher, dass Sie eintreteny.

5. Rufen Sie die URL der bereitgestellten Anwendung ab:

```
aws cloudformation describe-stacks --stack-name sam-app --query
 'Stacks[0].Outputs[?OutputKey==`HelloWorldApi`].OutputValue' --output text
```

6. Rufen Sie den API-Endpunkt auf:

```
curl <URL_FROM_PREVIOUS_STEP>
```

Wenn der Link erfolgreich ausgeführt wurde, sehen Sie die folgende Antwort:

```
{"message":"hello world"}
```

7. Führen Sie sam traces aus, um die Traces für die Funktion zu erhalten.

```
sam traces
```

Das Nachverfolgungsergebnis sieht folgendermaßen aus:

```
New XRay Service Graph
  Start time: 2023-02-20 23:05:16+08:00
  End time: 2023-02-20 23:05:16+08:00
  Reference Id: 0 - AWS::Lambda - sam-app-HelloWorldFunction-pNjujb7mEoew - Edges:
 [1]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
```

```
    - total response time: 2.814
  Reference Id: 1 - AWS::Lambda::Function - sam-app-HelloWorldFunction-pNjujb7mEoew
 - Edges: []
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 2.429
  Reference Id: 2 - (Root) AWS::ApiGateway::Stage - sam-app/Prod - Edges: [0]
   Summary_statistics:
     - total requests: 1
     - ok count(2XX): 1
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 2.839
  Reference Id: 3 - client - sam-app/Prod - Edges: [2]
   Summary_statistics:
     - total requests: 0
     - ok count(2XX): 0
     - error count(4XX): 0
     - fault count(5XX): 0
     - total response time: 0

XRay Event [revision 3] at (2023-02-20T23:05:16.521000) with id
 (1-63f38c2c-270200bf1d292a442c8e8a00) and duration (2.877s)
 - 2.839s - sam-app/Prod [HTTP: 200]
   - 2.836s - Lambda [HTTP: 200]
 - 2.814s - sam-app-HelloWorldFunction-pNjujb7mEoew [HTTP: 200]
 - 2.429s - sam-app-HelloWorldFunction-pNjujb7mEoew
   - 0.230s - Initialization
   - 2.389s - Invocation
     - 0.600s - ## FunctionHandler
       - 0.517s - Get Calling IP
   - 0.039s - Overhead
```

8. Dies ist ein öffentlicher API-Endpunkt, der über das Internet zugänglich ist. Es wird empfohlen, dass Sie den Endpunkt nach dem Testen löschen.

```
sam delete
```

X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

Instrumentierung Ihrer .NET-Funktionen mithilfe von X-Ray-SDK

Sie können Ihren Funktionscode instrumentieren, um Metadaten aufzuzeichnen und Downstream-Aufrufe zu verfolgen. Um Details zu Aufrufen aufzuzeichnen, die Ihre Funktion an andere Ressourcen und Dienste vornimmt, verwenden Sie das AWS X-Ray SDK for .NET. Um das SDK zu erhalten, fügen Sie die `AWSXRayRecorder`-Pakete Ihrer Projektdatei hinzu.

```
<Project Sdk="Microsoft.NET.Sdk">
  <PropertyGroup>
    <TargetFramework>net8.0</TargetFramework>
    <GenerateRuntimeConfigurationFiles>true</GenerateRuntimeConfigurationFiles>
    <AWSProjectType>Lambda</AWSProjectType>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Amazon.Lambda.Core" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.SQSEvents" Version="2.1.0" />
    <PackageReference Include="Amazon.Lambda.Serialization.Json" Version="2.1.0" />
    <PackageReference Include="AWSSDK.Core" Version="3.7.103.24" />
    <PackageReference Include="AWSSDK.Lambda" Version="3.7.104.3" />
    <PackageReference Include="AWSXRayRecorder.Core" Version="2.13.0" />
    <PackageReference Include="AWSXRayRecorder.Handlers.AwsSdk" Version="2.11.0" />
  </ItemGroup>
</Project>
```

Es gibt eine Reihe von Nuget-Paketen, die automatische Instrumentierung für AWS SDKs, Entity Framework und HTTP-Anfragen bieten. Den vollständigen Satz der Konfigurationsoptionen finden Sie unter AWS X-Ray SDK for .NET im AWS X-Ray -Entwicklerhandbuch.

Nachdem Sie die gewünschten Nuget-Pakete hinzugefügt haben, konfigurieren Sie die automatische Instrumentierung. Es empfiehlt sich, diese Konfiguration außerhalb der Handler-Funktion Ihrer

Funktion durchzuführen. So können Sie die Wiederverwendung der Ausführungsumgebung nutzen, um die Leistung Ihrer Funktion zu verbessern. Im folgenden Codebeispiel wird die `RegisterXRayForAllServices` Methode im Funktionskonstruktor aufgerufen, um Instrumentierung für alle SDK-Aufrufe hinzuzufügen. AWS

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function()
    {
        // Add auto instrumentation for all AWS SDK calls
        // It is important to call this method before initializing any SDK clients
        AWSSDKHandler.RegisterXRayForAllServices();
        this._repo = new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Aktivieren der Nachverfolgung mit der Lambda-Konsole

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

Aktivieren der Nachverfolgung mit der Lambda-API

Konfigurieren Sie die Ablaufverfolgung für Ihre Lambda-Funktion mit dem AWS CLI oder AWS SDK und verwenden Sie die folgenden API-Operationen:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Die Ablaufverfolgung wird aktiviert mit AWS CloudFormation

Um die Ablaufverfolgung für eine `AWS::Lambda::Function` Ressource in einer AWS CloudFormation Vorlage zu aktivieren, verwenden Sie die `TracingConfig` Eigenschaft.

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Interpretieren einer X-Ray-Nachverfolgung

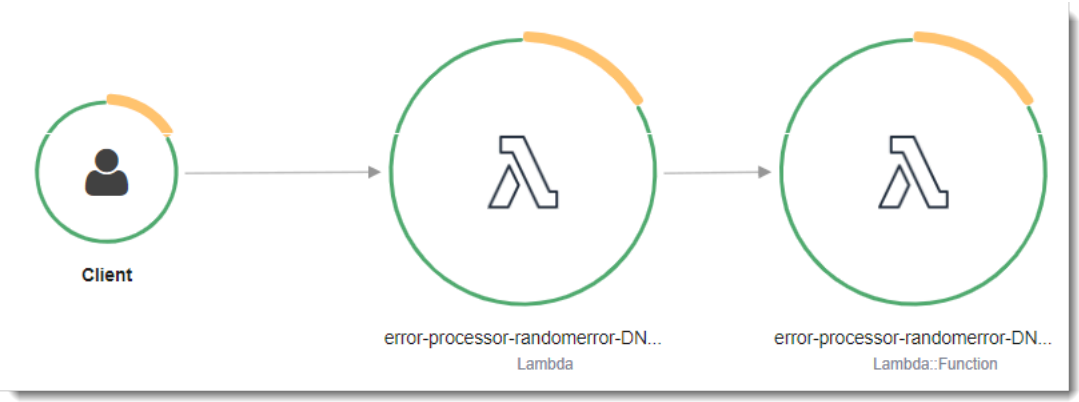
Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray.
Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

Nachdem Sie die aktive Nachverfolgung konfiguriert haben, können Sie bestimmte Anfragen über Ihre Anwendung beobachten. Das X-Ray-Service-Diagramm zeigt Informationen über Ihre Anwendung und alle ihre Komponenten an. Die folgende Abbildung zeigt eine Anwendung mit zwei Funktionen. Die primäre Funktion verarbeitet Ereignisse und gibt manchmal Fehler zurück. Die zweite Funktion an oberster Stelle verarbeitet Fehler, die in der Protokollgruppe der ersten auftreten, und verwendet das AWS SDK, um X-Ray, Amazon Simple Storage Service (Amazon S3) und Amazon CloudWatch Logs aufzurufen.

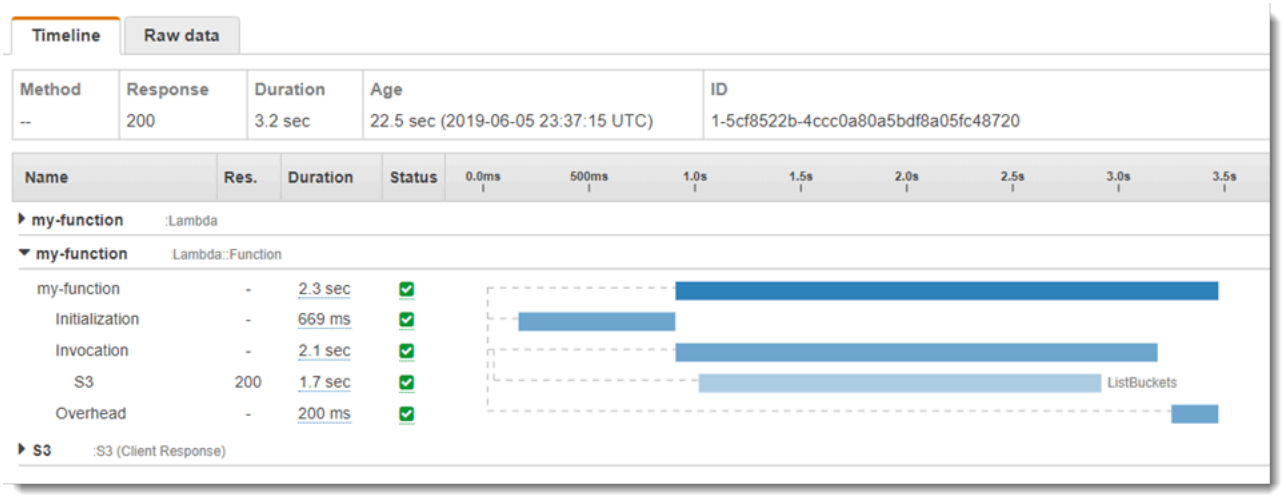
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



In diesem Beispiel wird das `AWS::Lambda::Function` Segment erweitert, sodass seine drei Untersegmente angezeigt werden:

- Initialisierung – Stellt die Zeit dar, die für das Laden Ihrer Funktion und das Ausführen des Initialisierungscodes aufgewendet wurde. Dieses Untersegment erscheint nur für das erste Ereignis, das jede Instance Ihrer Funktion verarbeitet.
- Invocation (Aufruf) – Stellt die Zeit dar, die beim Ausführen Ihres Handler-Codes vergeht.
- Overhead (Aufwand) – Stellt die Zeit dar, die von der Lambda-Laufzeitumgebung bei der Verarbeitung des nächsten Ereignisses verbraucht wird.

Sie können auch HTTP-Clients instrumentieren, SQL-Abfragen aufzeichnen und benutzerdefinierte Untersegmente mit Anmerkungen und Metadaten erstellen. Weitere Informationen finden Sie unter AWS X-Ray SDK for .NET im AWS X-Ray -Entwicklerhandbuch.

> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-

Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

AWS Lambda-Funktions-Testing in C#

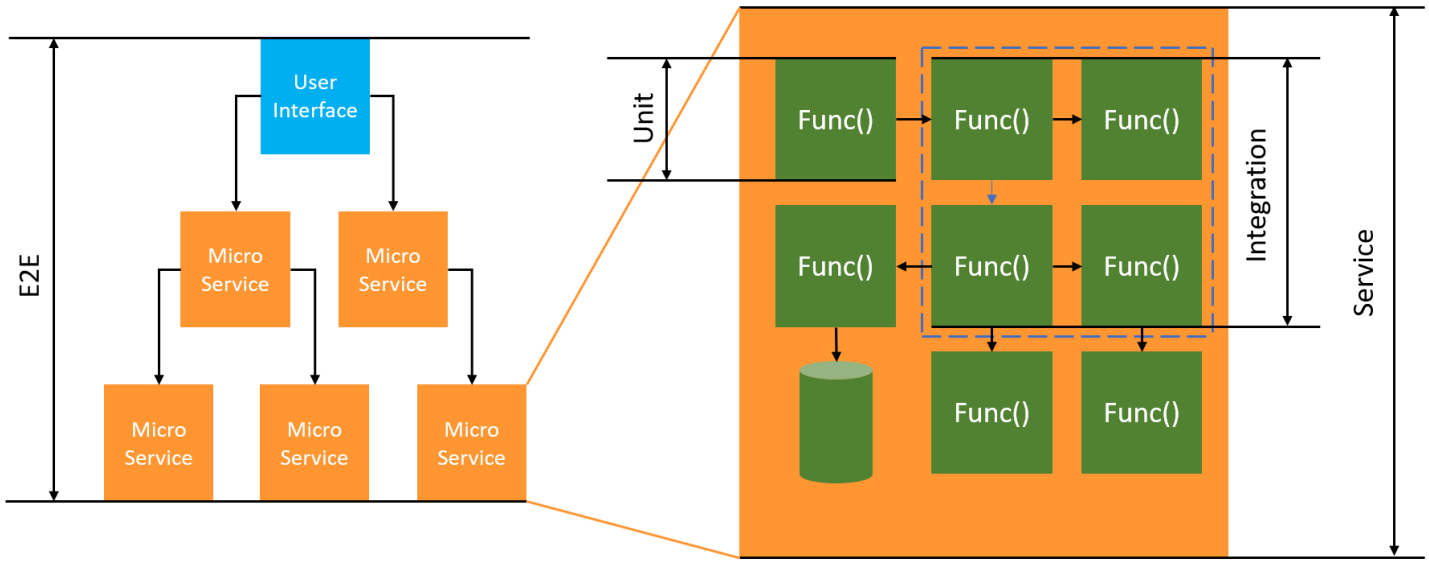
> **Note**
>
> Im Kapitel Testen von Funktionen finden Sie eine vollständige Einführung in Techniken und bewährte Methoden für das Testen von Serverless-Lösungen.

Beim Testen der Serverless-Funktionen werden herkömmliche Testtypen und -techniken verwendet. Erwägen Sie jedoch auch das Testen der Serverless-Anwendungen als Ganzes. Cloud-basierte Tests bieten das genaueste Maß für die Qualität sowohl Ihrer Funktionen als auch Ihrer Serverless-Anwendungen.

Eine Serverless-Anwendungsarchitektur umfasst verwaltete Services, die über API-Aufrufe wichtige Anwendungsfunktionen bereitstellen. Aus diesem Grund muss Ihr Entwicklungszyklus automatisierte Tests beinhalten, die bei der Interaktion Ihrer Funktionen und Services die Funktionalität überprüfen.

Wenn Sie keine cloud-basierten Tests erstellen, können aufgrund von Unterschieden zwischen Ihrer lokalen Umgebung und der bereitgestellten Umgebung Probleme auftreten. Ihr kontinuierlicher Integrationsprozess muss Tests anhand einer Reihe von Ressourcen durchführen, die in der Cloud bereitgestellt werden, bevor Ihr Code in die nächste Bereitstellungsumgebung wie QA, Staging oder Produktion übertragen wird.

Lesen Sie diesen kurzen Leitfaden weiter, um weitere Informationen zu Teststrategien für Serverless-Anwendungen zu erhalten, oder besuchen Sie das Serverless Test Samples Repository, um praktische Beispiele zu finden, die sich speziell auf die gewählte Sprache und Laufzeit beziehen.



Für Serverless-Tests schreiben Sie immer noch Einheiten , Integration und end-to-end Tests.

- Einheitentests — Tests, die an einem isolierten Codeblock ausgeführt werden. Zum Beispiel die Überprüfung der Geschäftslogik zur Berechnung der Bereitstellungskosten für einen bestimmten Artikel und Bestimmungsort.
- Integrationstests — Tests, an denen zwei oder mehr Komponenten oder Dienste beteiligt sind, die interagieren, in der Regel in einer Cloud-Umgebung. Bei der Überprüfung einer Funktion werden beispielsweise Ereignisse aus einer Warteschlange verarbeitet.
- E-nd-to-end Tests – Tests, die das Verhalten einer gesamten Anwendung überprüfen. Stellen Sie beispielsweise sicher, dass die Infrastruktur korrekt eingerichtet ist und die Ereignisse zwischen den Services wie erwartet ablaufen, um die Bestellungen der Kunden aufzuzeichnen.

Testen Ihrer Serverless-Anwendungen

In der Regel verwenden Sie eine Mischung aus verschiedenen Ansätzen, um Ihren Serverless-Anwendungscode zu testen, einschließlich Tests in der Cloud, Tests mit Mock-Code und gelegentlich Tests mit Emulatoren.

Testen in der Cloud

Tests in der Cloud sind für alle Testphasen nützlich, einschließlich Einheitentests, Integrationstests und end-to-end Tests. Sie führen Tests für Code durch, der in der Cloud bereitgestellt wird und mit cloud-basierten Services interagiert. Dieser Ansatz bietet das genaueste Maß für die Qualität Ihres Codes.

Eine bequeme Möglichkeit, Ihre Lambda-Funktion in der Cloud zu debuggen, ist die Verwendung der Konsole mit einem Testereignis. Ein Testereignis ist eine JSON-Eingabe für Ihre Funktion. Wenn Ihre Funktion keine Eingabe erfordert, kann das Ereignis ein leeres JSON-Dokument (`{}`) sein. Die Konsole bietet Beispielereignisse für eine Vielzahl von Service-Integrationen. Nachdem Sie ein Ereignis in der Konsole erstellt haben, können Sie es mit Ihrem Team teilen, um das Testen einfacher und einheitlicher zu gestalten.

> **Note**
>
> Das Testen einer Funktion in der Konsole ist ein schneller Einstieg, aber die Automatisierung Ihrer Testzyklen gewährleistet die Anwendungsqualität und die Entwicklungsgeschwindigkeit.

Test-Tools

Um Ihren Entwicklungszyklus zu beschleunigen, gibt es eine Reihe von Tools und Techniken, die Sie beim Testen Ihrer Funktionen verwenden können. AWS SAMAccelerate und AWS CDKWatch Mode reduzieren beispielsweise beide die Zeit, die für die Aktualisierung von Cloud-Umgebungen benötigt wird.

Die Art und Weise, wie Sie Ihren Lambda-Funktionscode definieren, macht es einfach, Komponententests hinzuzufügen. Lambda benötigt einen öffentlichen, parameterlosen Konstruktor, um Ihre Klasse zu initialisieren. Durch die Einführung eines zweiten, internen Konstruktors haben Sie die Kontrolle über die Abhängigkeiten, die Ihre Anwendung verwendet.

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSerializer

namespace GetProductHandler;

public class Function
{
    private readonly IDatabaseRepository _repo;

    public Function(): this(null)
    {
    }

    internal Function(IDatabaseRepository repo)
    {
```

```
        this._repo = repo ?? new DatabaseRepository();
    }

    public async Task<APIGatewayProxyResponse> FunctionHandler(APIGatewayProxyRequest
 request)
    {
        var id = request.PathParameters["id"];

        var databaseRecord = await this._repo.GetById(id);

        return new APIGatewayProxyResponse
        {
            StatusCode = (int)HttpStatusCode.OK,
            Body = JsonSerializer.Serialize(databaseRecord)
        };
    }
}
```

Um einen Test für diese Funktion zu schreiben, können Sie eine neue Instance Ihrer `Function`-Klasse initialisieren und eine simulierte Implementierung von `IDatabaseRepository` übergeben. Die folgenden Beispiele verwenden `XUnit`, `Moq` und `FluentAssertions`, um einen einfachen Test zu schreiben, der sicherstellt, dass `FunctionHandler` einen 200-Statuscode zurückgibt.

```
using Xunit;
using Moq;
using FluentAssertions;

public class FunctionTests
{
    [Fact]
    public async Task TestLambdaHandler_WhenInputIsValid_ShouldReturn200StatusCode()
    {
        // Arrange
        var mockDatabaseRepository = new Mock<IDatabaseRepository>();

        var functionUnderTest = new Function(mockDatabaseRepository.Object);

        // Act
        var response = await functionUnderTest.FunctionHandler(new
 APIGatewayProxyRequest());

        // Assert
        response.StatusCode.Should().Be(200);
```

```
    }
}
```

Ausführlichere Beispiele, einschließlich Beispiele für asynchrone Tests, finden Sie im Repository mit .NET-Testbeispielen auf GitHub.

Aufbau von Lambda-Funktionen mit PowerShell

In den folgenden Abschnitten wird erklärt, wie gängige Programmiermuster und Kernkonzepte beim Verfassen von Lambda-Funktionscode in PowerShell angewendet werden.

Lambda bietet die folgenden Beispielanwendungen für PowerShell:

- blank-powershell — Eine PowerShell Funktion, die die Verwendung von Logging, Umgebungsvariablen und dem SDK veranschaulicht. AWS

Bevor Sie beginnen, müssen Sie zunächst eine PowerShell Entwicklungsumgebung einrichten. Anweisungen dazu finden Sie unter Einrichten einer PowerShell Entwicklungsumgebung.

Weitere Informationen zur Verwendung des AWSLambdaPSCore Moduls zum Herunterladen von PowerShell Beispielprojekten aus Vorlagen, zum Erstellen von PowerShell Bereitstellungspaketen und zum Bereitstellen von PowerShell Funktionen in der AWS Cloud finden Sie unterBereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven.

Lambda stellt die folgenden Laufzeiten für .NET-Sprachen bereit:

.NET

Name	ID	Betriebssystem	Datum der Veraltung	Blockfunktion erstellen	Blockfunktion aktualisieren
.NET 8	`dotnet8`	Amazon Linux 2023			
.NET 6	`dotnet6`	Amazon Linux 2	12. November 2	28. Februar 2025	31. März 2025

Themen

Einrichten einer PowerShell Entwicklungsumgebung

Lambda bietet eine Reihe von Tools und Bibliotheken für die PowerShell Laufzeit. Installationsanweisungen finden Sie unter Lambda-Tools für PowerShell auf GitHub.

Das AWSLambdaPSCore Modul enthält die folgenden Cmdlets, um das Erstellen und Veröffentlichen von PowerShell Lambda-Funktionen zu unterstützen:

- Get-AWSPowerShellLambdaTemplate – Gibt eine Liste der Vorlagen für die ersten Schritte zurück.
- Neu –AWSPowerShellLambda Erstellt ein anfängliches PowerShell Skript basierend auf einer Vorlage.
- Publish-AWSPowerShellLambda – Veröffentlicht ein bestimmtes PowerShell Skript in Lambda.
- Neu –AWSPowerShellLambdaPackage Erstellt ein Lambda-Bereitstellungspaket, das Sie in einem CI/CD-System für die Bereitstellung verwenden können.

Bereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven

Ein Bereitstellungspaket für die PowerShell Laufzeit enthält Ihr PowerShell Skript, PowerShell Module, die für Ihr PowerShell Skript erforderlich sind, und die Komponenten, die zum Hosten von PowerShell Core erforderlich sind.

Erstellen der Lambda-Funktion

Um mit dem Schreiben und Aufrufen eines PowerShell Skripts mit Lambda zu beginnen, können Sie das `New-AWSPowerShellLambda` -Cmdlet verwenden, um ein Starter-Skript basierend auf einer Vorlage zu erstellen. Sie können das `Publish-AWSPowerShellLambda`-Cmdlet verwenden, um Ihr Skript in Lambda bereitzustellen. Anschließend können Sie Ihr Skript entweder über die Befehlszeile oder die Lambda-Konsole testen.

Gehen Sie wie folgt vor, um ein neues PowerShell Skript zu erstellen, es hochzuladen und zu testen:

1. Führen Sie den folgenden Befehl aus, um die Liste der verfügbaren Vorlagen anzuzeigen:

   ```
   PS C:\> Get-AWSPowerShellLambdaTemplate

   Template               Description
   --------               -----------
   Basic                  Bare bones script
   CodeCommitTrigger      Script to process AWS CodeCommit Triggers
   ...
   ```

2. Führen Sie den folgenden Befehl aus, um ein Beispielskript anhand der `Basic`-Vorlage zu erstellen:

   ```
   New-AWSPowerShellLambda -ScriptName MyFirstPSScript -Template Basic
   ```

   Eine neue Datei mit dem Namen `MyFirstPSScript.ps1` wird in einem neuen Unterverzeichnis des aktuellen Verzeichnisses erstellt. Der Name des Verzeichnisses basiert auf dem `-ScriptName`-Parameter. Sie können den `-Directory`-Parameter verwenden, um ein alternatives Verzeichnis auswählen.

   Sie können sehen, dass die neue Datei folgenden Inhalt hat:

```
# PowerShell script file to run as a Lambda function
#
# When executing in Lambda the following variables are predefined.
#   $LambdaInput - A PSObject that contains the Lambda function input data.
#   $LambdaContext - An Amazon.Lambda.Core.ILambdaContext object that contains
 information about the currently running Lambda environment.
#
# The last item in the PowerShell pipeline is returned as the result of the Lambda
 function.
#
# To include PowerShell modules with your Lambda function, like the
 AWSPowerShell.NetCore module, add a "#Requires" statement
# indicating the module and version.

#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}

# Uncomment to send the input to CloudWatch Logs
# Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
```

3. Um zu sehen, wie Protokollnachrichten von Ihrem PowerShell Skript an Amazon CloudWatch Logs gesendet werden, kommentieren Sie die `Write-Host` Zeile des Beispielskripts aus.

   Um zu veranschaulichen, wie Sie Daten von Ihren Lambda-Funktionen zurückgeben können, fügen Sie mit `$PSVersionTable` eine neue Zeile am Ende des Skripts hinzu. Dadurch wird `$PSVersionTable` der PowerShell Pipeline hinzugefügt. Nachdem das PowerShell Skript abgeschlossen ist, ist das letzte Objekt in der PowerShell Pipeline die Rückgabedaten für die Lambda-Funktion. `$PSVersionTable` ist eine PowerShell globale Variable, die auch Informationen über die laufende Umgebung bereitstellt.

   Nachdem Sie alle Änderungen vorgenommen haben, sehen die beiden letzten Zeilen des Beispielskripts wie folgt aus:

   ```
   Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 5)
   $PSVersionTable
   ```

4. Nachdem Sie die `MyFirstPSScript.ps1`-Datei bearbeitet haben, ändern Sie das Verzeichnis in den Speicherort des Skripts. Führen Sie anschließend führen Sie den folgenden Befehl aus, um das Skript in Lambda zu veröffentlichen:

```
Publish-AWSPowerShellLambda -ScriptPath .\MyFirstPSScript.ps1 -Name
 MyFirstPSScript -Region us-east-2
```

Beachten Sie, dass der `-Name`-Parameter den Lambda-Funktionsnamen angibt, der in der Lambda-Konsole angezeigt wird. Sie können diese Funktion auch verwenden, um Ihr Skript manuell aufzurufen.

5. Rufen Sie Ihre Funktion mit dem AWS Command Line Interface (AWS CLI) `invoke`-Befehl auf.

```
> aws lambda invoke --function-name MyFirstPSScript out
```

Definieren Sie den Lambda-Funktionshandler in PowerShell

Wenn eine Lambda-Funktion aufgerufen wird, ruft der Lambda-Handler das Skript auf. PowerShell

Wenn das PowerShell Skript aufgerufen wird, sind die folgenden Variablen vordefiniert:

- *$ LambdaInput* — Ein PSObject, das die Eingabe für den Handler enthält. Diese Eingabedaten können (von einer Ereignisquelle veröffentlichte) Ereignisdaten oder beliebige andere Eingabedaten sein, die Sie in Form einer Zeichenfolge oder eines benutzerdefinierten Datenobjekts übergeben.
- *$ LambdaContext* — Ein LambdaContext Amazon.Lambda.Core.I-Objekt, mit dem Sie auf Informationen über den aktuellen Aufruf zugreifen können, z. B. den Namen der aktuellen Funktion, das Speicherlimit, die verbleibende Ausführungszeit und die Protokollierung.

Betrachten PowerShell Sie zum Beispiel den folgenden Beispielcode.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host 'Function Name:' $LambdaContext.FunctionName
```

Dieses Skript gibt die FunctionName Eigenschaft zurück, die aus der LambdaContext Variablen $ abgerufen wurde.

> **Note**
>
> Sie müssen die `#Requires` Anweisung in Ihren PowerShell Skripten verwenden, um anzugeben, von welchen Modulen Ihre Skripten abhängen. Diese Anweisung erfüllt zwei wichtige Aufgaben. 1) Es teilt anderen Entwicklern mit, welche Module das Skript verwendet, und 2) es identifiziert die abhängigen Module, die AWS PowerShell Tools im Rahmen der Bereitstellung mit dem Skript paketieren müssen. Weitere Informationen zu der `#Requires` Anweisung in finden Sie PowerShell unter About requires. Weitere Informationen zu PowerShell Bereitstellungspaketen finden Sie unterBereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven.
>
> Wenn Ihre PowerShell Lambda-Funktion die AWS PowerShell Cmdlets verwendet, stellen Sie sicher, dass Sie eine `#Requires` Anweisung festlegen, die auf das `AWSPowerShell.NetCore` Modul verweist, das PowerShell Core unterstützt, und nicht auf das `AWSPowerShell` Modul, das nur Windows unterstützt. PowerShell Stellen Sie zudem sicher, dass Sie `AWSPowerShell.NetCore` Version 3.3.270.0 oder höher verwenden, da

diese den Cmdlet-Importvorgang optimiert. Mit älteren Versionen dauern Kaltstarts länger. Weitere Informationen finden Sie unter AWS Tools for PowerShell.

Zurückgeben von Daten

Einige Lambda-Aufrufe sollen Daten zurück an ihren Aufrufer zurückgeben. Beispiel: Wenn ein Aufruf als Reaktion auf eine Webanforderung aus API Gateway erfolgt ist, muss unsere Lambda-Funktion die Antwort zurückgeben. Für PowerShell Lambda sind das letzte Objekt, das der PowerShell Pipeline hinzugefügt wurde, die Rückgabedaten des Lambda-Aufrufs. Wenn es sich bei dem Objekt um eine Zeichenfolge handelt, werden die Daten im Ist-Zustand zurückgegeben. Andernfalls wird das Objekt mithilfe des `ConvertTo-Json`-Cmdlets in JSON konvertiert.

Stellen Sie sich zum Beispiel die folgende PowerShell Anweisung vor, die die Pipeline erweitert: `$PSVersionTable` PowerShell

```
$PSVersionTable
```

Nachdem das PowerShell Skript abgeschlossen ist, sind die Rückgabedaten für die Lambda-Funktion das letzte Objekt in der PowerShell Pipeline. `$PSVersionTable`ist eine PowerShell globale Variable, die auch Informationen über die laufende Umgebung bereitstellt.

AWS Lambda -Kontextobjekt in PowerShell

Wenn Lambda Ihre Funktion ausführt, werden Context-Informationen übergeben, indem eine `$LambdaContext`-Variable für den Handler verfügbar gemacht wird. Diese Variable stellt Methoden und Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Eigenschaften

- `FunctionName` – Der Name der Lambda-Funktion.
- `FunctionVersion` – Die Version der Funktion.
- `InvokedFunctionArn` – Der Amazon-Ressourcenname (ARN), der zum Aufrufen der Funktion verwendet wird. Gibt an, ob der Aufrufer eine Versionsnummer oder einen Alias angegeben hat.
- `MemoryLimitInMB` – Die Menge an Arbeitsspeicher, die der Funktion zugewiesen ist.
- `AwsRequestId` – Der Bezeichner der Aufrufanforderung.
- `LogGroupName` – Protokollgruppe für die Funktion.
- `LogStreamName` – Der Protokollstrom für die Funktionsinstance.
- `RemainingTime` – Die Anzahl der Millisekunden, die vor der Zeitüberschreitung der Ausführung verbleiben.
- `Identity` – Informationen zur Amazon-Cognito-Identität, die die Anforderung autorisiert hat.
- `ClientContext` – (mobile Apps) Clientkontext, der Lambda von der Clientanwendung bereitgestellt wird.
- `Logger` – Das Logger-Objekt für die Funktion.

Der folgende PowerShell Codeausschnitt zeigt eine einfache Handler-Funktion, die einige der Kontextinformationen druckt.

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host 'Function name:' $LambdaContext.FunctionName
Write-Host 'Remaining milliseconds:' $LambdaContext.RemainingTime.TotalMilliseconds
Write-Host 'Log group name:' $LambdaContext.LogGroupName
Write-Host 'Log stream name:' $LambdaContext.LogStreamName
```

AWS Lambda Funktion einloggen PowerShell

AWS Lambda überwacht automatisch Lambda-Funktionen in Ihrem Namen und sendet Protokolle an Amazon CloudWatch. Ihre Lambda-Funktion enthält eine CloudWatch Logs-Log-Gruppe und einen Log-Stream für jede Instanz Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda.

Auf dieser Seite wird beschrieben, wie Sie Protokollausgaben aus dem Code Ihrer Lambda-Funktion erstellen oder mit der AWS Command Line Interface Lambda-Konsole oder der CloudWatch Konsole auf Logs zugreifen.

Sections

Erstellen einer Funktion, die Protokolle zurückgibt

Um Protokolle aus Ihrem Funktionscode auszugeben, können Sie Cmdlets auf Microsoft verwenden. PowerShell.Utility oder ein beliebiges Protokollierungsmodul, das in oder schreibt. `stdout` `stderr` Im folgenden Beispiel wird verwende `Write-Host`.

Example function/Handler.ps1 – Protokollierung

```
#Requires -Modules @{ModuleName='AWSPowerShell.NetCore';ModuleVersion='3.3.618.0'}
Write-Host `## Environment variables
Write-Host AWS_LAMBDA_FUNCTION_VERSION=$Env:AWS_LAMBDA_FUNCTION_VERSION
Write-Host AWS_LAMBDA_LOG_GROUP_NAME=$Env:AWS_LAMBDA_LOG_GROUP_NAME
Write-Host AWS_LAMBDA_LOG_STREAM_NAME=$Env:AWS_LAMBDA_LOG_STREAM_NAME
Write-Host AWS_EXECUTION_ENV=$Env:AWS_EXECUTION_ENV
Write-Host AWS_LAMBDA_FUNCTION_NAME=$Env:AWS_LAMBDA_FUNCTION_NAME
Write-Host PATH=$Env:PATH
Write-Host `## Event
```

```
Write-Host (ConvertTo-Json -InputObject $LambdaInput -Compress -Depth 3)
```

Example Protokollformat

```
START RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Version: $LATEST
Importing module ./Modules/AWSPowerShell.NetCore/3.3.618.0/AWSPowerShell.NetCore.psd1
[Information] - ## Environment variables
[Information] - AWS_LAMBDA_FUNCTION_VERSION=$LATEST
[Information] - AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/blank-powershell-
function-18CIXMPLHFAJJ
[Information] - AWS_LAMBDA_LOG_STREAM_NAME=2020/04/01/
[$LATEST]53c5xmpl52d64ed3a744724d9c201089
[Information] - AWS_EXECUTION_ENV=AWS_Lambda_dotnet6_powershell_1.0.0
[Information] - AWS_LAMBDA_FUNCTION_NAME=blank-powershell-function-18CIXMPLHFAJJ
[Information] - PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
[Information] - ## Event
[Information] -
{
    "Records": [
        {
            "messageId": "19dd0b57-b21e-4ac1-bd88-01bbb068cb78",
            "receiptHandle": "MessageReceiptHandle",
            "body": "Hello from SQS!",
            "attributes": {
                "ApproximateReceiveCount": "1",
                "SentTimestamp": "1523232000000",
                "SenderId": "123456789012",
                "ApproximateFirstReceiveTimestamp": "1523232000001"
            },
            ...
END RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed
REPORT RequestId: 56639408-xmpl-435f-9041-ac47ae25ceed Duration: 3906.38 ms Billed
 Duration: 4000 ms Memory Size: 512 MB Max Memory Used: 367 MB Init Duration: 5960.19
 ms
XRAY TraceId: 1-5e843da6-733cxmple7d0c3c020510040 SegmentId: 3913xmpl20999446 Sampled:
 true
```

Die .NET-Laufzeit protokolliert die Zeilen `START`, `END` und `REPORT` für jeden Aufruf. Die Berichtszeile enthält die folgenden Details.

Datenfelder für REPORT-Zeilen

- RequestId— Die eindeutige Anforderungs-ID für den Aufruf.

- Dauer – Die Zeit, die die Handler-Methode Ihrer Funktion mit der Verarbeitung des Ereignisses verbracht hat.
- Fakturierte Dauer – Die für den Aufruf fakturierte Zeit.
- Speichergröße – Die der Funktion zugewiesene Speichermenge.
- Max. verwendeter Speicher – Die Speichermenge, die von der Funktion verwendet wird.
- Initialisierungsdauer – Für die erste Anfrage die Zeit, die zur Laufzeit zum Laden der Funktion und Ausführen von Code außerhalb der Handler-Methode benötigt wurde.
- XRAY TraceId — Für verfolgte Anfragen die AWS X-Ray Trace-ID.
- SegmentId— Für verfolgte Anfragen die X-Ray-Segment-ID.
- Stichprobe – Bei verfolgten Anforderungen das Stichprobenergebnis.

Verwenden von Lambda-Konsole

Sie können die Lambda-Konsole verwenden, um die Protokollausgabe nach dem Aufrufen einer Lambda-Funktion anzuzeigen.

Wenn Ihr Code über den eingebetteten Code-Editor getestet werden kann, finden Sie Protokolle in den Ausführungsergebnissen. Wenn Sie das Feature Konsolentest verwenden, um eine Funktion aufzurufen, finden Sie die Protokollausgabe im Abschnitt Details.

Verwenden der Konsole CloudWatch

Sie können die CloudWatch Amazon-Konsole verwenden, um Protokolle für alle Lambda-Funktionsaufrufe anzuzeigen.

Um Protokolle auf der Konsole anzuzeigen CloudWatch

1. Öffnen Sie die Seite Protokollgruppen auf der CloudWatch Konsole.
2. Wählen Sie die Protokollgruppe Ihrer Funktion aus (/aws/lambda/***your-function-name***).
3. Wählen Sie eine Protokollstream aus.

Jeder Protokoll-Stream entspricht einer Instance Ihrer Funktion. Ein Protokollstream wird angezeigt, wenn Sie Ihre Lambda-Funktion aktualisieren, und wenn zusätzliche Instances zum Umgang mit mehreren gleichzeitigen Aufrufen erstellt werden. Um Protokolle für einen bestimmten Aufruf zu finden, empfehlen wir, Ihre Funktion mit zu instrumentieren. AWS X-Ray X-Ray erfasst Details zu der Anforderung und dem Protokollstream in der Trace.

Verwenden von () AWS Command Line InterfaceAWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
```

```
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Löschen von Protokollen

Wenn Sie eine Funktion löschen, werden Protokollgruppen nicht automatisch gelöscht. Um das unbegrenzte Speichern von Protokollen zu vermeiden, löschen Sie die Protokollgruppe oder konfigurieren Sie eine Aufbewahrungszeitraum nach dem Protokolle automatisch gelöscht werden.

Erstellen von Lambda-Funktionen mit Rust

Da Rust zu nativem Code kompiliert wird, benötigen Sie keine spezielle Laufzeit, um Rust-Code auf Lambda auszuführen. Verwenden Sie stattdessen den Rust-Laufzeit-Client, um Ihr Projekt lokal zu erstellen, und stellen Sie es dann mithilfe der `provided.al2023`- oder `provided.al2`-Laufzeit auf Lambda bereit. Wenn Sie `provided.al2023` oder `provided.al2` verwenden, hält Lambda das Betriebssystem automatisch mit den neuesten Patches auf dem neuesten Stand.

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Tools und Bibliotheken für Rust

- AWS SDK for Rust: Das AWS SDK für Rust bietet Rust-APIs für die Interaktion mit den Infrastrukturdiensten von Amazon Web Services.
- Rust-Laufzeit-Client für Lambda: Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er unterliegt grundlegenden Änderungen und wird nicht für die Produktion empfohlen.
- Cargo Lambda: Diese Bibliothek bietet eine Befehlszeilenanwendung für die Arbeit mit Lambda-Funktionen, die mit Rust erstellt wurden.
- Lambda HTTP: Diese Bibliothek bietet einen Wrapper für die Arbeit mit HTTP-Ereignissen.
- Lambda-Erweiterung: Diese Bibliothek bietet Unterstützung für das Schreiben von Lambda-Erweiterungen mit Rust.
- AWS Lambda Ereignisse: Diese Bibliothek bietet Typdefinitionen für gängige Integrationen mit Ereignisquellen.

Beispiele für Lambda-Anwendungen für Rust

- Grundlegende Lambda-Funktion: Eine Rust-Funktion, die zeigt, wie grundlegende Ereignisse verarbeitet werden.
- Lambda-Funktion mit Fehlerbehandlung: Eine Rust-Funktion, die zeigt, wie benutzerdefinierte Rust-Fehler in Lambda behandelt werden.

- Lambda-Funktion mit gemeinsam genutzten Ressourcen: Ein Rust-Projekt, das gemeinsam genutzte Ressourcen initialisiert, bevor die Lambda-Funktion erstellt wird.
- Lambda-HTTP-Ereignisse: Eine Rust-Funktion, die HTTP-Ereignisse verarbeitet.
- Lambda-HTTP-Ereignisse mit CORS-Headern: Eine Rust-Funktion, die Tower verwendet, um CORS-Header zu injizieren.
- Lambda-REST-API: Eine REST-API, die Axum und Diesel verwendet, um eine Verbindung zu einer PostgreSQL-Datenbank herzustellen.
- Serverlose Rust-Demo: Ein Rust-Projekt, das die Verwendung der Rust-Bibliotheken, der Protokollierung, der Umgebungsvariablen und des SDK von Lambda zeigt. AWS
- Basic Lambda-Erweiterung: Eine Rust-Erweiterung, die zeigt, wie grundlegende Erweiterungsereignisse verarbeitet werden.
- Lambda Logs Amazon Data Firehose Extension: Eine Rust-Erweiterung, die zeigt, wie Lambda-Protokolle an Firehose gesendet werden.

Themen

- Definieren Sie den Lambda-Funktionshandler in Rust
- Lambda-Kontext-Objekt in Rust
- Verarbeitung von HTTP-Ereignissen mit Rust
- Bereitstellen von Lambda-Rust-Funktionen mit ZIP-Dateiarchiven
- Lambda-Funktionsprotokollierung in Rust

Definieren Sie den Lambda-Funktionshandler in Rust

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Der Lambda-Funktionshandler ist die Methode in Ihrem Funktionscode, die Ereignisse verarbeitet. Wenn Ihre Funktion aufgerufen wird, führt Lambda die Handler-Methode aus. Ihre Funktion wird so lange ausgeführt, bis der Handler eine Antwort zurückgibt, beendet wird oder ein Timeout auftritt.

Schreiben Sie Ihren Lambda-Funktionscode als ausführbare Rust-Datei. Implementieren Sie den Handler-Funktionscode und eine Hauptfunktion und fügen Sie Folgendes hinzu:

- Der lambda_runtime Crate von crates.io, den das Lambda-Programmiermodell für Rust implementiert.
- Nehmen Sie Tokio in Ihre Abhängigkeiten auf. Der Rust-Laufzeit-Client für Lambda verwendet Tokio, um asynchrone Aufrufe zu verarbeiten.

Example – Rust-Handler, der JSON-Ereignisse verarbeitet

Im folgenden Beispiel wird der serde_json Crate verwendet, um grundlegende JSON-Ereignisse zu verarbeiten:

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};

async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
 let payload = event.payload;
 let first_name = payload["firstName"].as_str().unwrap_or("world");
 Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
 lambda_runtime::run(service_fn(handler)).await
}
```

Beachten Sie Folgendes:

- `use`: Importiert die Bibliotheken, die Ihre Lambda-Funktion benötigt.
- `async fn main`: Der Eintrittspunkt, von dem aus der Lambda-Funktionscode ausgeführt wird. Der Rust-Laufzeit-Client verwendet Tokio als asynchrone Laufzeit, daher müssen Sie die Hauptfunktion mit `#[tokio::main]` annotieren.
- `async fn handler(event: LambdaEvent<Value>) -> Result<Value,Error>`: Dies ist die Lambda-Handler-Signatur. Sie enthält den Code, der ausgeführt wird, wenn die Funktion aufgerufen wird.
  - `LambdaEvent<Value>`: Dies ist ein generischer Typ, der das von der Lambda-Laufzeit empfangene Ereignis sowie den Lambda-Funktionskontext beschreibt.
  - `Result<Value, Error>`: Die Funktion gibt einen `Result`-Typ zurück. Wenn die Funktion erfolgreich ist, ist das Ergebnis ein JSON-Wert. Wenn die Funktion nicht erfolgreich ist, ist das Ergebnis ein Fehler.

Geteilten Zustand verwenden

Sie können geteilte Variablen deklarieren, die unabhängig vom Handler-Code Ihrer Lambda-Funktion sind. Diese Variablen können Ihnen helfen, Zustandsinformationen während des Init-Phase zu laden, bevor Ihre Funktion Ereignisse empfängt.

Example – Verwenden Sie den Amazon-S3-Client für mehrere Funktions-Instances

Beachten Sie Folgendes:

- `use aws_sdk_s3::Client`: In diesem Beispiel müssen Sie `aws-sdk-s3 = "0.26.0"` zur Liste der Abhängigkeiten in Ihrer `Cargo.toml`-Datei hinzufügen.
- `aws_config::from_env`: In diesem Beispiel müssen Sie `aws-config = "0.55.1"` zur Liste der Abhängigkeiten in Ihrer `Cargo.toml`-Datei hinzufügen.

```
use aws_sdk_s3::Client;
use lambda_runtime::{service_fn, Error, LambdaEvent};
use serde::{Deserialize, Serialize};

#[derive(Deserialize)]
struct Request {
    bucket: String,
}
```

```
#[derive(Serialize)]
struct Response {
    keys: Vec<String>,
}

async fn handler(client: &Client, event: LambdaEvent<Request>) -> Result<Response,
 Error> {
    let bucket = event.payload.bucket;
    let objects = client.list_objects_v2().bucket(bucket).send().await?;
    let keys = objects
        .contents()
        .map(|s| s.iter().flat_map(|o| o.key().map(String::from)).collect())
        .unwrap_or_default();
    Ok(Response { keys })
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    let shared_config = aws_config::from_env().load().await;
    let client = Client::new(&shared_config);
    let shared_client = &client;
    lambda_runtime::run(service_fn(move |event: LambdaEvent<Request>| async move {
        handler(&shared_client, event).await
    }))
    .await
}
```

Lambda-Kontext-Objekt in Rust

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Wenn Lambda Ihre Funktion ausführt, fügt es der , die der Handler empfängt LambdaEvent , ein Kontextobjekt hinzu. Dieses Objekt stellt Eigenschaften mit Informationen zum Aufruf, zur Funktion und zur Ausführungsumgebung bereit.

Context-Eigenschaften

- `request_id`: Die vom Lambda-Service generierte AWS-Anforderungs-ID.
- `deadline`: Die Ausführungsfrist für den aktuellen Aufruf in Millisekunden.
- `invoked_function_arn`: Der Amazon-Ressourcenname (ARN) der aufgerufenen Lambda-Funktion.
- `xray_trace_id`: Die AWS X-Ray-Trace-ID des aktuellen Aufrufs.
- `client_content`: Das vom mobilen AWS SDK gesendete Client-Kontext-Objekt. Dieses Feld ist leer, sofern die Funktion nicht mit einem mobilen AWS SDK aufgerufen wird.
- `identity`: Die Amazon-Cognito-Identität, die die Funktion aufgerufen hat. Dieses Feld ist leer, es sei denn, die Aufrufanforderung an die Lambda-APIs erfolgte unter Verwendung von AWS-Anmeldeinformationen, die von Amazon-Cognito-Identitätspools ausgestellt wurden.
- `env_config`: Die Lambda-Funktionskonfiguration aus den lokalen Umgebungsvariablen. Diese Eigenschaft umfasst Informationen wie den Funktionsnamen, die Speicherzuweisung, die Version und die Protokollstreams.

Zugreifen auf Aufrufkontextinformationen

Lambda-Funktionen haben Zugriff auf Metadaten über ihre Umgebung und die Aufrufanforderung. Das `LambaEvent` Objekt, das Ihr Funktionshandler empfängt, enthält die `context`-Metadaten:

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};
```

```
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    let invoked_function_arn = event.context.invoked_function_arn;
    Ok(json!({ "message": format!("Hello, this is function
 {invoked_function_arn}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Verarbeitung von HTTP-Ereignissen mit Rust

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Amazon API Gateway APIs, Application Load Balancer und Lambda-Funktions-URLs können HTTP-Ereignisse an Lambda senden. Sie können den aws_lambda_events Crate von crates.io verwenden, um Ereignisse aus diesen Quellen zu verarbeiten.

Example – API Gateway Proxy-Anfrage bearbeiten

Beachten Sie Folgendes:

- `use aws_lambda_events::apigw::{ApiGatewayProxyRequest, ApiGatewayProxyResponse}`: Der aws_lambda_events Crate enthält viele Lambda-Ereignisse. Um die Kompilierungszeit zu verkürzen, verwenden Sie Feature-Flags, um die benötigten Ereignisse zu aktivieren. Beispiel: `aws_lambda_events = { version = "0.8.3", default-features = false, features = ["apigw"] }`.
- `use http::HeaderMap`: Für diesen Import müssen Sie den HTTP Crate zu Ihren Abhängigkeiten hinzufügen.

```
use aws_lambda_events::apigw::{ApiGatewayProxyRequest, ApiGatewayProxyResponse};
use http::HeaderMap;
use lambda_runtime::{service_fn, Error, LambdaEvent};

async fn handler(
    _event: LambdaEvent<ApiGatewayProxyRequest>,
) -> Result<ApiGatewayProxyResponse, Error> {
    let mut headers = HeaderMap::new();
    headers.insert("content-type", "text/html".parse().unwrap());
    let resp = ApiGatewayProxyResponse {
        status_code: 200,
        multi_value_headers: headers.clone(),
        is_base64_encoded: false,
        body: Some("Hello AWS Lambda HTTP request".into()),
        headers,
```

```
    };
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Der Rust-Laufzeit-Client für Lambda bietet auch eine Abstraktion dieser Ereignistypen, die es Ihnen ermöglicht, mit nativen HTTP-Typen zu arbeiten, unabhängig davon, welcher Service die Ereignisse sendet. Der folgende Code entspricht dem vorherigen Beispiel und funktioniert sofort mit Lambda-Funktions-URLs, Application Load Balancer und API Gateway.

> **Note**
>
> Der lambda_http Crate verwendet den darunter liegenden lambda_runtime Crate. Sie müssen `lambda_runtime` nicht separat importieren.

Example – Bearbeitung von HTTP-Anforderungen

```
use lambda_http::{service_fn, Error, IntoResponse, Request, RequestExt, Response};

async fn handler(event: Request) -> Result<impl IntoResponse, Error> {
    let resp = Response::builder()
        .status(200)
        .header("content-type", "text/html")
        .body("Hello AWS Lambda HTTP request")
        .map_err(Box::new)?;
    Ok(resp)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_http::run(service_fn(handler)).await
}
```

Ein weiteres Beispiel für die Verwendung `lambda_http` finden Sie im Codebeispiel http-axum im AWS Labs-Repository. GitHub

Beispiel für HTTP-Lambda-Ereignisse für Rust

- Lambda-HTTP-Ereignisse: Eine Rust-Funktion, die HTTP-Ereignisse verarbeitet.
- Lambda-HTTP-Ereignisse mit CORS-Headern: Eine Rust-Funktion, die Tower verwendet, um CORS-Header zu injizieren.
- Lambda-HTTP-Ereignisse mit gemeinsam genutzten Ressourcen: Eine Rust-Funktion, die gemeinsam genutzte Ressourcen verwendet, die initialisiert werden, bevor der Funktionshandler erstellt wird.

Bereitstellen von Lambda-Rust-Funktionen mit ZIP-Dateiarchiven

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

Auf dieser Seite wird beschrieben, wie Sie Ihre Rust-Funktion kompilieren und dann die kompilierte Binärdatei mithilfe von Cargo Lambda auf AWS Lambda bereitstellen. Es zeigt auch, wie die kompilierte Binärdatei mit der AWS Command Line Interface und der AWS Serverless Application Model-CLI bereitgestellt wird.

Sections

Voraussetzungen

- Rust
- AWS Command Line Interface (AWS CLI) Version 2

Aufbau von Rust-Funktionen auf macOS, Windows oder Linux

Die folgenden Schritte veranschaulichen, wie Sie das Projekt für Ihre erste Lambda-Funktion mit Rust erstellen und es mit Cargo Lambda kompilieren.

1. Installieren Sie Cargo Lambda, einen Cargo-Unterbefehl, der Rust-Funktionen für Lambda auf macOS, Windows und Linux kompiliert.

   Verwenden Sie pip, um Cargo Lambda auf einem System zu installieren, auf dem Python 3 installiert ist:

   ```
   pip3 install cargo-lambda
   ```

Verwenden Sie Homebrew, um Cargo Lambda auf macOS oder Linux zu installieren:

```
brew tap cargo-lambda/cargo-lambda
brew install cargo-lambda
```

Verwenden Sie Scoop, um Cargo Lambda auf Windows zu installieren:

```
scoop bucket add cargo-lambda
scoop install cargo-lambda/cargo-lambda
```

Weitere Optionen finden Sie unter Installation in der Cargo-Lambda-Dokumentation.

2. Erstellen Sie die Paketstruktur. Dieser Befehl erstellt einen grundlegenden Funktionscode in `src/main.rs`. Sie können diesen Code zum Testen verwenden oder ihn durch Ihren eigenen ersetzen.

```
cargo lambda new my-function
```

3. Führen Sie im Stammverzeichnis des Pakets den Unterbefehl build aus, um den Code in Ihrer Funktion zu kompilieren.

```
cargo lambda build --release
```

(Optional) Wenn Sie AWS Graviton2 auf Lambda verwenden möchten, fügen Sie `--arm64`-Flag hinzu, um Ihren Code für ARM-CPUs zu kompilieren.

```
cargo lambda build --release --arm64
```

4. Bevor Sie Ihre Rust-Funktion bereitstellen, konfigurieren Sie die AWS-Anmeldeinformationen auf Ihrem Rechner.

```
aws configure
```

Bereitstellung der Binärdatei der Rust-Funktion mit Cargo Lambda

Verwenden Sie den Unterbefehl bereitstellen, um die kompilierte Binärdatei für Lambda bereitzustellen. Dieser Befehl erstellt eine Ausführungsrolle und erstellt dann die Lambda-Funktion. Um eine bestehende Ausführungsrolle anzugeben, verwenden Sie die --iam-role Flag.

```
cargo lambda deploy my-function
```

Bereitstellung der Binärdatei der Rust-Funktion mit der AWS CLI

Sie können Ihre Binärdatei auch mithilfe der AWS CLI bereitstellen.

1. Verwenden Sie den Unterbefehl build, um das .zip-Bereitstellungspaket zu erstellen.

   ```
   cargo lambda build --release --output-format zip
   ```

2. Stellen Sie das .zip-Paket für Lambda bereit. Für `--role` geben Sie den ARN der Ausführungsrolle an.

   ```
   aws lambda create-function --function-name my-function \
        --runtime provided.al2023 \
        --role arn:aws:iam::111122223333:role/lambda-role \
        --handler rust.handler \
        --zip-file fileb://target/lambda/my-function/bootstrap.zip
   ```

Bereitstellung der Binärdatei der Rust-Funktion mit der AWS SAM CLI

Sie können Ihre Binärdatei auch mithilfe der AWS SAM CLI bereitstellen.

1. Erstellen Sie eine AWS SAM-Vorlage mit der Ressourcen- und Eigenschaftsdefinition. Weitere Informationen finden Sie unter AWS::Serverless::Function im AWS Serverless Application Model-Entwicklerhandbuch.

   Example SAM-Ressourcen- und Eigenschaftsdefinition für eine Rust-Binärdatei

   ```
   AWSTemplateFormatVersion: '2010-09-09'
   Transform: AWS::Serverless-2016-10-31
   Description: SAM template for Rust binaries
   Resources:
     RustFunction:
   ```

```
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: target/lambda/my-function/
      Handler: rust.handler
      Runtime: provided.al2023
Outputs:
  RustFunction:
    Description: "Lambda Function ARN"
    Value: !GetAtt RustFunction.Arn
```

2. Verwenden Sie den Unterbefehl build, um die Funktion zu kompilieren.

```
cargo lambda build --release
```

3. Verwenden Sie den Befehl sam deploy, um die Funktion in Lambda bereitzustellen.

```
sam deploy --guided
```

Weitere Informationen zum Erstellen von Rust-Funktionen mit der AWS SAM CLI finden Sie im AWS Serverless Application Model-Entwicklerhandbuch unter Erstellen von Rust Lambda-Funktionen mit Cargo Lambda.

Aufrufen Ihrer Rust-Funktion mit Cargo Lambda

Verwenden Sie den Unterbefehl invoke, um Ihre Funktion mit einer Nutzlast zu testen.

```
cargo lambda invoke --remote --data-ascii '{"command": "Hello world"}' my-function
```

Aufrufen Ihrer Rust-Funktion mit der AWS CLI

Sie können auch die AWS CLI verwenden, um die Funktion aufzurufen.

```
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"command": "Hello world"}' /tmp/out.txt
```

Die cli-binary-format-Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface-Benutzerhandbuch für Version 2.

Lambda-Funktionsprotokollierung in Rust

> **Note**
>
> Der Rust-Laufzeit-Client ist ein experimentelles Paket. Er kann sich ändern und ist nur zu Evaluierungszwecken gedacht.

AWS Lambda überwacht automatisch Lambda-Funktionen in Ihrem Namen und sendet Protokolle an Amazon CloudWatch. Ihre Lambda-Funktion verfügt über eine CloudWatch Protokollgruppe und einen Protokollstream für jede Instance Ihrer Funktion. Die Lambda-Laufzeitumgebung sendet Details zu den einzelnen Aufrufen an den Protokollstream und leitet Protokolle und andere Ausgaben aus dem Code Ihrer Funktion weiter. Weitere Informationen finden Sie unter Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda. Auf dieser Seite wird beschrieben, wie Sie Protokollausgaben aus dem Code Ihrer Lambda-Funktion erstellen.

Erstellen einer Funktion, die Protokolle schreibt

Um Protokolle aus Ihrem Funktionscode auszugeben, können Sie jede Protokollierungsfunktion verwenden, die in `stdout` oder `stderr` schreibt, wie z. B. das `println!`-Makro. Das folgende Beispiel verwendet `println!`, um eine Nachricht zu drucken, wenn der Funktionshandler gestartet wird und bevor er beendet wird.

```
use lambda_runtime::{service_fn, LambdaEvent, Error};
use serde_json::{json, Value};
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    println!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    println!("Rust function responds to {}", &first_name);
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    lambda_runtime::run(service_fn(handler)).await
}
```

Fortgeschrittenes Protokollieren mit Tracing Crate

Tracing ist ein Framework zur Instrumentierung von Rust-Programmen zur Erfassung strukturierter, ereignisbasierter Diagnoseinformationen. Dieses Framework bietet Hilfsprogramme zum Anpassen der Logging-Ausgabestufen und -formate, wie zum Beispiel das Erstellen strukturierter JSON-Protokollnachrichten. Um dieses Framework verwenden zu können, müssen Sie einen `subscriber` initialisieren, bevor Sie den Funktionshandler implementieren. Anschließend können Sie Tracing-Makros wie `debug`, `info` und `error` verwenden, um die gewünschte Protokollierungsebene für jedes Szenario anzugeben.

Example – Verwenden von Tracing Crate

Beachten Sie Folgendes:

- `tracing_subscriber::fmt().json()`: Wenn diese Option enthalten ist, werden die Protokolle in JSON formatiert. Um diese Option verwenden zu können, müssen Sie die `json`-Funktion in die `tracing-subscriber`-Abhängigkeit aufnehmen (z. B. `tracing-subscriber = { version = "0.3.11", features = ["json"] }`).
- `#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]`: Diese Annotation generiert bei jedem Aufruf des Handlers eine Spanne. Diese Spanne fügt jeder Protokollzeile die Anforderungs-ID hinzu.
- `{ %first_name }`: Dieses Konstrukt fügt das `first_name`-Feld der Protokollzeile hinzu, in der es verwendet wird. Der Wert für dieses Feld entspricht der Variablen mit dem gleichen Namen.

```
use lambda_runtime::{service_fn, Error, LambdaEvent};
use serde_json::{json, Value};
#[tracing::instrument(skip(event), fields(req_id = %event.context.request_id))]
async fn handler(event: LambdaEvent<Value>) -> Result<Value, Error> {
    tracing::info!("Rust function invoked");
    let payload = event.payload;
    let first_name = payload["firstName"].as_str().unwrap_or("world");
    tracing::info!({ %first_name }, "Rust function responds to event");
    Ok(json!({ "message": format!("Hello, {first_name}!") }))
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt().json()
        .with_max_level(tracing::Level::INFO)
```

```
        // this needs to be set to remove duplicated information in the log.
        .with_current_span(false)
        // this needs to be set to false, otherwise ANSI color codes will
        // show up in a confusing manner in CloudWatch logs.
        .with_ansi(false)
        // disabling time is handy because CloudWatch will add the ingestion time.
        .without_time()
        // remove the name of the function from every log entry
        .with_target(false)
        .init();
    lambda_runtime::run(service_fn(handler)).await
}
```

Wenn diese Rust-Funktion aufgerufen wird, druckt sie zwei Protokollzeilen, die den folgenden ähneln:

```
{"level":"INFO","fields":{"message":"Rust function invoked"},"spans":
[{"req_id":"45daaaa7-1a72-470c-9a62-e79860044bb5","name":"handler"}]}
{"level":"INFO","fields":{"message":"Rust function responds to
 event","first_name":"David"},"spans":[{"req_id":"45daaaa7-1a72-470c-9a62-
e79860044bb5","name":"handler"}]}
```

Lambda mit Ereignissen aus anderen Diensten aufrufen AWS

Einige AWS Dienste können Lambda-Funktionen mithilfe von Triggern direkt aufrufen. Diese Dienste leiten Ereignisse an Lambda weiter, und die Funktion wird sofort aufgerufen, wenn das angegebene Ereignis eintritt. Trigger eignen sich für diskrete Ereignisse und die Verarbeitung in Echtzeit. Wenn Sie mit der Lambda-Konsole einen Trigger erstellen, interagiert die Konsole mit dem entsprechenden AWS Dienst, um die Ereignisbenachrichtigung für diesen Dienst zu konfigurieren. Der Trigger wird tatsächlich von dem Dienst gespeichert und verwaltet, der die Ereignisse generiert, nicht von Lambda.

Die Ereignisse sind im JSON-Format gegliedert. Die JSON-Struktur variiert je nach Service, der sie generiert und dem Ereignistyp, aber sie alle enthalten die Daten, die die Funktion benötigt, um das Ereignis zu verarbeiten.

Eine Funktion kann mehrere Auslöser haben. Jeder Auslöser fungiert als Client, der Ihre Funktion unabhängig aufruft, und jedes Ereignis, das Lambda an Ihre Funktion weitergibt, enthält Daten von nur einem Auslöser. Lambda wandelt das Ereignisdokument in ein Objekt um und leitet es an Ihren Funktions-Handler weiter.

Je nach Dienst kann der ereignisgesteuerte Aufruf synchron oder asynchron sein.

- Beim synchronen Aufruf wartet der Service, der das Ereignis generiert, auf die Antwort Ihrer Funktion. Dieser Service definiert die Daten, die die Funktion in der Antwort zurückgeben muss. Der Service steuert die Fehlerstrategie, z. B. ob bei Fehlern ein erneuter Versuch unternommen werden soll.
- Bei asynchronen Aufrufen verschiebt Lambda das Ereignis in die Warteschlange, bevor sie es an Ihre Funktion übergibt. Wenn Lambda das Ereignis in die Warteschlange stellt, sendet es sofort eine Erfolgsantwort an den Service der das Ereignis generiert hat. Nachdem die Funktion das Ereignis verarbeitet hat, gibt Lambda keine Antwort auf den ereignisgenerierenden Service zurück.

Einen Trigger erstellen

Der einfachste Weg, einen Trigger zu erstellen, ist die Verwendung der Lambda-Konsole. Wenn Sie mit der Konsole einen Trigger erstellen, fügt Lambda der ressourcenbasierten Richtlinie der Funktion automatisch die erforderlichen Berechtigungen hinzu.

So erstellen Sie einen Trigger mit der Lambda-Konsole

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, für die Sie einen Trigger erstellen möchten.
3. Wählen Sie im Bereich Function overview (Funktionsübersicht) die Option Add trigger (Auslöser hinzufügen).
4. Wählen Sie den AWS Dienst aus, den Sie Ihre Funktion aufrufen möchten.
5. Füllen Sie die Optionen im Bereich Trigger-Konfiguration aus und wählen Sie Hinzufügen. Je nachdem, welche Funktion AWS-Service Sie aufrufen möchten, unterscheiden sich die Konfigurationsoptionen für den Trigger.

Dienste, die Lambda-Funktionen aufrufen können

In der folgenden Tabelle sind Dienste aufgeführt, die Lambda-Funktionen aufrufen können.

Service	Methode des Aufrufs
Amazon Alexa	Ereignisgesteuert; synchroner Aufruf
Amazon Managed Streaming für Apache Kafka	Zuordnung der Ereignisquelle
Selbstverwaltetes Apache Kafka	Zuordnung der Ereignisquelle
Amazon API Gateway	Ereignisgesteuert; synchroner Aufruf
AWS CloudFormation	Ereignisgesteuert; asynchroner Aufruf
Amazon CloudFront (Lambda @Edge)	Ereignisgesteuert; synchroner Aufruf
CloudWatch Amazon-Protokolle	Ereignisgesteuert; asynchroner Aufruf
AWS CodeCommit	Ereignisgesteuert; asynchroner Aufruf
AWS CodePipeline	Ereignisgesteuert; asynchroner Aufruf

Service	Methode des Aufrufs
Amazon Cognito	Ereignisgesteuert; synchroner Aufruf
AWS Config	Ereignisgesteuert; asynchroner Aufruf
Amazon Connect	Ereignisgesteuert; synchroner Aufruf
Amazon-DynamoDB	Zuordnung der Ereignisquelle
Amazon Elastic File System	Spezielle Integration
Elastic Load Balancing (Application Load Balancer)	Ereignisgesteuert; synchroner Aufruf
AWS IoT	Ereignisgesteuert; asynchroner Aufruf
Amazon Kinesis	Zuordnung der Ereignisquelle
Amazon Data Firehose	Ereignisgesteuert; synchroner Aufruf
Amazon Lex	Ereignisgesteuert; synchroner Aufruf
Amazon MQ	Zuordnung der Ereignisquelle
Amazon Simple Email Service	Ereignisgesteuert; asynchroner Aufruf
Amazon Simple Notification Service	Ereignisgesteuert; asynchroner Aufruf
Amazon Simple Queue Service	Zuordnung der Ereignisquelle
Amazon-Simple-Storage-Service (Amazon-S3)	Ereignisgesteuert; asynchroner Aufruf
Amazon Simple Storage Service Batch	Ereignisgesteuert; synchroner Aufruf
Secrets Manager	Ereignisgesteuert; synchroner Aufruf

Service	Methode des Aufrufs
Amazon VPC Lattice	Ereignisgesteuert; synchroner Aufruf
AWS X-Ray	Spezielle Integration

Geläufige Lambda-Anwendungstypen und -Anwendungsfälle

Lambda-Funktionen und Trigger sind die Kernkomponenten beim Erstellen von Anwendungen auf AWS Lambda. Eine Lambda-Funktion ist der Code und die Laufzeit, die Ereignisse verarbeiten, während ein Auslöser der AWS-Service oder die Anwendung ist, die die Funktion aufruft. Berücksichtigen Sie zur Veranschaulichung die folgenden Szenarien:

- Dateiverarbeitung – Angenommen, Sie haben eine Bildaustausch-Anwendung. Ihre Anwendung wird zum Hochladen von Fotos verwendet und die Anwendung speichert die Benutzerfotos in einem Amazon-S3-Bucket. Ihre Anwendung erstellt dann eine Thumbnail-Version der Fotos der einzelnen Benutzer und zeigt diese auf der Profilseite des Benutzers an. In diesem Szenario können Sie eine Lambda -Funktion erstellen, die automatisch ein Thumbnail erstellt. Amazon S3 ist eine der unterstützten AWS-Ereignisquellen, die objekterstellte Ereignisse veröffentlichen und Ihre Lambda-Funktion aufrufen können. Der Lambda-Funktionscode kann das Fotoobjekt aus dem S3-Bucket lesen, eine Thumbnail-Version erstellen und diese dann in einem anderen S3-Bucket erstellen.
- Daten und Analyse – Angenommen, Sie erstellen eine Analyseanwendung und speichern unformatierte Daten in einer DynamoDB-Tabelle. Wenn Sie Elemente in eine Tabelle schreiben, aktualisieren oder löschen, können DynamoDB-Streams Update-Ereignisse für Elemente in einem Stream veröffentlichen, der mit der Tabelle verknüpft ist. In diesem Fall stellen die Ereignisdaten den Elementschlüssel, den Ereignisnamen (z. B. Einfügen, Aktualisieren und Löschen) sowie andere relevante Details bereit. Sie können eine Lambda-Funktion so schreiben, dass benutzerdefinierte Metriken durch Aggregieren von unformatierten Daten generiert werden.
- Websites – Angenommen, Sie erstellen eine Website und möchten die Backend-Logik in Lambda hosten. Sie können Ihre Lambda-Funktion über HTTP mithilfe von Amazon API Gateway als HTTP-Endpunkt aufrufen. Ihr Webclient kann nun die API aufrufen und API Gateway kann dann die Anforderung an Lambda weiterleiten.
- Mobile Anwendungen – Angenommen, Sie haben eine mobile Anwendung, die Ereignisse produziert. Sie können eine Lambda-Funktion erstellen, um Ereignisse zu verarbeiten, die von der benutzerdefinierten Anwendung veröffentlicht werden. Sie können beispielsweise eine Lambda-Funktion so verarbeiten, dass die Klicks innerhalb der benutzerdefinierten mobilen Anwendung verarbeitet werden.

AWS Lambda unterstützt viele AWS-Services als Ereignisquellen. Weitere Informationen finden Sie unter Lambda mit Ereignissen aus anderen Diensten aufrufen AWS. Wenn Sie diese Ereignisquelle so konfigurieren, dass eine Lambda-Funktion ausgelöst wird, wird die Lambda-Funktion automatisch

aufgerufen, wenn Ereignisse auftreten. Sie definieren die Ereignisquellen-Zuweisung, sodass Sie identifizieren können, welche Ereignisse verfolgt werden sollen und welche Lambda-Funktion aufgerufen werden soll.

Im Folgenden finden Sie einführende Beispiele für Ereignisquellen und wie die end-to-end Erfahrung funktioniert.

Beispiel 1: Amazon S3 pusht Ereignisse und ruft eine Lambda-Funktion auf

Amazon S3 kann Ereignisse unterschiedlicher Typen veröffentlichen, z. B. PUT-, POST-, COPY- und DELETE-Objektereignisse in einem Bucket. Mithilfe der Bucket-Benachrichtigungsfunktion können Sie eine Ereignisquellen-Zuweisung konfigurieren, die Amazon S3 anweist, eine Lambda-Funktion aufzurufen, wenn ein bestimmter Typ von Ereignis auftritt.

Im Folgenden sehen Sie eine typische Sequenz:

1. Der Benutzer erstellt ein Objekt in einem Bucket.
2. Amazon S3 erkennt das vom Ereignis erstellte Objekt.
3. Amazon S3 ruft die Lambda-Funktion mithilfe der von der Ausführungsrolle bereitgestellten Berechtigungen auf.
4. AWS Lambda führt die Lambda-Funktion aus und gibt dabei das Ereignis als Parameter an.

Sie konfigurieren Amazon S3, um Ihre Funktion als Bucket-Benachrichtigungsaktion aufzurufen. Sie erteilen Amazon S3 die Berechtigung zum Aufrufen der Funktion, indem Sie die ressourcenbasierten Richtlinien der Funktion aktualisieren.

Beispiel 2: AWS Lambda ruft Ereignisse aus einem Kinesis-Stream ab und ruft eine Lambda-Funktion auf

Für abfragebasierte Ereignisquellen fragt AWS Lambda die Quelle ab und ruft anschließend die Lambda-Funktion auf, wenn Datensätze in der Quelle erkannt werden.

- CreateEventSourceMapping
- UpdateEventSourceMapping

Die folgenden Schritte beschreiben, wie eine benutzerdefinierte Anwendung Datensätze in einen Kinesis-Stream schreibt:

1. Die benutzerdefinierte Anwendung schreibt die Datensätze in einen Kinesis-Stream.
2. AWS Lambda fragt den Stream kontinuierlich ab und ruft die Lambda-Funktion auf, wenn der Service neue Datensätze im Stream erkennt. AWS Lambda weiß anhand der Ereignisquellen-Zuweisung, die Sie in Lambda erstellen, welcher Stream abgefragt und welche Lambda-Funktion aufgerufen werden muss.
3. Die Lambda-Funktion wird mit dem eingehenden Ereignis aufgerufen.

Wenn Sie mit streambasierten Ereignisquellen arbeiten, erstellen Sie Ereignisquellen-Zuweisungen in AWS Lambda. Lambda liest Elemente aus dem Stream und ruft die Funktion synchron auf. Sie müssen Lambda keine Berechtigung zum Aufrufen der Funktion erteilen, sie benötigt jedoch eine Leseberechtigung für den Stream.

Verwenden von AWS Lambda mit Alexa

Sie können Lambda-Funktionen verwenden, um Services zu erstellen, die Alex, der Sprachassistentin von Amazon Echo, neue Qualifikationen verleihen. Das Alexa Skills Kit bietet die APIs, Tools und Dokumentation, um diese neuen Qualifikationen mit der Unterstützung Ihres eigenen als Lambda-Funktionen ausgeführten Services zu erstellen. Benutzer von Amazon Echo können auf diese neuen Qualifikationen zugreifen, indem sie Alexa Fragen stellen oder Anforderungen durchführen.

Das Alexa Skills Kit ist auf verfügbar GitHub.

- Alexa Skills Kit SDK für Java
- Alexa Skills Kit SDK für Node.js
- Alexa-Skills-Kit-SDK für Python

Example Alexa Smart Home-Ereignis

```
{
  "header": {
    "payloadVersion": "1",
    "namespace": "Control",
    "name": "SwitchOnOffRequest"
  },
  "payload": {
    "switchControlAction": "TURN_ON",
    "appliance": {
      "additionalApplianceDetails": {
        "key2": "value2",
        "key1": "value1"
      },
      "applianceId": "sampleId"
    },
    "accessToken": "sampleAccessToken"
  }
}
```

Weitere Informationen finden Sie unter Bereitstellen eines benutzerdefinierten Skills als AWS Lambda Lambda-Funktion im Handbuch Entwickeln von Skills mittels der Alexa Skills Kit.

Aufrufen einer Lambda-Funktion mithilfe eines Amazon API Gateway Gateway-Endpunkts

Sie können eine Web-API mit einem HTTP-Endpunkt für Ihre Lambda Funktion erstellen, indem Sie Amazon API Gateway verwenden. API Gateway bietet Tools zum Erstellen und Dokumentieren von Web-APIs, die HTTP-Anforderungen an Lambda-Funktionen weiterleiten. Sie können den Zugriff auf Ihre API mit Authentifizierungs- und Autorisierungskontrollen sichern. Ihre APIs können Datenverkehr über das Internet bereitstellen oder nur innerhalb Ihrer VPC zugänglich sein.

Ressourcen in Ihrer API definieren mindestens eine Methode, z. B. GET oder POST. Methoden haben eine Integration, die Anfragen an eine Lambda-Funktion oder einen anderen Integrationstyp weiterleitet. Sie können jede Ressource und jede Methode einzeln definieren oder spezielle Ressourcen- und Methodenarten verwenden, um alle Anforderungen abzugleichen, die einem Muster entsprechen. Eine Proxy-Ressource fängt alle Pfade unter einer Ressource ab. Die `ANY`-Methode fängt alle HTTP-Methoden ab.

Sections

Auswählen eines API-Typs

API Gateway unterstützt drei Arten von APIs, die Lambda-Funktionen aufrufen:

- HTTP-API: Eine schlanke RESTful-API mit niedriger Latenz.
- REST-API: Eine anpassbare, funktionsreiche RESTful-API.
- WebSocket API: Eine Web-API, die persistente Verbindungen zu Clients für die Vollduplex-Kommunikation unterhält.

HTTP-APIs und REST-APIs sind beides RESTful-APIs, die HTTP-Anforderungen verarbeiten und Antworten zurückgeben. HTTP-APIs sind neuer und werden mit der API der API-Gateway-Version 2 erstellt. Die folgenden Funktionen sind neu bei HTTP-APIs:

HTTP-API-Funktionen

- Automatische Bereitstellungen – wenn Sie Routen oder Integrationen ändern, werden Änderungen automatisch in Phasen bereitgestellt, bei denen die automatische Bereitstellung aktiviert ist.
- Standardphase – Sie können eine Standardphase (`$default`) erstellen, um Anforderungen am Stammpfad der URL Ihrer API zu bedienen. Bei benannten Phasen müssen Sie den Schrittnamen am Anfang des Pfades angeben.
- CORS-Konfiguration – Sie können Ihre API so konfigurieren, dass ausgehenden Antworten CORS-Header hinzugefügt werden, anstatt sie manuell in Ihrem Funktionscode hinzufügen zu müssen.

REST-APIs sind die klassischen RESTful-APIs, die von API Gateway seit dem Start unterstützt wurden. REST-APIs verfügen derzeit über mehr Anpassungs-, Integrations- und Verwaltungsfunktionen.

REST-API-Funktionen

- Integrationstypen – REST-APIs unterstützen benutzerdefinierte Lambda-Integrationen. Mit einer benutzerdefinierten Integration können Sie nur den Text der Anforderung an die Funktion senden oder eine Transformationsvorlage auf den Anforderungstext anwenden, bevor Sie sie an die Funktion senden.
- Zugriffskontrolle – REST-APIs unterstützen weitere Optionen für die Authentifizierung und Autorisierung.
- Überwachung und Ablaufverfolgung — REST-APIs unterstützen AWS X-Ray Tracing und zusätzliche Protokollierungsoptionen.

Einen detaillierten Vergleich finden Sie unter Auswählen zwischen HTTP-APIs und REST-APIs im API-Gateway-Entwicklerhandbuch.

WebSocket APIs verwenden auch die API Gateway Version 2 API und unterstützen einen ähnlichen Funktionsumfang. Verwenden Sie eine WebSocket API für Anwendungen, die von einer dauerhaften Verbindung zwischen dem Client und der API profitieren. WebSocket APIs bieten Vollduplex-Kommunikation, was bedeutet, dass sowohl der Client als auch die API kontinuierlich Nachrichten senden können, ohne auf eine Antwort warten zu müssen.

HTTP-APIs unterstützen ein vereinfachtes Ereignisformat (Version 2.0). Das folgende Beispiel zeigt ein Ereignis aus einer HTTP-API.

Example event-v2.json API-Gateway-Proxy-Ereignis (HTTP-API)

```
{
    "version": "2.0",
    "routeKey": "ANY /nodejs-apig-function-1G3XMPLZXVXYI",
    "rawPath": "/default/nodejs-apig-function-1G3XMPLZXVXYI",
    "rawQueryString": "",
    "cookies": [
        "s_fid=7AABXMPL1AFD9BBF-0643XMPL09956DE2",
        "regStatus=pre-register"
    ],
    "headers": {
        "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
        "accept-encoding": "gzip, deflate, br",
        ...
    },
    "requestContext": {
        "accountId": "123456789012",
        "apiId": "r3pmxmplak",
        "domainName": "r3pmxmplak.execute-api.us-east-2.amazonaws.com",
        "domainPrefix": "r3pmxmplak",
        "http": {
            "method": "GET",
            "path": "/default/nodejs-apig-function-1G3XMPLZXVXYI",
            "protocol": "HTTP/1.1",
            "sourceIp": "205.255.255.176",
            "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
        },
        "requestId": "JKJaXmPLvHcESHA=",
        "routeKey": "ANY /nodejs-apig-function-1G3XMPLZXVXYI",
        "stage": "default",
        "time": "10/Mar/2020:05:16:23 +0000",
        "timeEpoch": 1583817383220
    },
    "isBase64Encoded": true
}
```

Weitere Informationen finden Sie unter AWS Lambda -Integrationen im API Gateway-Entwicklerhandbuch.

Hinzufügen eines Endpunkts zur Lambda-Funktion

So fügen Sie Ihrer Lambda-Funktion einen öffentlichen Endpunkt hinzu

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie unter Function overview (Funktionsübersicht) die Option Add trigger (Trigger hinzufügen).
4. Wählen Sie API Gateway aus.
5. Wählen Sie Create an API (API erstellen) oder Use an existing API (Vorhandene API verwenden).
   a. Neue API: Wählen Sie als API type (API-Typ) HTTP API aus. Weitere Informationen finden Sie unter API-Typen.
   b. Vorhandene API: Wählen Sie die API aus dem Dropdown-Menü aus oder geben Sie die API-ID ein (z. B. r3pmxmplak).
6. Wählen Sie unter Security (Sicherheit) die Option Open (Öffnen) aus.
7. Wählen Sie Add aus.

Proxy-Integration

API-Gateway-APIs bestehen aus Phasen, Ressourcen, Methoden und Integrationen. Die Phase und die Ressource bestimmen den Pfad des Endpunkts:

API-Pfadformat

- `/prod/` – Die `prod`-Phase und die Root-Ressource.
- `/prod/user` – Die `prod`-Phase und die `user`-Ressource.
- `/dev/{proxy+}` – Jede Route in der `dev`-Phase.
- `/` – (HTTP-APIs) Die Standardphase und die Root-Ressource.

Eine Lambda-Integration ordnet einer Lambda-Funktion eine Pfad- und HTTP-Methodenkombination zu. Sie können API Gateway so konfigurieren, dass der Hauptteil der HTTP-Anforderung unverändert

(benutzerdefinierte Integration) übergeben oder der Anforderungstext in einem Dokument mit allen Anforderungsinformationen, einschließlich Header, Ressource, Pfad und Methode, gekapselt wird.

Weitere Informationen finden Sie unter Lambda-Proxyintegrationen in API Gateway einrichten.

Ereignisformat

Amazon API Gateway ruft Ihre Funktion synchron mit einem Ereignis auf, das eine JSON-Darstellung der HTTP-Anforderung enthält. Bei einer benutzerdefinierten Integration ist das Ereignis der Text der Anforderung. Bei einer Proxy-Integration hat das Ereignis eine definierte Struktur. Das folgende Beispiel zeigt ein Proxy-Ereignis aus einer API-Gateway-REST-API.

Example event.json API-Gateway-Proxy-Ereignis (REST-API)

```
{
      "resource": "/",
      "path": "/",
      "httpMethod": "GET",
      "requestContext": {
          "resourcePath": "/",
          "httpMethod": "GET",
          "path": "/Prod/",
          ...
      },
      "headers": {
          "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9",
          "accept-encoding": "gzip, deflate, br",
          "Host": "70ixmpl4fl.execute-api.us-east-2.amazonaws.com",
          "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36",
          "X-Amzn-Trace-Id": "Root=1-5e66d96f-7491f09xmpl79d18acf3d050",
          ...
      },
      "multiValueHeaders": {
          "accept": [
              "text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
          ],
          "accept-encoding": [
              "gzip, deflate, br"
          ],
          ...
```

```
      },
      "queryStringParameters": null,
      "multiValueQueryStringParameters": null,
      "pathParameters": null,
      "stageVariables": null,
      "body": null,
      "isBase64Encoded": false
  }
```

Reaktionsformat

API Gateway wartet auf eine Antwort von Ihrer Funktion und leitet das Ergebnis an den Aufrufer weiter. Für eine benutzerdefinierte Integration definieren Sie eine Integrationsantwort und eine Methodenantwort, um die Ausgabe von der Funktion in eine HTTP-Antwort zu konvertieren. Für eine Proxy-Integration muss die Funktion mit einer Darstellung der Antwort in einem bestimmten Format antworten.

Das folgende Beispiel zeigt ein Antwortobjekt aus einer Node.js-Funktion. Das Antwortobjekt stellt eine erfolgreiche HTTP-Antwort dar, die ein JSON-Dokument enthält.

Example index.mjs – Antwortobjekt der Proxy-Integration (Node.js)

```
var response = {
      "statusCode": 200,
      "headers": {
        "Content-Type": "application/json"
      },
      "isBase64Encoded": false,
      "multiValueHeaders": {
        "X-Custom-Header": ["My value", "My other value"],
      },
      "body": "{\n  \"TotalCodeSize\": 104330022,\n  \"FunctionCount\": 26\n}"
    }
```

Die Lambda-Laufzeit serialisiert das Antwortobjekt in JSON und sendet es an die API. Die API analysiert die Antwort und verwendet sie zur Erstellung einer HTTP-Antwort verwendet, die sie dann an den Client sendet, der die ursprüngliche Anforderung gestellt hat.

Example HTTP-Antwort

```
< HTTP/1.1 200 OK
  < Content-Type: application/json
```

```
< Content-Length: 55
< Connection: keep-alive
< x-amzn-RequestId: 32998fea-xmpl-4268-8c72-16138d629356
< X-Custom-Header: My value
< X-Custom-Header: My other value
< X-Amzn-Trace-Id: Root=1-5e6aa925-ccecxmplbae116148e52f036
<
{
  "TotalCodeSize": 104330022,
  "FunctionCount": 26
}
```

Berechtigungen

Amazon API Gateway erhält die Berechtigung zum Aufrufen Ihrer Funktion über die ressourcenbasierte Richtlinie der Funktion. Sie können eine Aufrufberechtigung für eine gesamte API erteilen oder einen eingeschränkten Zugriff auf eine Phase, eine Ressource oder eine Methode gewähren.

Wenn Sie Ihrer Funktion mithilfe der Lambda-Konsole, mithilfe der API-Gateway-Konsole oder in einer AWS SAM -Vorlage eine API hinzufügen, wird die ressourcenbasierte Richtlinie der Funktion automatisch aktualisiert. Es folgt eine Beispiel-Funktionsrichtlinie.

Example Funktionsrichtlinie

```
{
  "Version": "2012-10-17",
  "Id": "default",
  "Statement": [
    {
      "Sid": "nodejs-apig-functiongetEndpointPermissionProd-BWDBXMPLXE2F",
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-2:111122223333:function:nodejs-apig-
function-1G3MXMPLXVXYI",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "111122223333"
        },
```

```
        "ArnLike": {
          "aws:SourceArn": "arn:aws:execute-api:us-east-2:111122223333:ktyvxmpls1/*/
GET/"
        }
      }
    }
  ]
}
```

Sie können Funktionsrichtlinienberechtigungen manuell mit den folgenden API-Operationen verwalten:

- AddPermission
- RemovePermission
- GetPolicy

Mit dem `add-permission`-Befehl können Sie einer vorhandenen API Aufrufberechtigung erteilen.

```
aws lambda add-permission --function-name my-function \
--statement-id apigateway-get --action lambda:InvokeFunction \
--principal apigateway.amazonaws.com \
--source-arn "arn:aws:execute-api:us-east-2:123456789012:mnh1xmpli7/default/GET/"
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Statement": "{\"Sid\":\"apigateway-test-2\",\"Effect\":\"Allow\",\"Principal
\":{\"Service\":\"apigateway.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
\",\"Resource\":\"arn:aws:lambda:us-east-2:123456789012:function:my-function
\",\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":\"arn:aws:execute-api:us-
east-2:123456789012:mnh1xmpli7/default/GET\"}}}"
}
```

> **Note**
>
> Wenn sich Ihre Funktion und API unterscheiden AWS-Regionen, muss die Regionskennung im Quell-ARN mit der Region der Funktion übereinstimmen, nicht mit der Region der API. Wenn API Gateway eine Funktion aufruft, verwendet es einen Ressourcen-ARN, der auf dem ARN der API basiert, aber an die Region der Funktion angepasst wurde.

Der Quell-ARN in diesem Beispiel erteilt eine Berechtigung für eine Integration in die GET-Methode der Root-Ressource in der Standardphase einer API mit ID `mnh1xmpli7`. Sie können ein Sternchen im Quell-ARN verwenden, um Berechtigungen für mehrere Phasen, Methoden oder Ressourcen zu erteilen.

Ressourcenmuster

- `mnh1xmpli7/*/GET/*` – GET-Methode bei allen Ressourcen in allen Phasen.
- `mnh1xmpli7/prod/ANY/user` – JEDE Methode bei der `user`-Ressource in der `prod`-Phase.
- `mnh1xmpli7/*/*/*` – Jede Methode bei allen Ressourcen in allen Phasen.

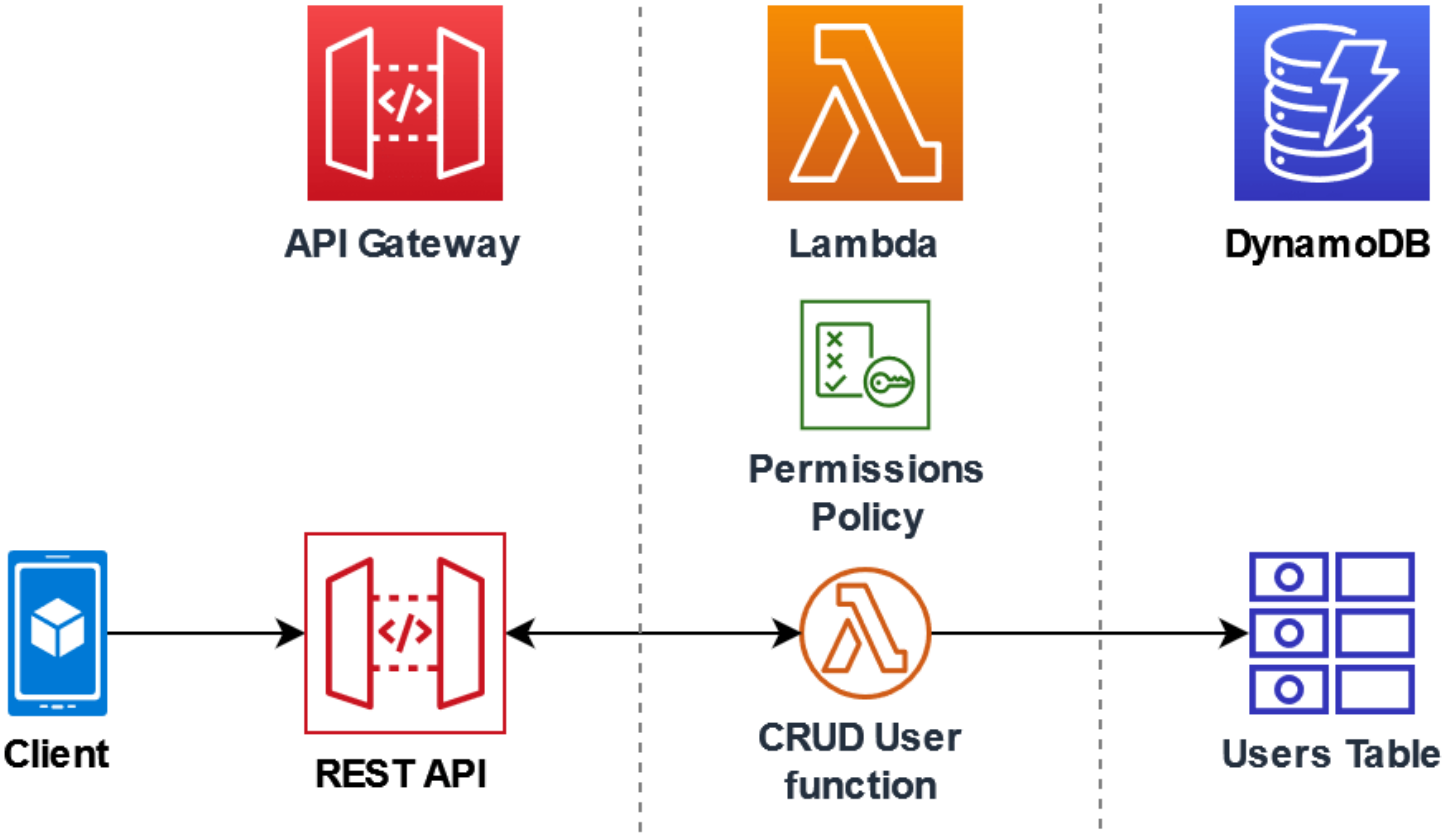
Weitere Informationen zum Anzeigen der Richtlinie und zum Entfernen von Anweisungen finden Sie unter Bereinigen von ressourcenbasierten Richtlinien.

Beispielanwendung

Die Beispiel-App API Gateway with Node.js enthält eine Funktion mit einer AWS SAM Vorlage, die eine REST-API erstellt, für die die AWS X-Ray Ablaufverfolgung aktiviert ist. Sie enthält auch Skripts für die Bereitstellung, den Aufruf der Funktion, das Testen der API und die Bereinigung.

Tutorial: Verwenden von Lambda mit API Gateway

In diesem Tutorial erstellen Sie eine REST-API, über die Sie eine Lambda-Funktion mithilfe einer HTTP-Anfrage aufrufen. Ihre Lambda-Funktion führt CRUD-Operationen (Erstellen, Lesen, Aktualisieren und Löschen) für eine DynamoDB-Tabelle durch. Diese Funktion wird hier zu Demonstrationszwecken bereitgestellt, aber Sie werden lernen, eine API-Gateway-REST-API zu konfigurieren, die jede Lambda-Funktion aufrufen kann.



Die Verwendung von API-Gateway bietet Benutzern einen sicheren HTTP-Endpunkt zum Aufrufen Ihrer Lambda-Funktion und kann dabei helfen, große Mengen an Aufrufen an Ihre Funktion zu verwalten, indem der Datenverkehr gedrosselt und API-Aufrufe automatisch validiert und autorisiert werden. API Gateway bietet auch flexible Sicherheitskontrollen mithilfe von AWS Identity and Access Management (IAM) und Amazon Cognito. Dies ist nützlich für Anwendungsfälle, in denen eine vorherige Autorisierung für Aufrufe zu Ihrer Anwendung erforderlich ist.

Um dieses Tutorial abzuschließen, werden Sie die folgenden Phasen durchlaufen:

1. Erstellen und Konfigurieren einer Lambda-Funktion in Python oder Node.js, um Operationen in einer DynamoDB-Tabelle auszuführen.
2. Erstellen einer REST-API in API Gateway, um eine Verbindung zu Ihrer Lambda-Funktion herzustellen.
3. Erstellen einer DynamoDB-Tabelle und Testen dieser Tabelle mit Ihrer Lambda-Funktion in der Konsole.
4. Bereitstellen Ihrer API und Testen der vollständigen Einrichtung mithilfe von curl in einem Terminal.

Durch Abschluss dieser Phasen lernen Sie, wie Sie mit API Gateway einen HTTP-Endpunkt erstellen, der eine Lambda-Funktion in jeder Größenordnung sicher aufrufen kann. Sie erfahren auch, wie Sie Ihre API bereitstellen und wie Sie sie in der Konsole und durch Senden einer HTTP-Anfrage über ein Terminal testen.

Sections

Voraussetzungen

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

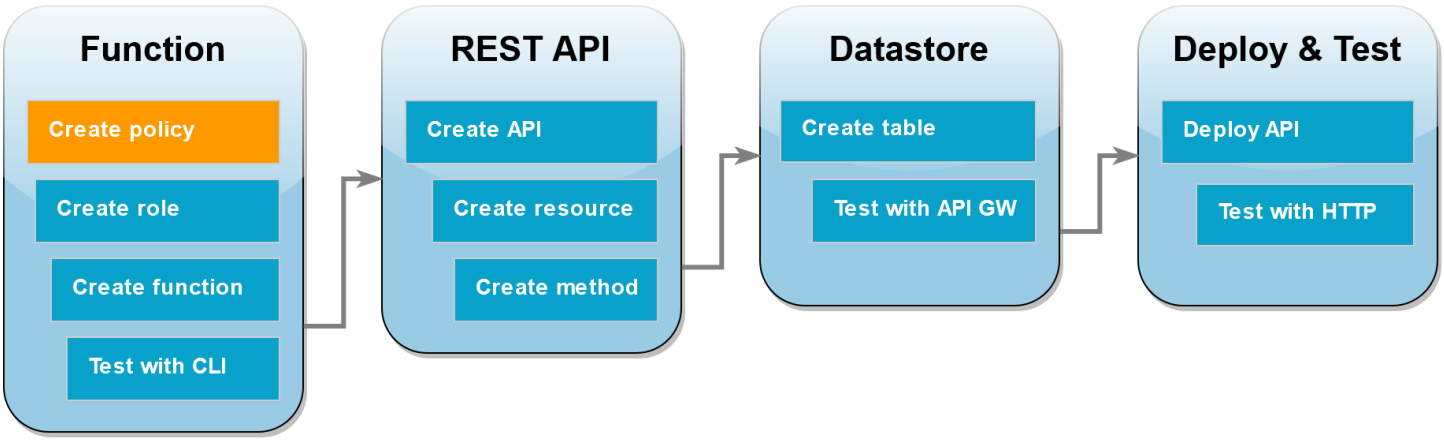
Installieren Sie das AWS Command Line Interface

Wenn Sie das noch nicht installiert haben AWS Command Line Interface, folgen Sie den Schritten unter Installieren oder Aktualisieren der neuesten Version von AWS CLI, um es zu installieren.

Das Tutorial erfordert zum Ausführen von Befehlen ein Befehlszeilenterminal oder eine Shell. Verwenden Sie unter Linux und macOS Ihre bevorzugte Shell und Ihren bevorzugten Paketmanager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux.

Erstellen einer Berechtigungsrichtlinie



Bevor Sie eine Ausführungsrolle für Ihre Lambda-Funktion erstellen können, müssen Sie zunächst eine Berechtigungsrichtlinie erstellen, um Ihrer Funktion die Erlaubnis zu erteilen, auf die erforderlichen AWS Ressourcen zuzugreifen. In diesem Tutorial ermöglicht die Richtlinie Lambda, CRUD-Operationen in einer DynamoDB-Tabelle durchzuführen und in Amazon Logs zu schreiben. CloudWatch

So erstellen Sie die Richtlinie

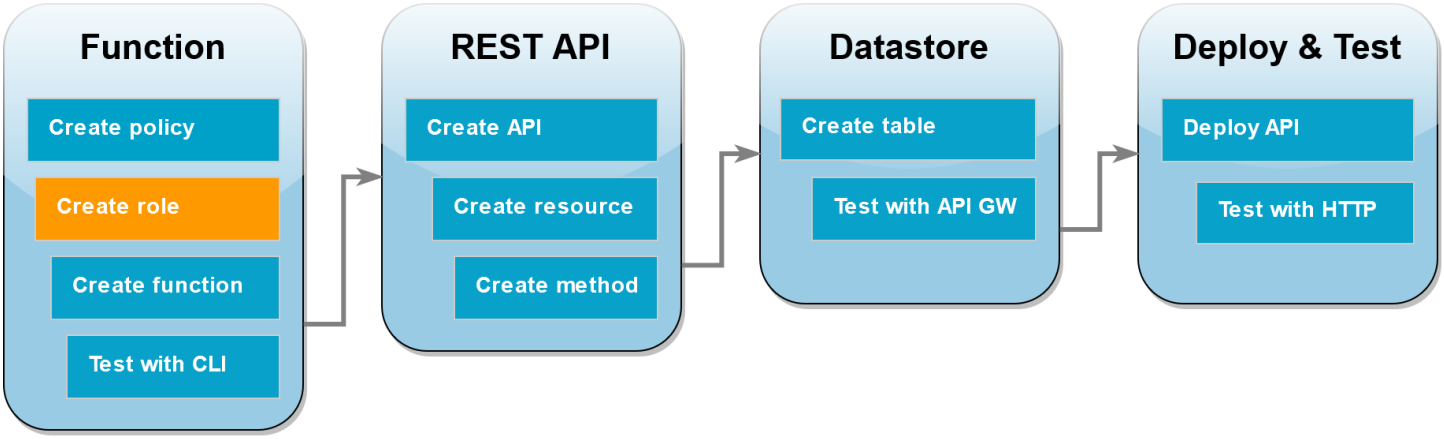
1. Öffnen Sie die Seite Richtlinien in der IAM-Konsole.
2. Wählen Sie Richtlinie erstellen aus.
3. Wählen Sie die Registerkarte JSON aus und kopieren Sie dann die folgende benutzerdefinierte JSON-Richtlinie in den JSON-Editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1428341300017",
      "Action": [
        "dynamodb:DeleteItem",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Query",
        "dynamodb:Scan",
        "dynamodb:UpdateItem"
      ],
      "Effect": "Allow",
      "Resource": "*"
```

```
    },
    {
      "Sid": "",
      "Resource": "*",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow"
    }
  ]
}
```

4. Wählen Sie Next: Tags (Weiter: Tags) aus.
5. Klicken Sie auf Weiter: Prüfen.
6. Geben Sie unter Review policy (Richtlinie prüfen) für den Richtlinien-Namen **`lambda-apigateway-policy`** ein.
7. Wählen Sie Richtlinie erstellen aus.

Erstellen einer Ausführungsrolle



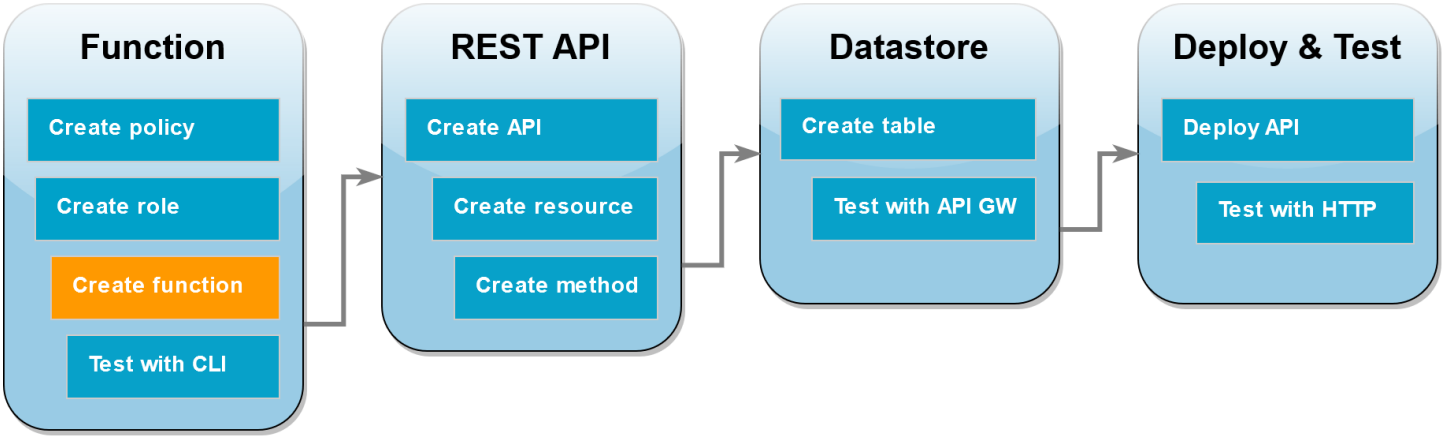
Eine Ausführungsrolle ist eine AWS Identity and Access Management (IAM-) Rolle, die einer Lambda-Funktion die Berechtigung zum Zugriff auf AWS Dienste und Ressourcen gewährt. Damit Ihre Funktion Vorgänge an einer DynamoDB-Tabelle ausführen kann, fügen Sie die Berechtigungsrichtlinie an, die Sie im vorherigen Schritt erstellt haben.

So erstellen Sie eine Ausführungsrolle und fügen Ihre benutzerdefinierte Berechtigungsrichtlinie hinzu

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie als Typ der vertrauenswürdigen Entität AWS -Service und dann als Anwendungsfall Lambda aus.
4. Wählen Sie Weiter aus.
5. Geben Sie im Feld für die Richtliniensuche **`lambda-apigateway-policy`** ein.
6. Wählen Sie in den Suchergebnissen die von Ihnen erstellte Richtlinie (`lambda-apigateway-policy`) und dann die Option Next (Weiter) aus.
7. Geben Sie unter Role details (Rollendetails) für den Role name (Rollennamen) **`lambda-apigateway-role`** ein und wählen Sie dann Create role (Rolle erstellen) aus.

Später im Tutorial benötigen Sie den Amazon-Ressourcennamen (ARN) der Rolle, die Sie gerade erstellt haben. Wählen Sie auf der Seite Roles (Rollen) der IAM-Konsole den Namen Ihrer Rolle (`lambda-apigateway-role`) und kopieren Sie den Role ARN (Rollen-ARN), der auf der Seite Summary (Zusammenfassung) angezeigt wird.

Erstellen der Funktion



Das folgende Codebeispiel empfängt eine Ereigniseingabe von API-Gateway, die eine Operation angibt, die für die zu erstellende DynamoDB-Tabelle und einige Nutzdaten ausgeführt werden soll. Wenn die von der Funktion empfangenen Parameter gültig sind, führt sie die angeforderte Operation für die Tabelle aus.

Node.js

Example index.mjs

```
console.log('Loading function');

import { DynamoDBDocumentClient, PutCommand, GetCommand,
         UpdateCommand, DeleteCommand} from "@aws-sdk/lib-dynamodb";
import { DynamoDBClient } from "@aws-sdk/client-dynamodb";

const ddbClient = new DynamoDBClient({ region: "us-west-2" });
const ddbDocClient = DynamoDBDocumentClient.from(ddbClient);

// Define the name of the DDB table to perform the CRUD operations on
const tablename = "lambda-apigateway";

/**
 * Provide an event that contains the following keys:
 *
 *   - operation: one of 'create,' 'read,' 'update,' 'delete,' or 'echo'
 *   - payload: a JSON object containing the parameters for the table item
 *              to perform the operation on
 */
export const handler = async (event, context) => {

     const operation = event.operation;

     if (operation == 'echo'){
          return(event.payload);
     }

    else {
        event.payload.TableName = tablename;

        switch (operation) {
          case 'create':
               await ddbDocClient.send(new PutCommand(event.payload));
               break;
          case 'read':
               var table_item = await ddbDocClient.send(new
 GetCommand(event.payload));
               console.log(table_item);
               break;
          case 'update':
```

```
                await ddbDocClient.send(new UpdateCommand(event.payload));
                break;
            case 'delete':
                await ddbDocClient.send(new DeleteCommand(event.payload));
                break;
            default:
              return ('Unknown operation: ${operation}');
            }
    }
};
```

> **Note**
>
> In diesem Beispiel ist der Name der DynamoDB-Tabelle als Variable in Ihrem Funktionscode definiert. In einer realen Anwendung besteht die bewährte Methode darin, diesen Parameter als Umgebungsvariable zu übergeben und den Tabellennamen nicht fest zu codieren. Weitere Informationen finden Sie unter AWS Lambda Umgebungsvariablen verwenden.

So erstellen Sie die Funktion

1. Speichern Sie das Codebeispiel als eine Datei mit dem Namen `index.mjs` und bearbeiten Sie gegebenenfalls die im Code angegebene AWS Region. Die im Code angegebene Region muss mit der Region übereinstimmen, in der Sie Ihre DynamoDB-Tabelle später im Tutorial erstellen.
2. Erstellen Sie ein Bereitstellungspaket mit dem folgenden `zip`-Befehl.

   ```
   zip function.zip index.mjs
   ```

3. Erstellen Sie mit dem `create-function` AWS CLI Befehl eine Lambda-Funktion. Geben Sie für den `role`-Parameter den zuvor kopierten Amazon-Ressourcennamen (ARN) der Ausführungsrolle ein.

   ```
   aws lambda create-function \
   --function-name LambdaFunctionOverHttps \
   --zip-file fileb://function.zip \
   --handler index.handler \
   --runtime nodejs20.x \
   ```

```
--role arn:aws:iam::123456789012:role/service-role/lambda-apigateway-role
```

Python 3

Example LambdaFunctionOverHttps.py

```
import boto3
import json

# define the DynamoDB table that Lambda will connect to
tableName = "lambda-apigateway"

# create the DynamoDB resource
dynamo = boto3.resource('dynamodb').Table(tableName)

print('Loading function')

def lambda_handler(event, context):
    '''Provide an event that contains the following keys:

      - operation: one of the operations in the operations dict below
      - payload: a JSON object containing parameters to pass to the
                 operation being performed
    '''

    # define the functions used to perform the CRUD operations
    def ddb_create(x):
        dynamo.put_item(**x)

    def ddb_read(x):
        dynamo.get_item(**x)

    def ddb_update(x):
        dynamo.update_item(**x)

    def ddb_delete(x):
        dynamo.delete_item(**x)

    def echo(x):
        return x

    operation = event['operation']
```

```
    operations = {
        'create': ddb_create,
        'read': ddb_read,
        'update': ddb_update,
        'delete': ddb_delete,
        'echo': echo,
    }

    if operation in operations:
        return operations[operation](event.get('payload'))
    else:
        raise ValueError('Unrecognized operation "{}"'.format(operation))
```

> **Note**
>
> In diesem Beispiel ist der Name der DynamoDB-Tabelle als Variable in Ihrem Funktionscode definiert. In einer realen Anwendung besteht die bewährte Methode darin, diesen Parameter als Umgebungsvariable zu übergeben und den Tabellennamen nicht fest zu codieren. Weitere Informationen finden Sie unter AWS Lambda Umgebungsvariablen verwenden.

So erstellen Sie die Funktion

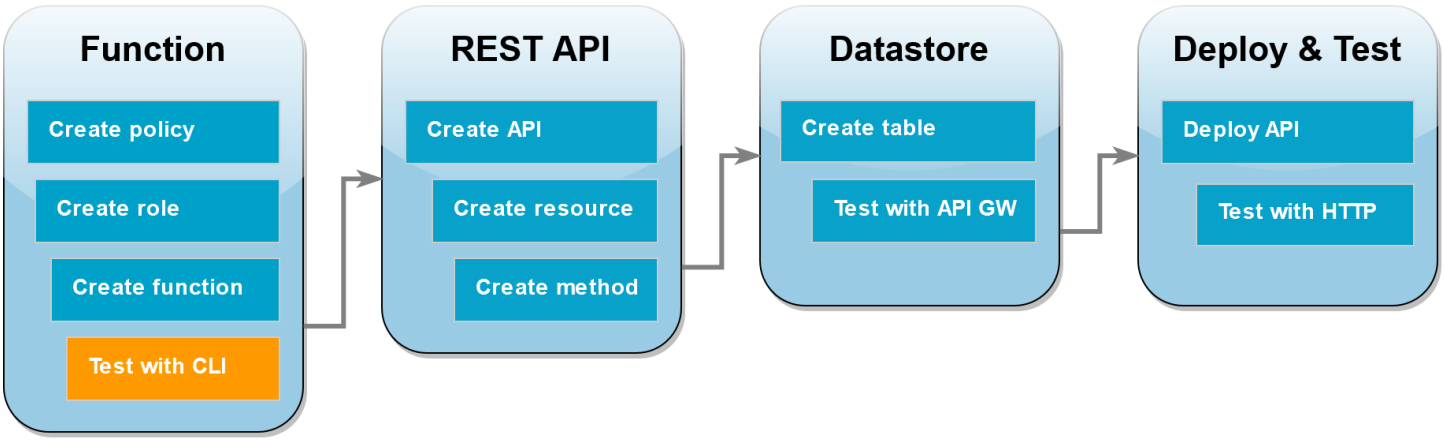
1. Speichern Sie das Codebeispiel als Datei mit dem Namen `LambdaFunctionOverHttps.py`.
2. Erstellen Sie ein Bereitstellungspaket mit dem folgenden `zip`-Befehl.

   ```
   zip function.zip LambdaFunctionOverHttps.py
   ```

3. Erstellen Sie mit dem `create-function` AWS CLI Befehl eine Lambda-Funktion. Geben Sie für den `role`-Parameter den zuvor kopierten Amazon-Ressourcennamen (ARN) der Ausführungsrolle ein.

   ```
   aws lambda create-function \
   --function-name LambdaFunctionOverHttps \
   --zip-file fileb://function.zip \
   --handler LambdaFunctionOverHttps.lambda_handler \
   --runtime python3.12 \
   --role arn:aws:iam::123456789012:role/service-role/lambda-apigateway-role
   ```

Rufen Sie die Funktion mit dem AWS CLI



Bestätigen Sie vor der Integration Ihrer Funktion mit API-Gateway, dass Sie die Funktion erfolgreich bereitgestellt haben. Erstellen Sie ein Testereignis mit den Parametern, die Ihre API-Gateway-API an Lambda sendet, und verwenden Sie den AWS CLI `invoke` Befehl, um Ihre Funktion auszuführen.

Um die Lambda-Funktion aufzurufen mit AWS CLI

1. Speichern Sie die folgende JSON als Datei mit dem Namen `input.txt`.

```
{
    "operation": "echo",
    "payload": {
        "somekey1": "somevalue1",
        "somekey2": "somevalue2"
    }
}
```

2. Führen Sie den Befehl `invoke` AWS CLI aus.

```
aws lambda invoke \
--function-name LambdaFunctionOverHttps \
--payload file://input.txt outputfile.txt \
--cli-binary-format raw-in-base64-out
```

   Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

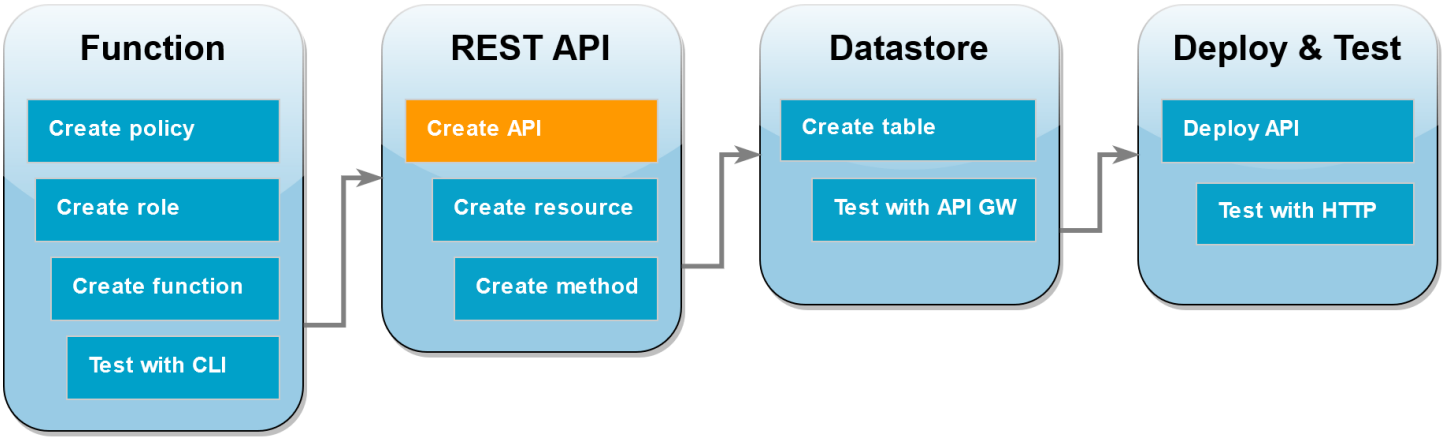
Sie sollten die folgende Antwort sehen:

```
{
"StatusCode": 200,
"ExecutedVersion": "LATEST"
}
```

3. Bestätigen Sie, dass Ihre Funktion die `echo`-Operation ausgeführt hat, die Sie im JSON-Testereignis angegeben haben. Überprüfen Sie die `outputfile.txt`-Datei und stellen Sie sicher, dass diese Folgendes enthält:

```
{"somekey1": "somevalue1", "somekey2": "somevalue2"}
```

Erstellen Sie eine REST-API mit API Gateway

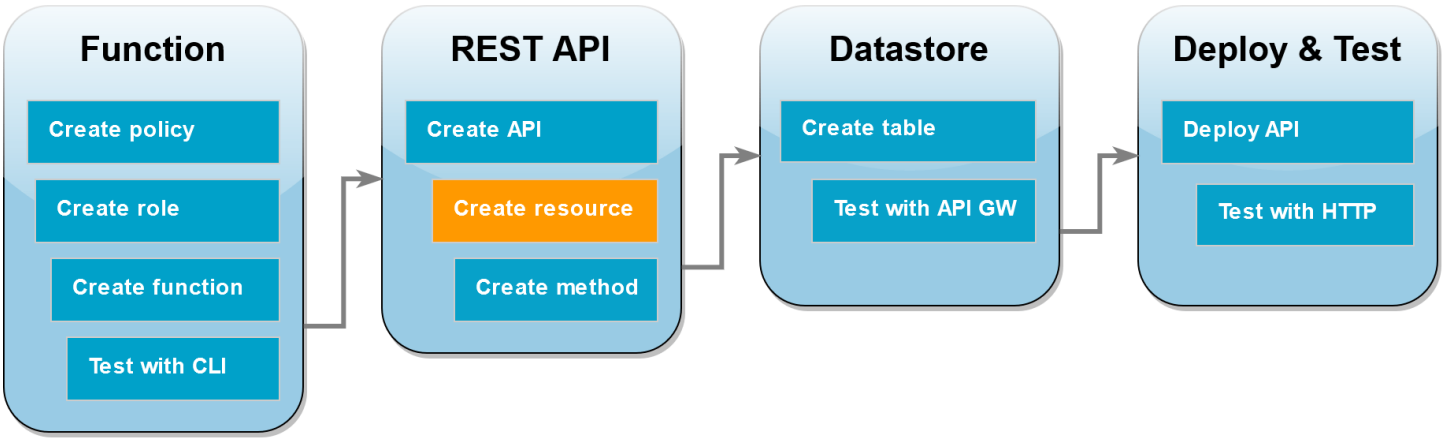


In diesem Schritt erstellen Sie die API-Gateway-REST-API, die Sie zum Aufrufen Ihrer Lambda-Funktion verwenden.

So erstellen Sie die API

1. Öffnen Sie die API Gateway-Konsole.
2. Wählen Sie Create API (API erstellen) aus.
3. Wählen Sie im Feld REST-API die Option Entwickeln aus.
4. Lassen Sie unter API details (API-Details) die Option New API (Neue API) ausgewählt und geben Sie für API Name (API-Name) **`DynamoDBOperations`** ein.
5. Wählen Sie Create API (API erstellen) aus.

Erstellen einer Ressource für Ihre REST-API

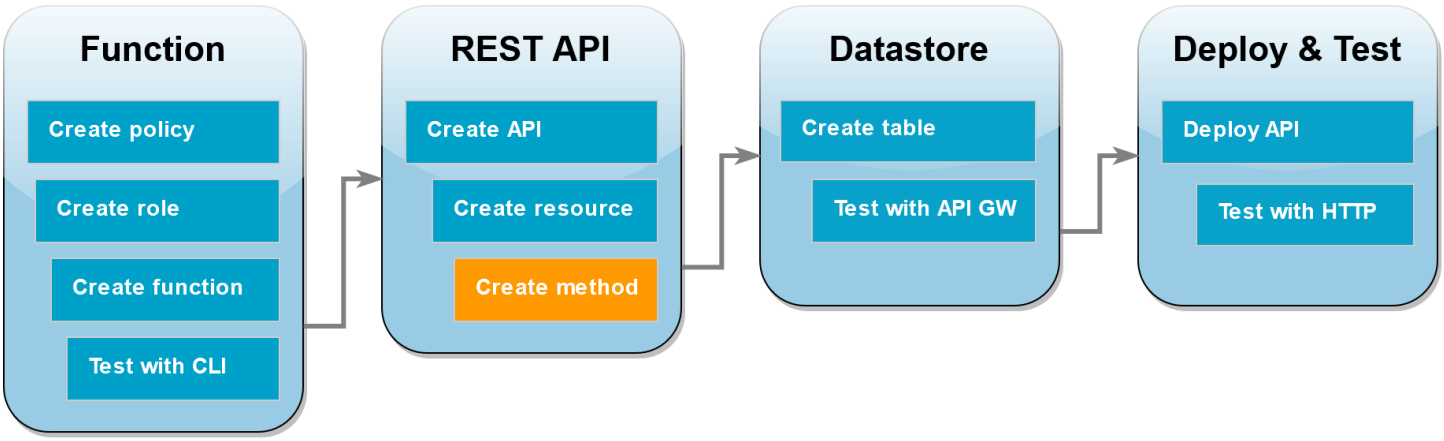


Um Ihrer API eine HTTP-Methode hinzuzufügen, müssen Sie zunächst eine Ressource erstellen, mit der diese Methode ausgeführt werden kann. Hier erstellen Sie die Ressource zur Verwaltung Ihrer DynamoDB-Tabelle.

So erstellen Sie die Ressource

1. Wählen Sie in der API Gateway-Konsole auf der Seite Resources (Ressourcen) für Ihre API die Option Create Resource (Ressource erstellen) aus.
2. Geben Sie im Feld Resource details (Ressourcendetails) für Resource name (Ressourcenname) **`DynamoDBManager`** ein.
3. Wählen Sie Create Resource (Ressource erstellen) aus.

Erstellen einer HTTP-POST-Methode



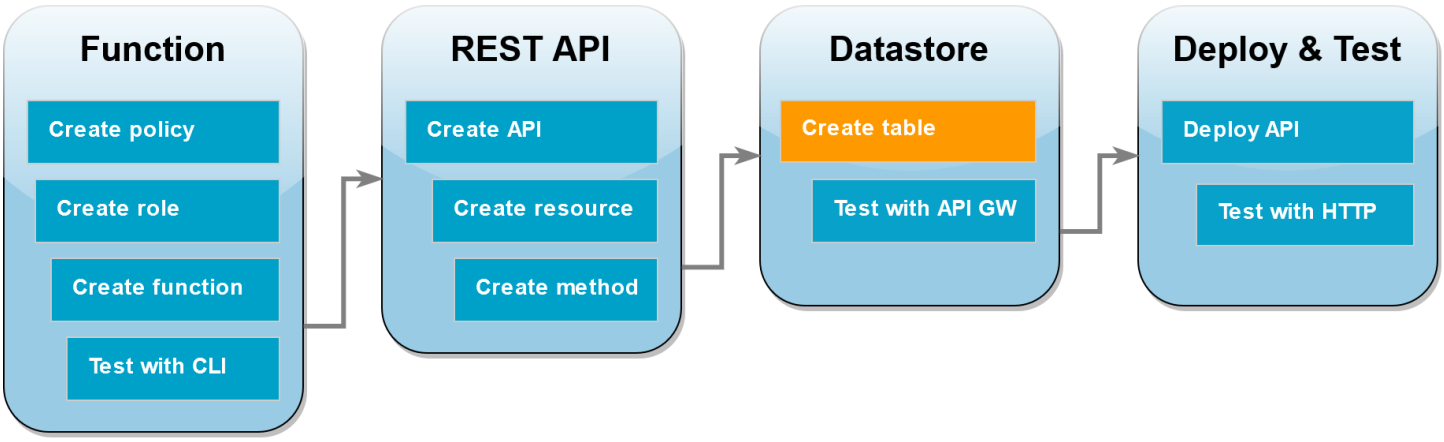
In diesem Schritt erstellen Sie eine Methode (`POST`) für Ihre `DynamoDBManager`-Ressource. Sie verknüpfen diese `POST`-Methode mit Ihrer Lambda-Funktion, sodass API-Gateway Ihre Lambda-Funktion aufruft, wenn die Methode eine HTTP-Anfrage empfängt.

> **Note**
>
> Für die Zwecke dieses Tutorials wird eine HTTP-Methode (`POST`) verwendet, um eine einzelne Lambda-Funktion aufzurufen, die alle Operationen in Ihrer DynamoDB-Tabelle ausführt. In einer realen Anwendung besteht die bewährte Methode darin, für jede Operation eine andere Lambda-Funktion und HTTP-Methode zu verwenden. Weitere Informationen finden Sie bei Serverless Land unter The Lambda monolith.

So erstellen Sie die POST-Methode

1. Vergewissern Sie sich, dass die `/DynamoDBManager`-Ressource auf der Seite Resources (Ressourcen) für Ihre API markiert ist. Wählen Sie dann im Bereich Methods (Methoden) die Option Create Method (Methode erstellen) aus.
2. Wählen Sie in Method type (Methodentyp) POST.
3. Lassen Sie für den Integration type (Integrationstyp) die Option Lambda function (Lambda-Funktion) ausgewählt.
4. Wählen Sie für die Lambda function (Lambda-Funktion) den Amazon Ressourcennamen (ARN) für Ihre Funktion (`LambdaFunctionOverHttps`).
5. Wählen Sie Methode erstellen aus.

Erstellen einer DynamoDB-Tabelle

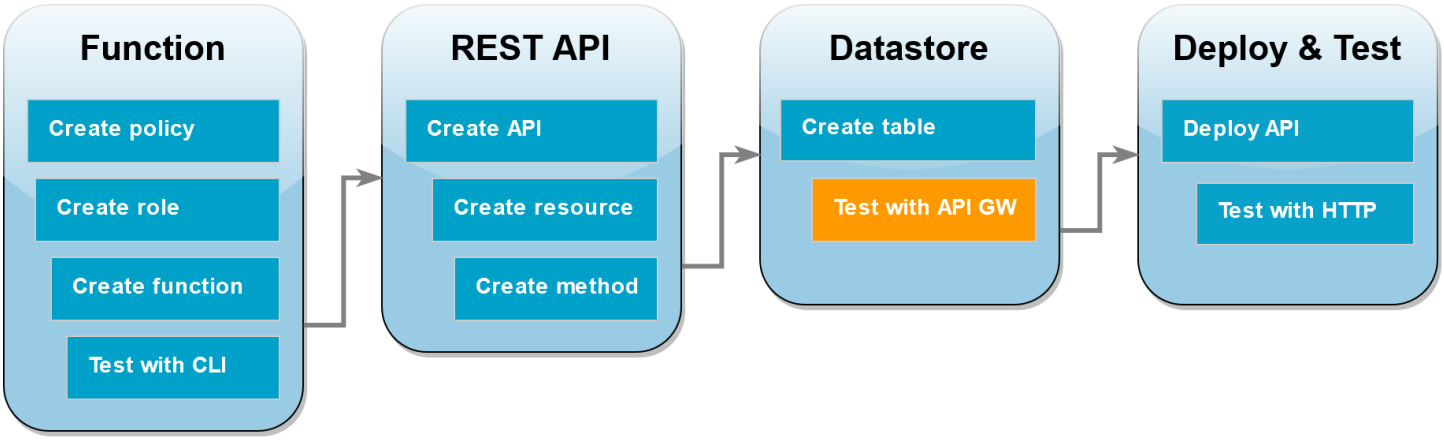


Erstellen Sie eine leere DynamoDB-Tabelle, an der Ihre Lambda-Funktion CRUD-Operationen ausführt.

Erstellen einer DynamoDB-Tabelle

1. Öffnen Sie die Seite Tables (Tabellen) in der DynamoDB-Konsole.
2. Wählen Sie Create table (Tabelle erstellen) aus.
3. Führen Sie unter Tabellendetails die folgenden Schritte aus:
    1. Geben Sie für Table name (Tabellenname) **`lambda-apigateway`** ein.
    2. Geben Sie für Partitionsschlüssel **`id`** ein und behalten Sie den Datentyp als Zeichenfolge bei.
4. Behalten Sie unter Table settings (Tabelleneinstellungen) die Default settings (Standardeinstellungen) bei.
5. Wählen Sie Create table (Tabelle erstellen) aus.

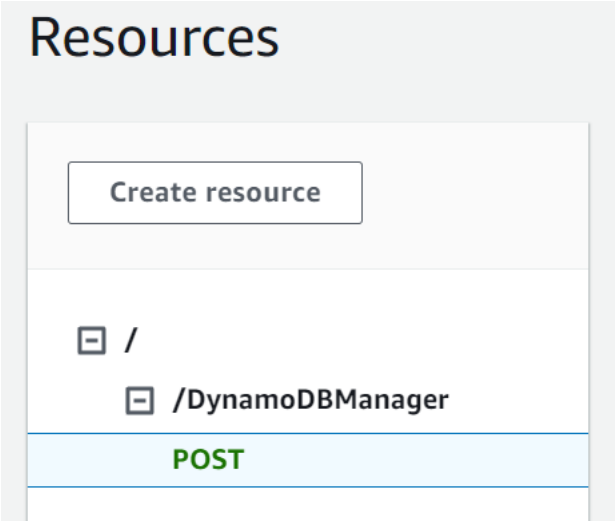
Testen der Integration von API-Gateway, Lambda und DynamoDB



Sie können nun die Integration Ihrer APIä-Gateway-API-Methode mit Ihrer Lambda-Funktion und Ihrer DynamoDB-Tabelle testen. Mit der API Gateway-Konsole senden Sie Anfragen mithilfe der Testfunktion der Konsole direkt an Ihre `POST`-Methode. In diesem Schritt verwenden Sie zuerst eine `create`-Operation, um Ihrer DynamoDB-Tabelle ein neues Element hinzuzufügen, und verwenden dann eine `update`-Operation, um das Element zu ändern.

Test 1: So erstellen Sie ein neues Element in Ihrer DynamoDB-Tabelle

1. Wählen Sie in der API-Gateway-Konsole Ihre API aus (`DynamoDBOperations`).
2. Wählen Sie unter der `DynamoDBManager` Ressource die POST-Methode aus.



3. Wählen Sie die Registerkarte Test. Möglicherweise müssen Sie die rechte Pfeiltaste wählen, um die Registerkarte anzuzeigen.
4. Lassen Sie unter Test method (Testmethode) die Felder Query strings (Query-Strings) und Headers (Header) leer. Fügen Sie für Request body (Anforderungstext) den folgenden JSON-Code ein:

```
{
  "operation": "create",
  "payload": {
    "Item": {
      "id": "1234ABCD",
      "number": 5
    }
  }
}
```

5. Wählen Sie Test aus.

   Die Ergebnisse, die nach Abschluss des Tests angezeigt werden, sollten den Status `200` anzeigen. Dieser Statuscode zeigt an, dass die `create`-Operation erfolgreich war.

   Überprüfen Sie zur Bestätigung, ob Ihre DynamoDB-Tabelle jetzt das neue Element enthält.
6. Öffnen Sie die Seite Tabellen der DynamoDB-Konsole und wählen Sie die `lambda-apigateway`-Tabelle aus.
7. Wählen Sie Explore table items (Tabellenelemente erkunden) aus. Im Bereich Items returned (Zurückgegebene Elemente) sollten ein Element mit der id (ID) `1234ABCD` und der number (Nummer) `5` angezeigt werden.

Test 2: So aktualisieren Sie das Element in Ihrer DynamoDB-Tabelle

1. Kehren Sie in der API-Gateway-Konsole zum Bereich Test Ihrer POST-Methode zurück.
2. Lassen Sie unter Test method (Testmethode) die Felder Query strings (Query-Strings) und Headers (Header) leer. Fügen Sie für Request body (Anforderungstext) den folgenden JSON-Code ein:

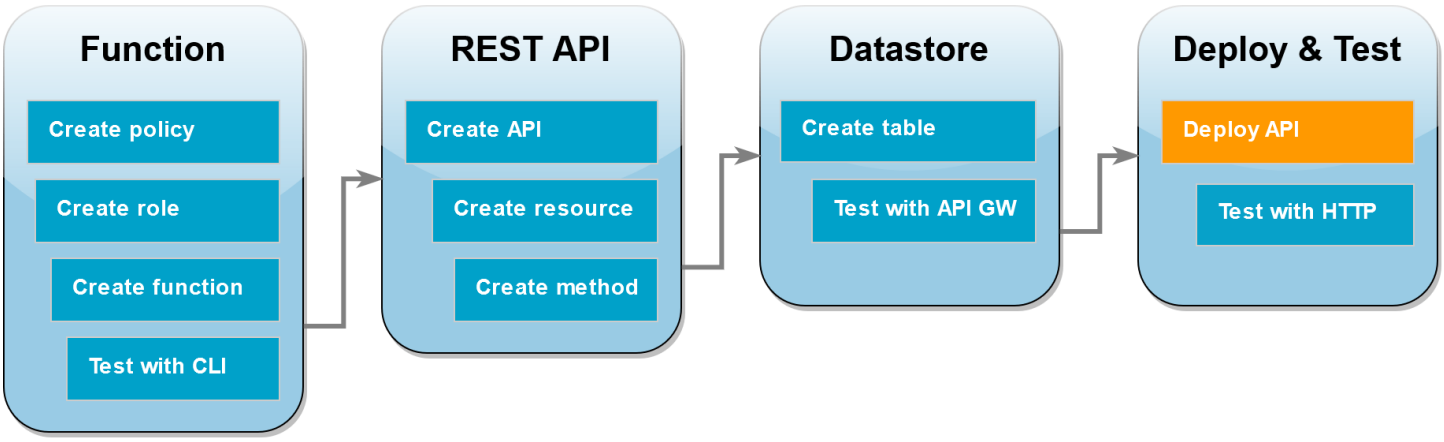
```
{
    "operation": "update",
    "payload": {
        "Key": {
            "id": "1234ABCD"
        },
        "AttributeUpdates": {
            "number": {
                "Value": 10
            }
        }
    }
}
```

3. Wählen Sie Test aus.

   Die Ergebnisse, die nach Abschluss des Tests angezeigt werden, sollten den Status `200` anzeigen. Dieser Statuscode zeigt an, dass die `update`-Operation erfolgreich war.

   Überprüfen Sie zur Bestätigung, ob das Element in Ihrer DynamoDB-Tabelle geändert wurde.
4. Öffnen Sie die Seite Tabellen der DynamoDB-Konsole und wählen Sie die `lambda-apigateway`-Tabelle aus.
5. Wählen Sie Explore table items (Tabellenelemente erkunden) aus. Im Bereich Items returned (Zurückgegebene Elemente) sollten ein Element mit der id (ID) `1234ABCD` und der number (Nummer) `10` angezeigt werden.

Bereitstellen der API

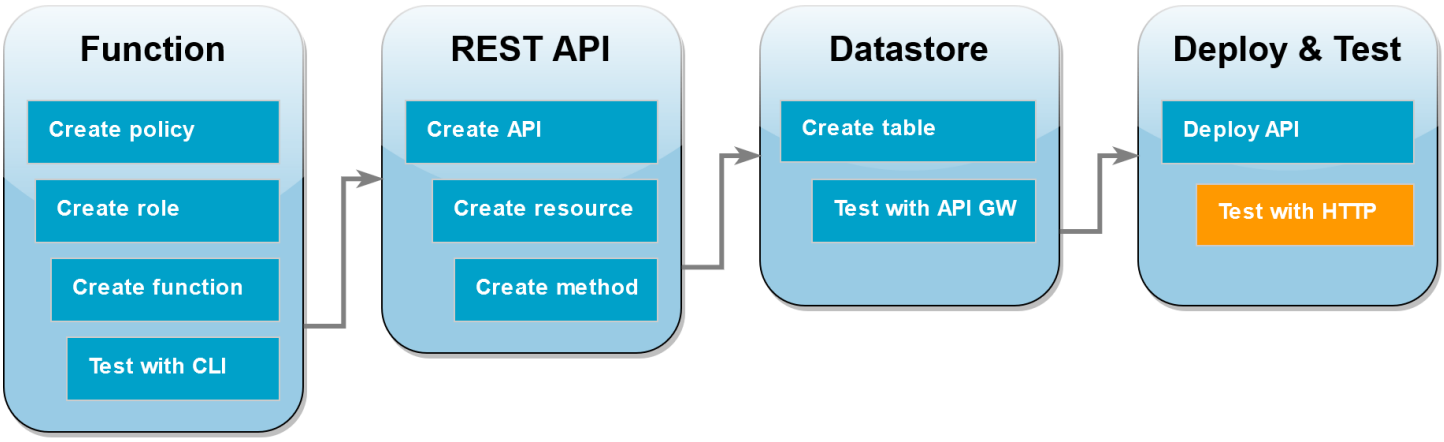


Damit ein Client die API aufrufen kann, müssen Sie eine Bereitstellung und eine zugehörige Stufe erstellen. Eine Phase stellt eine Momentaufnahme Ihrer API dar, einschließlich ihrer Methoden und Integrationen.

So stellen Sie die API bereit

1. Öffnen Sie die APIs-Seite der API-Gateway-Konsole und wählen Sie die `DynamoDBOperations`-API aus.
2. Wählen Sie auf der Seite Resources (Ressourcen) für Ihre API die Option Deploy API (API bereitstellen) aus.
3. Wählen Sie für Stage (Stufe) *New stage* (*Neue Stufe*) und geben Sie dann als Stage name (Phasenname) **`test`** ein.
4. Wählen Sie Bereitstellen.
5. Kopieren Sie im Bereich Stage details (Stufendetails) die Invoke URL (Aufruf-URL). Sie werden diese im nächsten Schritt verwenden, um Ihre Funktion mithilfe einer HTTP-Anfrage aufzurufen.

Verwenden von curl zum Aufrufen Ihrer Funktion mithilfe von HTTP-Anfragen



Sie können Ihre Lambda-Funktion jetzt aufrufen, indem Sie eine HTTP-Anfrage an Ihre API senden. In diesem Schritt erstellen Sie ein neues Element in Ihrer DynamoDB-Tabelle und löschen es anschließend.

So rufen Sie die Lambda-Funktion mit curl auf

1. Führen Sie den folgenden `curl`-Befehl mit der Aufruf-URL aus, die Sie im vorherigen Schritt kopiert haben. Wenn Sie curl mit der `-d` (Daten)-Option verwenden, wird automatisch die HTTP-POST-Methode verwendet.

   ```
   curl https://l8togsqxd8.execute-api.us-west-2.amazonaws.com/test/DynamoDBManager \
   -d '{"operation": "create", "payload": {"Item": {"id": "5678EFGH", "number": 15}}}'
   ```

2. Gehen Sie wie folgt vor, um zu überprüfen, ob der Erstellungsvorgang erfolgreich war:

   1. Öffnen Sie die Seite Tabellen in der DynamoDB-Konsole und wählen Sie die `lambda-apigateway`-Tabelle aus.
   2. Wählen Sie Explore Table Items (Tabellenelemente erkudnen) aus. Im Bereich Items returned (Zurückgegebene Elemente) sollte ein Element mit der id (ID) `5678EFGH` und der number (Nummer) `15` angezeigt werden.

3. Führen Sie den folgenden `curl`-Befehl aus, um das soeben erstellte Element zu löschen. Verwenden Sie Ihre eigene Aufruf-URL.

   ```
   curl https://l8togsqxd8.execute-api.us-west-2.amazonaws.com/test/DynamoDBManager \
   -d '{"operation": "delete", "payload": {"Key": {"id": "5678EFGH"}}}'
   ```

4. Bestätigen Sie, dass der Löschvorgang erfolgreich war. Stellen Sie im Bereich Items returned (Zurückgegebene Elemente) der Seite Explore items (Elemente erkunden) der DynamoDB-Konsole sicher, dass das Element mit der id (ID) `5678EFGH` nicht mehr in der Tabelle enthalten ist.

Bereinigen Ihrer Ressourcen (optional)

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die API

1. Öffnen Sie die API-Seite der API-Gateway-Konsole.
2. Wählen Sie die von Ihnen erstellte API aus.
3. Wählen Sie Aktionen, Löschen aus.
4. Wählen Sie Delete (Löschen) aus.

So löschen Sie die DynamoDB-Tabelle

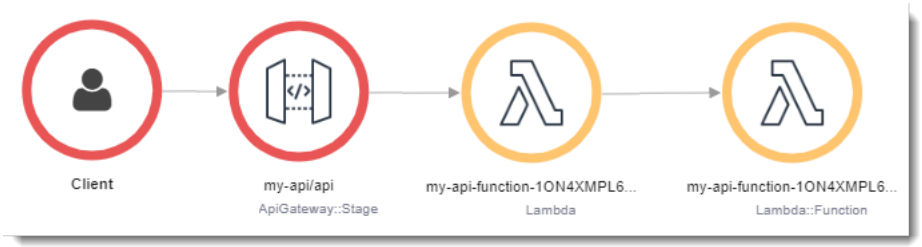
1. Öffnen Sie die Seite Tables (Tabellen) in der DynamoDB-Konsole.
2. Wählen Sie die von Ihnen erstellte Tabelle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie **`delete`** in das Textfeld ein.
5. Wählen Sie Delete Table (Tabelle löschen).

Behandlung von Lambda-Fehlern mit einer API-Gateway-API

API Gateway behandelt alle Aufruf- und Funktionsfehler als interne Fehler. Wenn die Lambda-API die Aufruf-Anforderung ablehnt, gibt API Gateway einen 500-Fehlercode zurück. Wenn die Funktion ausgeführt wird, aber einen Fehler oder eine Antwort im falschen Format zurückgibt, gibt API Gateway den Fehlercode 502 zurück. In beiden Fällen lautet der Text der Antwort von API Gateway „`{"message": "Internal server error"}`“.

> **Note**
>
> API Gateway wiederholt keine Lambda-Aufrufe. Wenn Lambda einen Fehler zurückgibt, gibt API Gateway eine Fehlerantwort an den Client zurück.

Das folgende Beispiel zeigt eine X-Ray-Ablaufverfolgungszuordnung für eine Anforderung, die zu einem Funktionsfehler und einen 502-Fehler von API Gateway führte. Der Client erhält die generische Fehlermeldung.



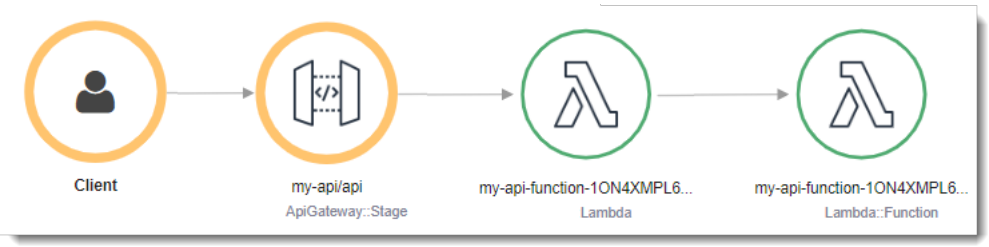
Um die Fehlerantwort anzupassen, müssen Sie Fehler im Code abfangen und eine Antwort im erforderlichen Format formatieren.

Example index.mjs – Formatierfehler

```
var formatError = function(error){
```

```
  var response = {
    "statusCode": error.statusCode,
    "headers": {
      "Content-Type": "text/plain",
      "x-amzn-ErrorType": error.code
    },
    "isBase64Encoded": false,
    "body": error.code + ": " + error.message
  }
  return response
}
```

API Gateway konvertiert diese Antwort in einen HTTP-Fehler mit einem benutzerdefinierten Statuscode und Text. In der Ablaufverfolgungszuweisung ist der Funktionsknoten grün, da er den Fehler behandelt hat.



Verwenden AWS Lambda mit AWS Application Composer

AWS Application Composer ist ein Visual Builder zum Entwerfen moderner Anwendungen auf AWS. Sie entwerfen Ihre Anwendungsarchitektur, indem Sie sie auf einer visuellen Leinwand ziehen, gruppieren und verbinden AWS-Services . Application Composer erstellt anhand Ihres Entwurfs IaC-Vorlagen (Infrastructure as Code), die Sie mithilfe von AWS SAM oder AWS CloudFormation bereitstellen können.

Exportieren einer Lambda-Funktion nach Application Composer

Sie können mit der Verwendung von Application Composer beginnen, indem Sie mithilfe der Lambda-Konsole ein neues Projekt erstellen, das auf der Konfiguration einer vorhandenen Lambda-Funktion basiert. Gehen Sie wie folgt vor, um die Konfiguration und den Code Ihrer Funktion nach Application Composer zu exportieren und ein neues Projekt zu erstellen:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie die Funktion aus, die Sie als Grundlage für Ihr Application-Composer-Projekt verwenden möchten.
3. Wählen Sie im Bereich Funktionsübersicht die Option Nach Application Composer exportieren aus.

   Um die Konfiguration und den Code Ihrer Funktion nach Application Composer zu exportieren, erstellt Lambda einen Amazon-S3-Bucket in Ihrem Konto, um diese Daten vorübergehend zu speichern.
4. Wählen Sie im Dialogfeld Projekt bestätigen und erstellen aus, um den Standardnamen für diesen Bucket zu akzeptieren und die Konfiguration und den Code Ihrer Funktion nach Application Composer zu exportieren.
5. (Optional) Um einen anderen Namen für den von Lambda erstellten Amazon-S3-Bucket auszuwählen, geben Sie einen neuen Namen ein und wählen Sie Projekt bestätigen und erstellen aus. Die Amazon-S3-Bucket-Namen müssen global eindeutig sein und den Regeln für die Benennung von Buckets entsprechen.
6. Um Ihre Projekt- und Funktionsdateien in Application Composer zu speichern, aktivieren Sie den lokalen Synchronisierungsmodus.

> **Note**
>
> Wenn Sie die Funktion Nach Application Composer exportieren bereits verwendet und einen Amazon-S3-Bucket mit dem Standardnamen erstellt haben, kann Lambda diesen Bucket wiederverwenden, falls er noch existiert. Akzeptieren Sie den Standard-Bucket-Namen im Dialogfeld, um den vorhandenen Bucket wiederzuverwenden.

Konfiguration des Amazon-S3-Transfer-Buckets

Der Amazon-S3-Bucket, den Lambda für die Übertragung der Konfiguration Ihrer Funktion erstellt, verschlüsselt Objekte automatisch mit dem Verschlüsselungsstandard AES 256. Lambda konfiguriert den Bucket auch so, dass er die Bucket-Besitzer-Bedingung verwendet, um sicherzustellen, dass nur Sie AWS-Konto Objekte zum Bucket hinzufügen können.

Lambda konfiguriert den Bucket so, dass Objekte 10 Tage nach dem Hochladen automatisch gelöscht werden. Lambda löscht den Bucket selbst jedoch nicht automatisch. Um den Bucket aus Ihrem zu löschen AWS-Konto, folgen Sie den Anweisungen unter Bucket löschen. Der Standard-

Bucket-Name verwendet das Präfix`lambdasam`, eine 10-stellige alphanumerische Zeichenfolge und das, in dem AWS-Region Sie Ihre Funktion erstellt haben:

```
lambdasam-06f22da95b-us-east-1
```

Um zusätzliche Gebühren zu vermeiden, empfehlen wir Ihnen AWS-Konto, den Amazon S3 S3-Bucket zu löschen, sobald Sie den Export Ihrer Funktion in Application Composer abgeschlossen haben.

Es gelten die Standardpreise von Amazon S3.

Erforderliche Berechtigungen

Um die Lambda-Integration mit Application Composer nutzen zu können, benötigen Sie bestimmte Berechtigungen, um eine AWS SAM Vorlage herunterzuladen und die Konfiguration Ihrer Funktion in Amazon S3 zu schreiben.

Um eine AWS SAM Vorlage herunterzuladen, benötigen Sie die Erlaubnis, die folgenden API-Aktionen zu verwenden:

- GetPolicy
- iam: Version GetPolicy
- ich bin: GetRole
- iam: Richtlinie GetRole
- ich bin: ListAttached RolePolicies
- iam: Richtlinien ListRole
- iam: ListRoles

Sie können die Erlaubnis zur Verwendung all dieser Aktionen erteilen, indem Sie die `AWSLambda_ReadOnlyAccess` AWS verwaltete Richtlinie zu Ihrer IAM-Benutzerrolle hinzufügen.

Damit Lambda die Konfiguration Ihrer Funktion in Amazon S3 schreiben kann, benötigen Sie die Erlaubnis, die folgenden API-Aktionen zu verwenden:

- S3: PutObject
- S 3: CreateBucket
- S3: PutBucket Verschlüsselung

- S3: PutBucket LifecycleConfiguration

Wenn Sie die Konfiguration Ihrer Funktion nicht nach Application Composer exportieren können, überprüfen Sie, ob Ihr Konto über die erforderlichen Berechtigungen für diese Operationen verfügt. Wenn Sie über die erforderlichen Berechtigungen verfügen, die Konfiguration Ihrer Funktion aber immer noch nicht exportieren können, suchen Sie nach ressourcenbasierten Richtlinien, die möglicherweise den Zugriff auf Amazon S3 einschränken.

Sonstige Ressourcen

Ein ausführlicheres Tutorial zum Entwerfen einer Serverless-Anwendung in Application Composer auf der Grundlage einer vorhandenen Lambda-Funktion finden Sie unter the section called “Infrastructure as Code (IaC)”.

Um Application Composer AWS SAM zu verwenden und eine vollständige serverlose Anwendung mit Lambda zu entwerfen und bereitzustellen, können Sie auch dem AWS Application Composer Tutorial im AWS Serverless Patterns Workshop folgen.

Lambda mit CloudWatch Protokollen verwenden

Sie können eine Lambda-Funktion verwenden, um Protokolle aus einem Amazon CloudWatch Logs-Protokollstream zu überwachen und zu analysieren. Erstellen Sie Abonnements für einen oder mehrere Protokoll-Streams, um eine Funktion aufzurufen, wenn Protokolle erstellt werden oder mit einem optionalen Muster übereinstimmen. Verwenden Sie die Funktion, um eine Benachrichtigung zu senden oder das Protokoll an eine Datenbank oder einen Speicher weiterzugeben.

CloudWatch Logs ruft Ihre Funktion asynchron mit einem Ereignis auf, das Protokolldaten enthält. Der Wert des Datenfelds ist ein Base64-codiertes ZIP-Dateiarchiv.

Example CloudWatch Protokolliert das Nachrichtenereignis

```
{
  "awslogs": {
    "data":
 "ewogICAgIm1lc3NhZ2VUeXBlIjogIkRBVEFfTUVTU0FHRSIsCiAgICAib3duZXIiOiAiMTIzNDU2Nzg5MDEyIiwKICAgI
  }
}
```

Nach ihrer Entschlüsselung ist die Protokolldatei ein JSON-Dokument mit der folgenden Struktur.

Example CloudWatch Protokolliert Nachrichtendaten (dekodiert)

```
{
    "messageType": "DATA_MESSAGE",
    "owner": "123456789012",
    "logGroup": "/aws/lambda/echo-nodejs",
    "logStream": "2019/03/13/[$LATEST]94fa867e5374431291a7fc14e2f56ae7",
    "subscriptionFilters": [
        "LambdaStream_cloudwatchlogs-node"
    ],
    "logEvents": [
        {
            "id": "34622316099697884706540976068822859012661220141643892546",
            "timestamp": 1552518348220,
            "message": "REPORT RequestId: 6234bffe-149a-b642-81ff-2e8e376d8aff
\tDuration: 46.84 ms\tBilled Duration: 47 ms \tMemory Size: 192 MB\tMax Memory Used: 72
 MB\t\n"
        }
    ]
```

```
}
```

Verwenden AWS Lambda mit AWS CloudFormation

In einer AWS CloudFormation Vorlage können Sie eine Lambda-Funktion als Ziel einer benutzerdefinierten Ressource angeben. Verwenden Sie benutzerdefinierte Ressourcen, um während Ereignissen im Stack-Lebenszyklus Parameter zu verarbeiten, Konfigurationswerte abzurufen oder andere AWS Dienste aufzurufen.

Das folgende Beispiel ruft eine Funktion auf, die an anderer Stelle in der Vorlage definiert ist.

Example – benutzerdefinierte Ressourcendefinition

```
Resources:
  primerinvoke:
    Type: AWS::CloudFormation::CustomResource
    Version: "1.0"
    Properties:
      ServiceToken: !GetAtt primer.Arn
      FunctionName: !Ref randomerror
```

Das Service-Token ist der Amazon-Ressourcenname (ARN) der Funktion, die AWS CloudFormation aufgerufen wird, wenn Sie den Stack erstellen, aktualisieren oder löschen. Sie können auch zusätzliche Eigenschaften hinzufügen`FunctionName`, wie z. B., was AWS CloudFormation unverändert an Ihre Funktion übergeben wird.

AWS CloudFormation ruft Ihre Lambda-Funktion asynchron mit einem Ereignis auf, das eine Callback-URL enthält.

Example AWS CloudFormation — Nachrichtenereignis

```
{
    "RequestType": "Create",
    "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-
processor-primer-14ROR2T3JKU66",
    "ResponseURL": "https://cloudformation-custom-resource-response-useast1.s3-us-
east-1.amazonaws.com/arn%3Aaws%3Acloudformation%3Aus-east-1%3A123456789012%3Astack/
lambda-error-processor/1134083a-2608-1e91-9897-022501a2c456%7Cprimerinvoke
%7C5d478078-13e9-baf0-464a-7ef285ecc786?
AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Expires=1555451971&Signature=28UijZePE5I4dvukKQqM
%2F9Rf1o4%3D",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-
processor/1134083a-2608-1e91-9897-022501a2c456",
    "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
```

```
    "LogicalResourceId": "primerinvoke",
    "ResourceType": "AWS::CloudFormation::CustomResource",
    "ResourceProperties": {
        "ServiceToken": "arn:aws:lambda:us-east-1:123456789012:function:lambda-error-
processor-primer-14ROR2T3JKU66",
        "FunctionName": "lambda-error-processor-randomerror-ZWUC391MQAJK"
    }
}
```

Die Funktion ist für die Rückgabe einer Antwort an die Rückruf-URL zuständig, die Erfolg oder Misserfolg bedeutet. Die vollständige Antwortsyntax finden Sie unter Benutzerdefinierte Ressourcenantwortobjekte.

Example — AWS CloudFormation benutzerdefinierte Ressourcenantwort

```
{
    "Status": "SUCCESS",
    "PhysicalResourceId": "2019/04/18/[$LATEST]b3d1bfc65f19ec610654e4d9b9de47a0",
    "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/lambda-error-
processor/1134083a-2608-1e91-9897-022501a2c456",
    "RequestId": "5d478078-13e9-baf0-464a-7ef285ecc786",
    "LogicalResourceId": "primerinvoke"
}
```

AWS CloudFormation stellt eine aufgerufene Bibliothek bereit`cfn-response`, die das Senden der Antwort übernimmt. Wenn Sie Ihre Funktion innerhalb einer Vorlage definieren, können Sie die Bibliothek anhand des Namens angeben. AWS CloudFormation fügt dann die Bibliothek dem Bereitstellungspaket hinzu, das sie für die Funktion erstellt.

Wenn Ihre Funktion, die eine benutzerdefinierte Ressource verwendet, mit einer Elastic Network Interface verbunden ist, fügen Sie die folgenden Ressourcen zur VPC-Richtlinie hinzu, wobei **`region`** die Region ist, in der sich die Funktion befindet, ohne Bindestriche angegeben ist. Zum Beispie, `us-east-1` ist `useast1`. Dadurch kann die benutzerdefinierte Ressource auf die Callback-URL antworten, die ein Signal zurück an den AWS CloudFormation Stack sendet.

```
arn:aws:s3:::cloudformation-custom-resource-response-region",
"arn:aws:s3:::cloudformation-custom-resource-response-region/*",
```

Die folgende Beispielfunktion ruft eine zweite Funktion auf. Wenn der Aufruf erfolgreich ist, sendet die Funktion eine Erfolgsantwort an AWS CloudFormation, und das Stack-Update wird fortgesetzt. Die

Vorlage verwendet den AWS::Serverless::FunctionRessourcentyp, der von bereitgestellt wird AWS Serverless Application Model.

Example — Benutzerdefinierte Ressourcenfunktion

```
Transform: 'AWS::Serverless-2016-10-31'
Resources:
  primer:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs16.x
      InlineCode: |
        var aws = require('aws-sdk');
        var response = require('cfn-response');
        exports.handler = function(event, context) {
            // For Delete requests, immediately send a SUCCESS response.
            if (event.RequestType == "Delete") {
                response.send(event, context, "SUCCESS");
                return;
            }
            var responseStatus = "FAILED";
            var responseData = {};
            var functionName = event.ResourceProperties.FunctionName
            var lambda = new aws.Lambda();
            lambda.invoke({ FunctionName: functionName }, function(err, invokeResult) {
                if (err) {
                    responseData = {Error: "Invoke call failed"};
                    console.log(responseData.Error + ":\n", err);
                }
                else responseStatus = "SUCCESS";
                response.send(event, context, responseStatus, responseData);
            });
        };
      Description: Invoke a function to create a log stream.
      MemorySize: 128
      Timeout: 8
      Role: !GetAtt role.Arn
      Tracing: Active
```

Wenn die Funktion, die die benutzerdefinierte Ressource aufruft, nicht in einer Vorlage definiert ist, können Sie den Quellcode für `cfn-response` das Modul cfn-response im AWS CloudFormation Benutzerhandbuch abrufen.

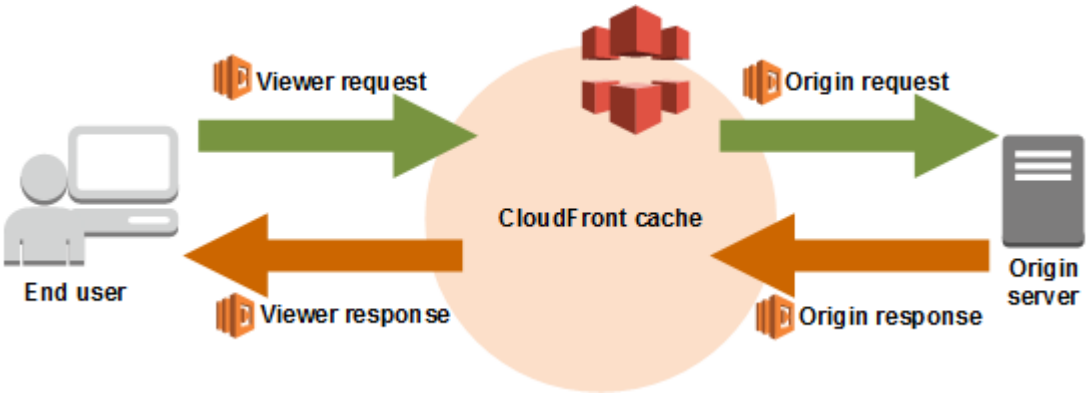
Weitere Informationen zu benutzerdefinierten Ressourcen finden Sie unter Benutzerdefinierte Ressourcen im AWS CloudFormation -Benutzerhandbuch.

Verwenden von AWS Lambda mit CloudFront Lambda@Edge

Lambda@Edge ist eine Erweiterung von AWS Lambda, mit der Sie Python- und Node.js-Funktionen an Amazon CloudFront -Edge-Standorten bereitstellen können. Ein häufiger Anwendungsfall von Lambda@Edge besteht darin, Funktionen zu verwenden, um den Inhalt anzupassen, den Ihre CloudFront Verteilung Ihren Endbenutzern bereitstellt. Der Aufruf dieser Funktionen in der Nähe des Betrachters statt auf den Ursprungsservern reduziert die Latenzzeiten erheblich und verbessert das Benutzererlebnis.

Wenn Sie eine CloudFront Verteilung mit einer Lambda@Edge-Funktion verknüpfen, CloudFront fängt Anfragen und Antworten an CloudFront Edge-Standorten ab. CloudFront ruft dann Ihre Lambda-Funktion auf, indem es ein Ereignis sendet. Sie können Ihre Lambda-Funktion CloudFront aufrufen lassen, wenn die folgenden Ereignisse eintreten:

- Wenn eine Anfrage von einem Betrachter CloudFront erhält (Betrachteranfrage)
- Bevor eine Anforderung an den Ursprung CloudFront weiterleitet (Ursprungsanforderung)
- Wenn eine Antwort vom Ursprung CloudFront empfängt (Ursprungsantwort)
- Bevor die Antwort an den Betrachter CloudFront zurückgibt (Betrachterantwort)



> **Note**
>
> Lambda@Edge unterstützt eine begrenzte Anzahl von Laufzeiten und Funktionen. Weitere Informationen finden Sie unter Anforderungen und Einschränkungen für Lambda-Funktionen im Amazon- CloudFront Entwicklerhandbuch.

Im Folgenden finden Sie ein Beispiel für ein - CloudFront Ereignis.

Example CloudFront Nachrichtenereignis

```
{
  "Records": [
    {
      "cf": {
        "config": {
          "distributionId": "EDFDVBD6EXAMPLE"
        },
        "request": {
          "clientIp": "2001:0db8:85a3:0:0:8a2e:0370:7334",
          "method": "GET",
          "uri": "/picture.jpg",
          "headers": {
            "host": [
              {
                "key": "Host",
                "value": "d111111abcdef8.cloudfront.net"
              }
            ],
            "user-agent": [
              {
                "key": "User-Agent",
                "value": "curl/7.51.0"
              }
            ]
          }
        }
      }
    }
  ]
}
```

Weitere Informationen zur Verwendung von Lambda@Edge finden Sie unter Verwenden von CloudFront mit Lambda@Edge.

Verwenden von AWS Lambda mit AWS CodeCommit

Sie können einen Auslöser für ein AWS CodeCommit-Repository erstellen, damit Ereignisse im Repository eine Lambda-Funktion aufrufen. Sie können zum Beispiel eine Lambda-Funktion aufrufen, wenn ein Branch oder ein Tag erstellt wurde oder ein Push zu einem vorhandenen Branch ausgeführt wurde.

Example AWS CodeCommit-Nachrichtenereignis

```
{
    "Records": [
        {
            "awsRegion": "us-east-2",
            "codecommit": {
                "references": [
                    {
                        "commit": "5e493c6f3067653f3d04eca608b4901eb227078",
                        "ref": "refs/heads/master"
                    }
                ]
            },
            "eventId": "31ade2c7-f889-47c5-a937-1cf99e2790e9",
            "eventName": "ReferenceChanges",
            "eventPartNumber": 1,
            "eventSource": "aws:codecommit",
            "eventSourceARN": "arn:aws:codecommit:us-east-2:123456789012:lambda-
pipeline-repo",
            "eventTime": "2019-03-12T20:58:25.400+0000",
            "eventTotalParts": 1,
            "eventTriggerConfigId": "0d17d6a4-efeb-46f3-b3ab-a63741badeb8",
            "eventTriggerName": "index.handler",
            "eventVersion": "1.0",
            "userIdentityARN": "arn:aws:iam::123456789012:user/intern"
        }
    ]
}
```

Weitere Informationen finden Sie unter Verwalten von Auslösern für ein AWS CodeCommit-Repository.

Verwenden von AWS Lambda mit Amazon Cognito

Mit der Amazon-Cognito-Ereignisfunktion können Sie Lambda-Funktionen als Reaktion auf Ereignisse in Amazon Cognito ausführen. Amazon Cognito bietet Authentifizierung, Autorisierung und Benutzerverwaltung für Ihre Web- und Mobil-Apps. Sie können eine Lambda-Funktion als Reaktion auf wichtige Ereignisse in Amazon Cognito aufrufen. Mit den Sync-Auslöser-Ereignissen können Sie beispielsweise eine Lambda-Funktion aufrufen, die jedes Mal veröffentlicht wird, wenn ein Datensatz synchronisiert wird. Weitere Informationen und ein praktisches Beispiel finden Sie unter Introducing Amazon Cognito Events: Sync Triggers im Entwicklung für Mobilgeräte-Blog.

Example Nachrichten-Ereignis von Amazon Cognito

```
{
  "datasetName": "datasetName",
  "eventType": "SyncTrigger",
  "region": "us-east-1",
  "identityId": "identityId",
  "datasetRecords": {
    "SampleKey2": {
      "newValue": "newValue2",
      "oldValue": "oldValue2",
      "op": "replace"
    },
    "SampleKey1": {
      "newValue": "newValue1",
      "oldValue": "oldValue1",
      "op": "replace"
    }
  },
  "identityPoolId": "identityPoolId",
  "version": 2
}
```

Die Konfiguration des Ereignisquellen-Zuweisung nehmen Sie in Amazon Cognito in der Ereignisabonnement-Konfiguration vor. Weitere Informationen zum Ereignisquellen-Mapping und ein Beispiel-Ereignis finden Sie unter Amazon-Cognito-Ereignisse im Amazon-Cognito-Entwicklerhandbuch.

Verwenden von Lambda mit Amazon Connect

Sie können eine Lambda-Funktion verwenden, um Anforderungen von Amazon Connect zu bearbeiten. Sie können Amazon Connect verwenden, um ein Cloud-Kontakt-Center zu erstellen.

Amazon Connect ruft Ihre Lambda-Funktion synchron mit einem Ereignis auf, das den Text und die Metadaten der Anforderung enthält.

Example Amazon Connect-Anforderungsereignis

```
{
  "Details": {
      "ContactData": {
          "Attributes": {},
          "Channel": "VOICE",
          "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
          "CustomerEndpoint": {
              "Address": "+1234567890",
              "Type": "TELEPHONE_NUMBER"
          },
          "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
          "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
          "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/
c8c0e68d-2200-4265-82c0-XXXXXXXXXX",
          "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
          "Queue": {
             "ARN": "arn:aws:connect:eu-west-2:111111111111:instance/cccccccc-bbbb-
dddd-eeee-ffffffffffff/queue/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
             "Name": "PasswordReset"
           },
          "SystemEndpoint": {
              "Address": "+1234567890",
              "Type": "TELEPHONE_NUMBER"
          }
      },
      "Parameters": {
          "sentAttributeKey": "sentAttributeValue"
      }
  },
  "Name": "ContactFlowEvent"
}
```

Informationen zur Verwendung von Amazon Connect mit finden Sie unter Aufrufen von Lambda-Funktionen im Amazon-Connect-Administratorhandbuch.

Verwendung AWS Lambda mit Amazon EC2

Sie können AWS Lambda es verwenden, um Lebenszyklusereignisse aus Amazon Elastic Compute Cloud zu verarbeiten und Amazon EC2 EC2-Ressourcen zu verwalten. Amazon EC2 sendet Ereignisse an Amazon EventBridge (CloudWatch Events) für Lebenszyklusereignisse, z. B. wenn sich der Status einer Instance ändert, wenn ein Amazon Elastic Block Store-Volume-Snapshot abgeschlossen ist oder wenn die Beendigung einer Spot-Instance geplant ist. Sie konfigurieren EventBridge (CloudWatch Events) so, dass diese Ereignisse zur Verarbeitung an eine Lambda-Funktion weitergeleitet werden.

EventBridge (CloudWatch Events) ruft Ihre Lambda-Funktion asynchron mit dem Ereignisdokument von Amazon EC2 auf.

Example Instance-Lebenszyklusereignis

```
{
    "version": "0",
    "id": "b6ba298a-7732-2226-xmpl-976312c1a050",
    "detail-type": "EC2 Instance State-change Notification",
    "source": "aws.ec2",
    "account": "111122223333",
    "time": "2019-10-02T17:59:30Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:111122223333:instance/i-0c314xmplcd5b8173"
    ],
    "detail": {
        "instance-id": "i-0c314xmplcd5b8173",
        "state": "running"
    }
}
```

Einzelheiten zur Konfiguration von Ereignissen finden Sie unter. Verwenden von Lambda mit Amazon EventBridge Scheduler Eine Beispielfunktion, die Amazon EBS-Snapshot-Benachrichtigungen verarbeitet, finden Sie unter EventBridge Scheduler for Amazon EBS.

Sie können das AWS SDK auch verwenden, um Instances und andere Ressourcen mit der Amazon EC2 EC2-API zu verwalten.

Berechtigungen

Um Lebenszyklusereignisse von Amazon EC2 verarbeiten zu können, benötigt EventBridge (CloudWatch Events) die Erlaubnis, Ihre Funktion aufzurufen. Diese Berechtigung stammt aus der ressourcenbasierten Richtlinie der Funktion. Wenn Sie die Konsole EventBridge (CloudWatch Events) verwenden, um einen Event-Trigger zu konfigurieren, aktualisiert die Konsole die ressourcenbasierte Richtlinie in Ihrem Namen. Andernfalls fügen Sie eine Anweisung wie die folgende hinzu:

Example Ressourcenbasierte Richtlinienanweisung für Amazon-EC2-Lebenszyklusbenachrichtigungen

```
{
  "Sid": "ec2-events",
  "Effect": "Allow",
  "Principal": {
    "Service": "events.amazonaws.com"
  },
  "Action": "lambda:InvokeFunction",
  "Resource": "arn:aws:lambda:us-east-1:12456789012:function:my-function",
  "Condition": {
    "ArnLike": {
      "AWS:SourceArn": "arn:aws:events:us-east-1:12456789012:rule/*"
    }
  }
}
```

Verwenden Sie den Befehl, um eine Anweisung hinzuzufügen. `add-permission` AWS CLI

```
aws lambda add-permission --action lambda:InvokeFunction --statement-id ec2-events \
--principal events.amazonaws.com --function-name my-function --source-arn
 'arn:aws:events:us-east-1:12456789012:rule/*'
```

Wenn Ihre Funktion das AWS SDK zur Verwaltung von Amazon EC2 EC2-Ressourcen verwendet, fügen Sie der Ausführungsrolle der Funktion Amazon EC2 EC2-Berechtigungen hinzu.

Tutorial: Konfigurieren einer Lambda-Funktion für den Zugriff auf Amazon ElastiCache in einer Amazon VPC

Informationen zum Konfigurieren von Lambda für den Zugriff auf Amazon ElastiCache in einer Amazon VPC finden Sie im Lambda-Tutorial im ElastiCache Benutzerhandbuch für Redis.

Verarbeiten von Application Load Balancer Balancer-Anfragen mit Lambda

Sie können eine Lambda-Funktion verwenden, um Anforderungen aus einem Application Load Balancer zu verarbeiten. Elastic Load Balancing unterstützt Lambda-Funktionen als Ziel für Application Load Balancer. Sie können Load Balancer-Regeln zum Weiterleiten von HTTP-Anforderungen an eine Funktion verwenden, basierend auf Pfad- oder Header-Werten. Die Anforderung wird verarbeitet und es wird eine HTTP-Antwort aus Ihrer Lambda-Funktion zurückgegeben.

Elastic Load Balancing ruft Ihre Lambda-Funktion synchron mit einem Ereignis auf, das den Text und die Metadaten der Anforderung enthält.

Example Anforderungsereignis von einem Application Load Balancer

```
{
    "requestContext": {
        "elb": {
            "targetGroupArn": "arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/lambda-279XGJDqGZ5rsrHC2Fjr/49e9d65c45c6791a"
        }
    },
    "httpMethod": "GET",
    "path": "/lambda",
    "queryStringParameters": {
        "query": "1234ABCD"
    },
    "headers": {
        "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8",
        "accept-encoding": "gzip",
        "accept-language": "en-US,en;q=0.9",
        "connection": "keep-alive",
        "host": "lambda-alb-123578498.us-east-1.elb.amazonaws.com",
        "upgrade-insecure-requests": "1",
        "user-agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36",
        "x-amzn-trace-id": "Root=1-5c536348-3d683b8b04734faae651f476",
        "x-forwarded-for": "72.12.164.125",
        "x-forwarded-port": "80",
        "x-forwarded-proto": "http",
```

```
        "x-imforwards": "20"
    },
    "body": "",
    "isBase64Encoded": False
}
```

Ihre Funktion verarbeitet das Ereignis und gibt ein Antwortdokument in JSON an die Lastenverteilung zurück. Elastic Load Balancing konvertiert das Dokument in eine HTTP-Erfolgs- oder Fehlerantwort und gibt es an den Benutzer zurück.

Example Format des Antwortdokuments

```
{
    "statusCode": 200,
    "statusDescription": "200 OK",
    "isBase64Encoded": False,
    "headers": {
        "Content-Type": "text/html"
    },
    "body": "<h1>Hello from Lambda!</h1>"
}
```

Um eine Application Load Balancer als Funktionsauslöser zu konfigurieren, gewähren Sie Elastic Load Balancing die Berechtigung zur Ausführung der Funktion, erstellen eine Zielgruppe, die Anforderungen an die Funktion weiterleitet und fügen der Lastenverteilung eine Regel hinzu, die Anforderungen an die Zielgruppe sendet.

Sie können den Befehl `add-permission` verwenden, um der ressourcenbasierten Richtlinie Ihrer Funktion eine Berechtigungsanweisung hinzuzufügen.

```
aws lambda add-permission --function-name alb-function \
--statement-id load-balancer --action "lambda:InvokeFunction" \
--principal elasticloadbalancing.amazonaws.com
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Statement": "{\"Sid\":\"load-balancer\",\"Effect\":\"Allow\",\"Principal\":
{\"Service\":\"elasticloadbalancing.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction
\",\"Resource\":\"arn:aws:lambda:us-west-2:123456789012:function:alb-function\"}"
}
```

Anweisungen zum Konfigurieren des Application Load Balancer-Listeners und der Zielgruppe finden Sie unter Lambda-Funktionen als Ziel im Benutzerhandbuch für Application Load Balancer.

Verwenden von Amazon EFS mit Lambda

Lambda lässt sich in Amazon Elastic File System (Amazon EFS) integrieren, um sicheren, gemeinsam genutzten Dateisystemzugriff für Lambda-Anwendungen zu unterstützen. Sie können Funktionen konfigurieren, um ein Dateisystem während der Initialisierung mit dem NFS-Protokoll über das lokale Netzwerk innerhalb einer VPC zu mounten. Lambda verwaltet die Verbindung und verschlüsselt den gesamten Datenverkehr zum und vom Dateisystem.

Das Dateisystem und die Lambda-Funktion müssen sich in derselben Region befinden. Eine Lambda-Funktion in einem Konto kann ein Dateisystem in einem anderen Konto mounten. In diesem Szenario konfigurieren Sie VPC-Peering zwischen der Funktion-VPC und der Dateisystem-VPC.

> **Note**
>
> Informationen zum Konfigurieren einer Funktion zum Herstellen einer Verbindung mit einem Dateisystem finden Sie unter Konfigurieren des Dateisystemzugriffs für Lambda-Funktionen.

Amazon EFS unterstützt das Sperren von Dateien, um Beschädigungen zu verhindern, wenn mehrere Funktionen gleichzeitig in dasselbe Dateisystem schreiben. Sperren in Amazon EFS verwenden das NFS v4.1-Protokoll für empfohlene Sperren, das Ihren Anwendungen die Verwendung von Datei- und Byte-Bereichssperren ermöglicht.

Amazon EFS bietet Optionen zum Anpassen des Dateisystems an, basierend auf der Notwendigkeit Ihrer Anwendung, skalierbare hohe Leistung zu halten. Es sind drei Hauptfaktoren zu berücksichtigen: die Anzahl der Verbindungen, der Durchsatz (in MiB pro Sekunde) und IOPS.

> **Kontingente**
>
> Weitere Informationen zu Dateisystemkontingenten und -limits finden Sie unter Kontingente für Amazon-EFS-Dateisysteme im Amazon-Elastic-File-System-Benutzerhandbuch.

Um Probleme mit Skalierung, Durchsatz und IOPS zu vermeiden, überwachen Sie die Metriken, die Amazon EFS an Amazon sendet CloudWatch. Eine Übersicht über die Überwachung in Amazon EFS finden Sie unter Überwachung von Amazon EFS im Amazon-Elastic-File-System-Benutzerhandbuch.

Sections

Verbindungen

Amazon EFS unterstützt bis zu 25.000 Verbindungen pro Dateisystem. Während der Initialisierung erstellt jede Instance einer Funktion eine einzelne Verbindung zu ihrem Dateisystem, die über Aufrufe hinweg besteht. Dies bedeutet, dass Sie 25.000 Nebenläufigkeit über eine oder mehrere Funktionen erreichen können, die mit einem Dateisystem verbunden sind. Um die Anzahl der Verbindungen zu begrenzen, die eine Funktion erstellt, verwenden Sie reservierte Nebenläufigkeit.

Wenn Sie jedoch Änderungen am Code oder der Konfiguration Ihrer Funktion im Maßstab vornehmen, gibt es eine vorübergehende Erhöhung der Anzahl der Funktionsinstances über die aktuelle Nebenläufigkeit hinaus. Lambda stellt neue Instances bereit, um neue Anforderungen zu verarbeiten, und es gibt eine gewisse Verzögerung, bevor alte Instances ihre Verbindungen zum Dateisystem schließen. Verwenden Sie fortlaufende Bereitstellungenum das Maximum an Verbindungen während einer Bereitstellung zu vermeiden. Bei fortlaufender Bereitstellungen verlagern Sie den Datenverkehr bei jeder Änderung schrittweise auf die neue Version.

Wenn Sie sich von anderen Diensten wie zum Beispiel Amazon EC2 mit demselben Dateisystem verbinden, sollten Sie sich auch über das Skalierungsverhalten von Verbindungen in Amazon EFS bewusst sein. Ein Dateisystem unterstützt die Erstellung von bis zu 3.000 Verbindungen in einem Burst, woraufhin es 500 neue Verbindungen pro Minute unterstützt.

Verwenden Sie die `ClientConnections`-Metrik, um einen Alarm bei Verbindungen zu überwachen und auszulösen.

Durchsatz

Im Maßstab ist es auch möglich, den maximalen Durchsatz für ein Dateisystem zu überschreiten. Im Bursting-Modus (Standardeinstellung) weist ein Dateisystem einen niedrigen Basisdurchsatz auf, der linear mit seiner Größe skaliert wird. Um Aktivitätsspitzen zu ermöglichen, werden dem Dateisystem Burst-Credits gewährt, die es ermöglichen, 100 MiB/s oder mehr Durchsatz zu verwenden. Credits sammeln sich kontinuierlich an und werden mit jedem Lese- und Schreibvorgang aufgewendet. Wenn das Dateisystem keine Credits mehr hat, drosselt es Lese- und Schreibvorgänge über den Basisdurchsatz hinaus, was dazu führen kann, dass Aufrufe zeitüberschreitend sind.

> **Note**
>
> Wenn Sie bereitgestellte Nebenläufigkeit, verwenden, kann Ihre Funktion Burst-Credits auch im Leerlauf verbrauchen. Mit bereitgestellter Nebenläufigkeit initialisiert Lambda Instances Ihrer Funktion, bevor sie aufgerufen wird, und recycelt Instanzen alle paar Stunden. Wenn Sie während der Initialisierung Dateien auf einem angehängten Dateisystem verwenden, kann diese Aktivität alle Ihre Burst-Credits verwenden.

Verwenden Sie die `BurstCreditBalance`-Metrik, um den Durchsatz zu überwachen und einen Alarm auszulösen. Es sollte zunehmen, wenn die Nebenläufigkeit Ihrer Funktion niedrig ist und abnimmt, wenn sie hoch ist. Wenn es bei geringer Aktivität immer abnimmt oder nicht genug ansammelt, um den Peak-Datenverkehr abzudecken, müssen Sie möglicherweise die Nebenläufigkeit Ihrer Funktion einschränken oder den bereitgestellten Durchsatzaktivieren.

IOPS

Input/Output Operations pro Sekunde (IOPS) ist ein Maß für die Anzahl der Lese- und Schreibvorgänge, die vom Dateisystem verarbeitet werden. Im Allzweckmodus ist IOPS zugunsten einer niedrigeren Latenz begrenzt, was für die meisten Anwendungen von Vorteil ist.

Verwenden Sie die `PercentIOLimit`-Metrik, um IOPS im Allzweckmodus zu überwachen und einen Alarm einzurichten. Wenn diese Metrik 100 % erreicht, kann es für Ihre Funktion beim Warten auf den Abschluss von Lese- und Schreibvorgängen zu einer Zeitüberschreitung kommen.

Verwenden von Lambda mit Amazon EventBridge Scheduler

Amazon EventBridge Scheduler ist ein Serverless-Scheduler, mit dem Sie Aufgaben von einem zentralen, verwalteten Service aus erstellen, ausführen und verwalten können. Mit EventBridge Scheduler können Sie Zeitpläne mit 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 unverarbeitete Ereignisse festlegen.

Wenn Sie EventBridge Scheduler mit Lambda einrichten, ruft EventBridge Scheduler Ihre Lambda-Funktion asynchron auf. Auf dieser Seite wird erläutert, wie Sie mit dem EventBridge Scheduler eine Lambda-Funktion nach einem Zeitplan aufrufen.

Einrichten der Ausführungsrolle

Wenn Sie einen neuen Zeitplan erstellen, muss EventBridge Scheduler über die Berechtigung verfügen, seine Ziel-API-Operation in Ihrem Namen aufzurufen. Sie erteilen EventBridge Scheduler diese Berechtigungen mithilfe einer Ausführungsrolle . Die Berechtigungsrichtlinie, die Sie der Ausführungsrolle Ihres Zeitplans hinzufügen, definiert die erforderlichen Berechtigungen. Diese Berechtigungen hängen von der Ziel-API ab, die EventBridge Scheduler aufrufen soll.

Wenn Sie die EventBridge Scheduler-Konsole verwenden, um einen Zeitplan zu erstellen, wie im folgenden Verfahren, richtet EventBridge Scheduler automatisch eine Ausführungsrolle basierend auf Ihrem ausgewählten Ziel ein. Wenn Sie einen Zeitplan mit einem der EventBridge Scheduler-SDKs , oder erstellen möchten AWS CLI AWS CloudFormation, müssen Sie über eine vorhandene Ausführungsrolle verfügen, die die Berechtigungen gewährt, die EventBridge Scheduler zum Aufrufen eines Ziels benötigt. Weitere Informationen zum manuellen Einrichten einer Ausführungsrolle für Ihren Zeitplan finden Sie unter Einrichten einer Ausführungsrolle im EventBridge Scheduler-Benutzerhandbuch.

Erstellen eines Zeitplans

So erstellen Sie einen Zeitplan mithilfe der Konsole

1. Öffnen Sie die Amazon- EventBridge Scheduler-Konsole unter https://console.aws.amazon.com/scheduler/home.
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. (Optional) Geben Sie unter Beschreibung eine Beschreibung für Ihren Zeitplan ein. Beispiel: **`My first schedule`**

   c. Wählen Sie für Zeitplangruppe eine Zeitplangruppe aus der Dropdown-Liste aus. Wenn Sie noch keine Gruppe haben, wählen Sie Standard. Um eine Zeitplangruppe zu erstellen, wählen Sie Eigenen Zeitplan erstellen.

   Sie verwenden Zeitplangruppen, um Tags zu Zeitplangruppen hinzuzufügen.

4. • Wählen Sie Ihre Zeitplanoptionen.

Vorkommen	Vorgehensweise	
Einmaliger Zeitplan Ein einmaliger Zeitplan ruft ein Ziel nur einmal zu dem von Ihnen angegebenen Datum und der angegeben en Uhrzeit auf.	Gehen Sie für Datum und Uhrzeit wie folgt vor: • Geben Sie ein gültiges Datum im `YYYY/MM/DD` -Format ein. • Geben Sie einen Zeitstempel im 24-Stunden-Format (`hh:mm`) ein. • Wählen Sie unter Zeitzone die Zeitzone aus.	
Wiederkehrender Zeitplan Ein wiederkehrender Zeitplan ruft ein Ziel mit einer Rate auf, die Sie mit einem cron-Ausdruck	a. Gehen Sie bei Zeitplant yp wie folgt vor: • Um den Zeitplan mithilfe eines Cron-Ausdrucks zu definiere n, wählen Sie Cron-	

Vorkommen	Vorgehensweise	
oder einem Rate-Ausdruck angeben.	basierter Zeitplan und geben Sie den Cron-Ausdruck ein. • Um den Zeitplan mithilfe eines Rate-Ausdrucks zu definieren, wählen Sie Rate-Ausdruck ein. Weitere Informationen zu Cron- und Rate-Ausdrücken finden Sie unter Zeitplantypen auf EventBridge Scheduler im Amazon- EventBridge Scheduler-Benutzerhandbuch. b. Wählen Sie für Flexibles Zeitfenster die Option Aus, um die Option zu deaktivieren, oder wählen Sie eines der vordefinierten Zeitfenster aus. 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. (Optional) Wenn Sie im vorherigen Schritt Wiederkehrender Zeitplan ausgewählt haben, gehen Sie im Abschnitt Zeitrahmen wie folgt vor:

   a. Wählen Sie unter Zeitzone eine Zeitzone aus.

   b. Geben Sie für Startdatum und -uhrzeit ein gültiges Datum im `YYYY/MM/DD`-Format ein und geben Sie dann einen Zeitstempel im 24-Stunden-Format (`hh:mm`) an.

   c. Geben Sie für Enddatum und -uhrzeit ein gültiges Datum im `YYYY/MM/DD`-Format ein und geben Sie dann einen Zeitstempel im 24-Stunden-Format (`hh:mm`) an.

6. Wählen Sie Weiter aus.

7. Wählen Sie auf der Seite Ziel auswählen den AWS API-Vorgang aus, den EventBridge Scheduler aufruft:

   a. Wählen Sie AWS Lambda aufrufen aus.

   b. Wählen Sie im Abschnitt Aufrufen eine Funktion aus oder wählen Sie Neue Lambda-Funktion erstellen.

   c. (Optional) Geben Sie eine JSON-Nutzlast ein. Wenn Sie keine Nutzlast eingeben, verwendet EventBridge Scheduler ein leeres Ereignis, um die Funktion aufzurufen.

8. Wählen Sie Weiter aus.

9. Führen Sie auf der Seite Settings (Einstellungen) die folgenden Schritte aus:

   a. Um den Zeitplan zu aktivieren, schalten Sie unter Zeitplanstatus die Option Zeitplan aktivieren ein.

   b. Um eine Wiederholungsrichtlinie für Ihren Zeitplan zu konfigurieren, gehen Sie unter Wiederholungsrichtlinie und Warteschlange für unzustellbare Nachrichten (DLQ) wie folgt vor:

      - Aktivieren Sie die Option Wiederholen.
      - Geben Sie für Höchstalter des Ereignisses die maximale Stunde(n) und min(s) ein, die EventBridge Scheduler ein unverarbeitetes Ereignis beibehalten muss.
      - Die Höchstdauer beträgt 24 Stunden.
      - Geben Sie für Maximale Anzahl Wiederholungen die maximale Anzahl von Wiederholungen des Zeitplans durch den EventBridge Scheduler ein, wenn das Ziel einen Fehler zurückgibt.

        Der Maximalwert beträgt 185 Wiederholungen.

Wenn bei Wiederholungsrichtlinien ein Zeitplan sein Ziel nicht aufrufen kann, führt EventBridge Scheduler den Zeitplan erneut aus. Falls konfiguriert, müssen Sie die maximale Aufbewahrungszeit und Wiederholungsversuche für den Zeitplan festlegen.

c. Wählen Sie aus, wo EventBridge Scheduler nicht zugestellte Ereignisse speichert.

Option für Warteschlange für unzustellbare Nachrichten (DLQ)	Vorgehensweise
Nicht speichern	Wählen Sie None.
Speichern Sie das Ereignis in derselben AWS-Konto , in der Sie den Zeitplan erstellen	a. Wählen Sie Eine Amazon SQS-Warteschlange in meinem AWS-Konto als DLQ auswählen aus. b. Wählen Sie den Amazon-Ressourcennamen (ARN) der Amazon SQS-Warteschlange.
Speichern Sie das Ereignis in einer anderen AWS-Konto als der, in der Sie den Zeitplan erstellen	a. Wählen Sie Eine Amazon SQS-Warteschlange in anderen AWS-Konten als DLQ angeben aus. b. Geben Sie den Amazon-Ressourcennamen (ARN) der Amazon-SQS-Warteschlange ein.

d. Um einen kundenverwalteten Schlüssel zur Verschlüsselung Ihrer Zieleingabe zu verwenden, wählen Sie unter Verschlüsselung die Option Verschlüsselungseinstellungen anpassen (erweitert).

Wenn Sie diese Option wählen, geben Sie einen vorhandenen CMK-ARN ein oder wählen Sie Erstellen eines AWS KMS key, um zur AWS KMS -Konsole zu navigieren. Weitere Informationen darüber, wie EventBridge Scheduler Ihre Daten im Ruhezustand verschlüsselt, finden Sie unter Verschlüsselung im Ruhezustand im Amazon- EventBridge Scheduler-Benutzerhandbuch.

e. Damit EventBridge Scheduler eine neue Ausführungsrolle für Sie erstellt, wählen Sie Neue Rolle für diesen Zeitplan erstellen aus. Geben Sie dann einen Namen für Rollenname ein. Wenn Sie diese Option wählen, fügt EventBridge Scheduler der Rolle die erforderlichen Berechtigungen für Ihr Vorlagenziel hinzu.

10. Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Zeitplan überprüfen und erstellen die Details Ihres Zeitplans. Wählen Sie in jedem Abschnitt Bearbeiten aus, um zu diesem Schritt zurückzukehren und seine Details zu bearbeiten.
12. Wählen Sie Zeitplan erstellen.

    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.

Um zu bestätigen, dass EventBridge Scheduler die Funktion aufgerufen hat, überprüfen Sie die Amazon- CloudWatch Protokolle der Funktion .

Zugehörige Ressourcen

Weitere Informationen zu EventBridge Scheduler finden Sie hier:

- EventBridge Scheduler-Benutzerhandbuch
- EventBridge Scheduler-API-Referenz
- EventBridge Scheduler-Preise

Verwenden von AWS Lambda mit AWS IoT

AWS IoT bietet eine sichere Kommunikation zwischen über das Internet verbundenen Geräten (z. B. Sensoren) und der AWS Cloud. Auf diese Weise können Sie die Telemetriedaten von mehreren Geräten erfassen, speichern und analysieren.

Sie können AWS IoT-Regeln für Ihre Geräte erstellen, um mit AWS-Services zu interagieren. Die AWS IoT-Regel-Engine bietet eine SQL-basierte Sprache zur Auswahl von Daten aus Nachrichten-Nutzlasten und zum Senden von Daten zu anderen Services, z. B. Amazon S3, Amazon DynamoDB und AWS Lambda. Sie definieren eine Regel zum Aufrufen einer Lambda-Funktion, wenn Sie einen anderen AWS-Service oder den Service eines Drittanbieters aufrufen möchten.

Wenn eine eingehende IoT-Nachricht die Regel auslöst, ruft AWS IoT Ihre Lambda-Funktion asynchron auf und übergibt Daten aus der IoT-Nachricht an die Funktion.

Das folgende Beispiel zeigt einen Feuchtigkeitsablesung von einem Gewächshaussensor. Die Werte row und pos bestimmen die Position des Sensors. Dieses Beispielereignis basiert auf dem Gewächshaustyp in den AWS IoT-Regel-Tutorials.

Example AWS IoT-Nachrichtenereignis

```
{
    "row" : "10",
    "pos" : "23",
    "moisture" : "75"
}
```

Bei asynchronem Aufruf stellt Lambda die Nachricht in die Warteschlange und wiederholt den Vorgang, wenn Ihre Funktion einen Fehler zurückgibt. Konfigurieren Sie Ihre Funktion mit einem Ziel, um Ereignisse beizubehalten, die Ihre Funktion nicht verarbeiten konnte.

Sie müssen die Berechtigung für den AWS IoT-Service erteilen, um Ihre Lambda-Funktion aufzurufen. Sie können den Befehl `add-permission` verwenden, um der ressourcenbasierten Richtlinie Ihrer Funktion eine Berechtigungsanweisung hinzuzufügen.

```
aws lambda add-permission --function-name my-function \
--statement-id iot-events --action "lambda:InvokeFunction" --principal
 iot.amazonaws.com
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Statement": "{\"Sid\":\"iot-events\",\"Effect\":\"Allow\",\"Principal\":
{\"Service\":\"iot.amazonaws.com\"},\"Action\":\"lambda:InvokeFunction\",\"Resource\":
\"arn:aws:lambda:us-east-1:123456789012:function:my-function\"}"
}
```

Weitere Informationen zur Verwendung von Lambda mit AWS IoT finden Sie unter Erstellen einer AWS Lambda-Regel.

Verwenden von AWS Lambda mit Amazon Data Firehose

Amazon Data Firehose erfasst, transformiert und lädt Streaming-Daten in Downstream-Services wie Managed Service für Apache Flink oder Amazon S3. Sie können Lambda-Funktionen schreiben, um eine zusätzliche, benutzerdefinierte Verarbeitung der Daten vor der nachgeschalteten Weiterleitung anzufordern.

Example Amazon-Data-Firehose-Nachrichtenereignis


```
{
  "invocationId": "invoked123",
  "deliveryStreamArn": "aws:lambda:events",
  "region": "us-west-2",
  "records": [
    {
      "data": "SGVsbG8gV29ybGQ=",
      "recordId": "record1",
      "approximateArrivalTimestamp": 1510772160000,
      "kinesisRecordMetadata": {
        "shardId": "shardId-000000000000",
        "partitionKey": "4d1ad2b9-24f8-4b9d-a088-76e9947c317a",
        "approximateArrivalTimestamp": "2012-04-23T18:25:43.511Z",
        "sequenceNumber": "49546986683135544286507457936321625675700192471156785154",
        "subsequenceNumber": ""
      }
    },
    {
      "data": "SGVsbG8gV29ybGQ=",
      "recordId": "record2",
      "approximateArrivalTimestamp": 151077216000,
      "kinesisRecordMetadata": {
        "shardId": "shardId-000000000001",
        "partitionKey": "4d1ad2b9-24f8-4b9d-a088-76e9947c318a",
        "approximateArrivalTimestamp": "2012-04-23T19:25:43.511Z",
        "sequenceNumber": "49546986683135544286507457936321625675700192471156785155",
        "subsequenceNumber": ""
      }
    }
  ]
}
```

Weitere Informationen finden Sie unter Amazon-Data-Firehose-Datentransformation im Firehose-Entwicklerhandbuch.

Verwenden von AWS Lambda mit Amazon Lex

Sie können mit Amazon Lex einen Conversation-Bot in Ihre Anwendung integrieren. Der Amazon-Lex-Bot bietet eine Konversationsoberfläche mit Ihren Benutzern. Amazon Lex bietet eine vorgefertigte Integration mit Lambda, mit der Sie eine Lambda-Funktion mit Ihrem Amazon-Lex-Bot verwenden können.

Wenn Sie einen Amazon-Lex-Bot konfigurieren, können Sie eine Lambda-Funktion angeben, um die Validierung, die Erfüllung oder beides durchzuführen. Zur Validierung ruft Amazon Lex die Lambda-Funktion nach jeder Antwort des Benutzers auf. Die Lambda-Funktion kann die Antwort validieren und ggf. korrigierende Rückmeldungen an den Benutzer liefern. Zur Erfüllung ruft Amazon Lex die Lambda-Funktion auf, um die Benutzeranforderung zu erfüllen, nachdem der Bot erfolgreich alle erforderlichen Informationen sammelt und eine Bestätigung vom Benutzer erhält.

Sie können die Parallelität Ihrer Lambda-Funktion verwalten, um die maximale Anzahl gleichzeitiger Bot-Unterhaltungen zu steuern, die Sie bedienen. Die Amazon-Lex-API gibt einen HTTP 429-Statuscode (Too Many Requests) zurück, wenn die Funktion maximale Parallelität aufweist.

Die API gibt einen HTTP 424-Statuscode (Dependency Failed Exception) zurück, wenn die Lambda-Funktion eine Ausnahme auswirft.

Der Amazon-Lex-Bot ruft Ihre Lambda-Funktion synchron auf. Der Ereignisparameter enthält Informationen über den Bot und den Wert jedes Slots im Dialog. Definitionen der Ereignis- und Antwortfelder finden Sie unter Lambda-Ereignis- und Antwortformat im Amazon-Lex-Entwicklerhandbuch. Der `invocationSource` Parameter im Amazon Lex-Nachrichtenereignis gibt an, ob die Lambda-Funktion die Eingaben validieren (DialogCodeHook) oder die Absicht erfüllen (FulfillmentCodeHook).

Ein Beispiel-Tutorial, das zeigt, wie Lambda mit Amazon Lex verwendet wird, finden Sie unter Übung 1: Erstellen eines Amazon-Lex-Bots mithilfe eines Plans im Amazon-Lex-Entwicklerhandbuch.

Rollen und Berechtigungen

Sie müssen eine serviceverknüpfte Rolle als Ausführungsrolle der Funktion verknüpfen. Amazon Lex definiert die serviceverknüpfte Rolle mit vordefinierten Berechtigungen. Wenn Sie einen Amazon-Lex-Bot mit der Konsole erstellen, wird die serviceverknüpfte Rolle automatisch erstellt. Verwenden Sie den AWS CLI-Befehl, um eine serviceverknüpfte Rolle mit der `create-service-linked-role` zu erstellen.

```
aws iam create-service-linked-role --aws-service-name lex.amazonaws.com
```

Dieser Befehl erstellt die folgende Rolle.

```
{
  "Role": {
      "AssumeRolePolicyDocument": {
          "Version": "2012-10-17",
          "Statement": [
              {
                  "Action": "sts:AssumeRole",
                  "Effect": "Allow",
                  "Principal": {
                      "Service": "lex.amazonaws.com"
                  }
              }
          ]
      },
      "RoleName": "AWSServiceRoleForLexBots",
      "Path": "/aws-service-role/lex.amazonaws.com/",
      "Arn": "arn:aws:iam::account-id:role/aws-service-role/lex.amazonaws.com/
AWSServiceRoleForLexBots"
}
```

Wenn Ihre Lambda-Funktion andere AWS-Services verwendet, müssen Sie der serviceverknüpften Rolle die entsprechenden Berechtigungen hinzufügen.

Sie verwenden eine ressourcenbasierte Berechtigungsrichtlinie, um dem Amazon Lex-Bot das Aufrufen Ihrer Lambda-Funktion zu erlauben. Wenn Sie die Amazon-Lex-Konsole verwenden, wird die Berechtigungsrichtlinie automatisch erstellt. Verwenden Sie in der AWS CLI den Lambda-Befehl `add-permission`, um die Berechtigung festzulegen.

Führen Sie für Amazon Lex V2 den folgenden Befehl aus. Ersetzen Sie im Quell-ARN `us-east-1` durch das AWS-Region, in dem sich Ihr Amazon Lex-Bot befindet, und verwenden Sie Ihre eigene AWS-Konto-Nummer und Ihren Bot-Alias.

```
aws lambda add-permission \
    --function-name LexCodeHook \
    --statement-id LexInvoke-MyBot \
```

```
    --action lambda:InvokeFunction \
    --principal lex.amazonaws.com \
    --source-arn "arn:aws:lex:us-east-1:123456789012:bot-alias/MYBOT/MYBOTALIAS"
```

Sie können Amazon Lex V1 auch verwenden, um eine Lambda-Funktion aufzurufen. Führen Sie für Amazon Lex V1 den folgenden Befehl aus. Ersetzen Sie im Quell-ARN `us-east-1` durch das AWS-Region, in dem sich Ihre Amazon Lex-Absicht befindet, und verwenden Sie Ihre eigene AWS-Konto-Nummer und Ihren Absichtsnamen.

```
aws lambda add-permission \
    --function-name LexCodeHook \
    --statement-id LexInvoke-MyIntent \
    --action lambda:InvokeFunction \
    --principal lex.amazonaws.com \
    --source-arn "arn:aws:lex:us-east-1:123456789012 ID:intent:MYINTENT:*"
```

Beachten Sie, dass Amazon Lex V1 nicht mehr unterstützt wird. Wir empfehlen die Verwendung von Amazon Lex V2.

Verwendung AWS Lambda mit Amazon RDS

Sie können eine Lambda-Funktion direkt und über einen Amazon-RDS-Proxy mit einer Amazon Relational Database Service (Amazon RDS)-Datenbank verbinden. Direkte Verbindungen sind in einfachen Szenarien nützlich, und Proxys werden für die Produktion empfohlen. Ein Datenbank-Proxy verwaltet einen Pool gemeinsam genutzter Datenbankverbindungen, sodass Ihre Funktion eine hohe Gleichkeitigkeitsstufe erreichen kann, ohne dass die Datenbankverbindungen erschöpft werden.

Wir empfehlen die Verwendung von Amazon-RDS-Proxy für Lambda-Funktionen, die häufig kurze Datenbankverbindungen herstellen oder eine große Anzahl von Datenbankverbindungen öffnen und schließen.

Konfigurieren Ihrer Funktion

In der Lambda-Konsole können Sie Amazon RDS-Datenbank-Instances und Proxyressourcen bereitstellen und konfigurieren. Weitere Informationen finden Sie unter RDS-Datenbanken auf der Registerkarte Konfiguration. Alternativ können Sie auch Verbindungen zu Lambda-Funktionen in der Amazon-RDS-Konsole erstellen und konfigurieren.

- Um eine Verbindung zu einer Datenbank herzustellen, muss sich die Funktion in derselben Amazon VPC befinden, in der Ihre Datenbank ausgeführt wird.
- Sie können Amazon-RDS-Datenbanken mit MySQL-, MariaDB-, PostgreSQL- oder Microsoft-SQL-Server-Engines verwenden.
- Sie können Aurora-DB-Cluster auch mit MySQL- oder PostgreSQL-Engines verwenden.
- Sie müssen ein Secrets-Manager-Geheimnis für die Authentifizierung der Datenbank angeben.
- Eine IAM-Rolle muss die Berechtigung zur Verwendung des Geheimnisses sowie eine Vertrauensrichtlinie bereitstellen, mit der Amazon RDS die Rolle übernehmen kann.
- Der IAM-Principal, der die Konsole verwendet, um die Amazon RDS-Ressource zu konfigurieren und sie mit Ihrer Funktion zu verbinden, muss über die folgenden Berechtigungen verfügen:

> **Note**
>
> Sie benötigen die Amazon RDS-Proxy-Berechtigungen nur, wenn Sie einen Amazon RDS-Proxy für die Verwaltung eines Pools Ihrer Datenbankverbindungen konfigurieren.

Example Berechtigungsrichtlinie

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:CreateNetworkInterface",
        "ec2:DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds-db:connect",
        "rds:CreateDBProxy",
        "rds:CreateDBInstance",
        "rds:CreateDBSubnetGroup",
        "rds:DescribeDBClusters",
        "rds:DescribeDBInstances",
        "rds:DescribeDBSubnetGroups",
        "rds:DescribeDBProxies",
        "rds:DescribeDBProxyTargets",
        "rds:DescribeDBProxyTargetGroups",
        "rds:RegisterDBProxyTargets",
        "rds:ModifyDBInstance",
        "rds:ModifyDBProxy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
        "lambda:CreateFunction",
        "lambda:ListFunctions",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:AttachPolicy",
        "iam:CreateRole",
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds",
        "secretsmanager:CreateSecret"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon RDS berechnet einen Stundensatz für Proxys, der auf der Größe der Datenbank-Instance basiert. Weitere Informationen finden Sie unter RDS-Proxy-Preise. Weitere Informationen zu Proxy-Verbindungen finden Sie unter Verwendung von Amazon-RDS-Proxy im Amazon-RDS-Benutzerhandbuch.

Einrichtung von Lambda und Amazon RDS

Sowohl die Lambda- als auch die Amazon RDS-Konsole unterstützen Sie bei der automatischen Konfiguration einiger der erforderlichen Ressourcen, um eine Verbindung zwischen Lambda und Amazon RDS herzustellen.

Stellen Sie in einer Lambda-Funktion eine Connect zu einer Amazon RDS-Datenbank her

Das folgende Codebeispiel zeigt, wie eine Lambda-Funktion implementiert wird, die eine Verbindung zu einer Amazon RDS-Datenbank herstellt. Die Funktion stellt eine einfache Datenbankanfrage und gibt das Ergebnis zurück.

Go

SDK für Go V2

Note

Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Mit Go eine Verbindung zu einer Amazon RDS-Datenbank in einer Lambda-Funktion herstellen.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Golang v2 code here.
*/

package main

import (
 "context"
 "database/sql"
 "encoding/json"
 "fmt"
```

```
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
 _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
 Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {

 var dbName string = "DatabaseName"
 var dbUser string = "DatabaseUser"
 var dbHost string = "mysqldb.123456789012.us-east-1.rds.amazonaws.com"
 var dbPort int = 3306
 var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
 var region string = "us-east-1"

 cfg, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  panic("configuration error: " + err.Error())
 }

 authenticationToken, err := auth.BuildAuthToken(
  context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
 if err != nil {
  panic("failed to create authentication token: " + err.Error())
 }

 dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
  dbUser, authenticationToken, dbEndpoint, dbName,
 )

 db, err := sql.Open("mysql", dsn)
 if err != nil {
  panic(err)
 }

 defer db.Close()

 var sum int
 err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
```

```
 if err != nil {
  panic(err)
 }
 s := fmt.Sprint(sum)
 message := fmt.Sprintf("The selected sum is: %s", s)

 messageBytes, err := json.Marshal(message)
 if err != nil {
  return nil, err
 }

 messageString := string(messageBytes)
 return map[string]interface{}{
  "statusCode": 200,
  "headers":    map[string]string{"Content-Type": "application/json"},
  "body":       messageString,
 }, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

JavaScript

SDK für JavaScript (v2)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Herstellen einer Verbindung zu einer Amazon RDS-Datenbank in einer Lambda-Funktion mithilfe von Javascript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Node.js code here.
```

```
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {

    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;

}
```

```
export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
};
```

Verarbeiten von Amazon-RDS-Ereignisbenachrichtigungen

Sie können Lambda verwenden, um Ereignisbenachrichtigungen aus einer Amazon-RDS-Datenbank zu verarbeiten. Amazon RDS sendet Benachrichtigungen an ein Amazon-Simple-Notification-Service-(Amazon-SNS)-Thema, das Sie so konfigurieren können, dass eine Lambda-Funktion aufgerufen wird. Amazon SNS wickelt die Nachricht von Amazon RDS in ein eigenes Ereignisdokument und sendet sie an Ihre Funktion.

Weitere Informationen zum Konfigurieren einer Amazon-RDS-Datenbank zum Senden von Benachrichtigungen finden Sie unter Verwendung von Amazon-RDS-Ereignisbenachrichtigungen.

Example Amazon-RDS-Nachricht in einem Amazon-SNS-Ereignis

```
{
        "Records": [
          {
            "EventVersion": "1.0",
            "EventSubscriptionArn": "arn:aws:sns:us-east-2:123456789012:rds-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
            "EventSource": "aws:sns",
            "Sns": {
              "SignatureVersion": "1",
              "Timestamp": "2023-01-02T12:45:07.000Z",
              "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi
+tE/1+82j...65r==",
              "SigningCertUrl": "https://sns.us-east-2.amazonaws.com/
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",
              "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
              "Message": "{\"Event Source\":\"db-instance\",\"Event Time\":\"2023-01-02
 12:45:06.000\",\"Identifier Link\":\"https://console.aws.amazon.com/rds/home?
```

```
region=eu-west-1#dbinstance:id=dbinstanceid\",\"Source ID\":\"dbinstanceid\",\"Event ID
\":\"http://docs.amazonwebservices.com/AmazonRDS/latest/UserGuide/USER_Events.html#RDS-
EVENT-0002\",\"Event Message\":\"Finished DB Instance backup\"}",
              "MessageAttributes": {},
              "Type": "Notification",
              "UnsubscribeUrl": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&amp;SubscriptionArn=arn:aws:sns:us-east-2:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
              "TopicArn":"arn:aws:sns:us-east-2:123456789012:sns-lambda",
              "Subject": "RDS Notification Message"
            }
          }
        ]
      }
```

Tutorial zu Lambda und Amazon RDS

- Verwendung einer Lambda-Funktion für den Zugriff auf eine Amazon-RDS-Datenbank – Im Benutzerhandbuch zu Amazon RDS wird beschrieben, wie Sie eine Lambda-Funktion verwenden, um Daten über einen Amazon-RDS-Proxy in eine Amazon-RDS-Datenbank zu schreiben. Ihre Lambda-Funktion liest Datensätze aus einer Amazon-SQS-Warteschlange und schreibt jedes Mal, wenn eine Nachricht hinzugefügt wird, neue Elemente in eine Tabelle in Ihrer Datenbank.

Verarbeiten Sie Amazon S3 S3-Ereignisbenachrichtigungen mit Lambda

Sie können Lambda verwenden, um Ereignisbenachrichtigungen von Amazon Simple Storage Service zu verarbeiten. Amazon S3 kann ein Ereignis an eine Lambda-Funktion senden, wenn ein Objekt erstellt oder gelöscht wird. Sie konfigurieren Benachrichtigungseinstellungen für einen Bucket und erteilen die Amazon-S3-Berechtigung zum Aufrufen einer Funktion in der ressourcenbasierten Berechtigungsrichtlinie der Funktion.

> **Warning**
>
> Wenn Ihre Lambda-Funktion den gleichen Bucket verwendet, der sie auslöst, könnte dies dazu führen, dass die Funktion in einer Schleife ausgeführt wird. Wenn der Bucket z. B. eine Funktion immer dann auslöst, wenn ein Objekt hochgeladen wird, und die Funktion ein Objekt in den Bucket hochlädt, löst die Funktion sich indirekt selbst aus. Um dies zu vermeiden, verwenden Sie zwei Buckets oder konfigurieren Sie den Auslöser so, dass er nur für einen Präfix gilt, der für eingehende Objekte verwendet wird.

Amazon S3 ruft Ihre Funktion asynchron mit einem Ereignis auf, das Details über das Objekt enthält. Das folgende Beispiel zeigt ein Ereignis, das Amazon S3 gesendet hat, als ein Bereitstellungspaket in Amazon S3 hochgeladen wurde.

Example Amazon-S3-Benachrichtigungsereignis

```
{
  "Records": [
    {
      "eventVersion": "2.1",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-2",
      "eventTime": "2019-09-03T19:37:27.192Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "AWS:AIDAINPONIXQXHT3IKHL2"
      },
      "requestParameters": {
        "sourceIPAddress": "205.255.255.255"
      },
```

```
      "responseElements": {
        "x-amz-request-id": "D82B88E5F771F645",
        "x-amz-id-2":
  "vlR7PnpV2Ce81l0PRw6jlUpck7Jo5ZsQjryTjKlc5aLWGVHPZLj5NeC6qMa0emYBDXOo6QBU0Wo="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "828aa6fc-f7b5-4305-8584-487c791949c1",
        "bucket": {
          "name": "DOC-EXAMPLE-BUCKET",
          "ownerIdentity": {
            "principalId": "A3I5XTEXAMAI3E"
          },
          "arn": "arn:aws:s3:::lambda-artifacts-deafc19498e3f2df"
        },
        "object": {
          "key": "b21b84d653bb07b05b1e6b33684dc11b",
          "size": 1305107,
          "eTag": "b21b84d653bb07b05b1e6b33684dc11b",
          "sequencer": "0C0F6F405D6ED209E1"
        }
      }
    }
  ]
}
```

Um Ihre Funktion aufzurufen, benötigt Amazon S3 die Berechtigung von der ressourcenbasierten Richtlinie der Funktion. Wenn Sie einen Amazon-S3-Auslöser in der Lambda-Konsole konfigurieren, ändert die Konsole die ressourcenbasierte Richtlinie so, dass Amazon S3 die Funktion aufrufen kann, wenn der Bucket-Name und die Konto-ID übereinstimmen. Wenn Sie die Benachrichtigung in Amazon S3 konfigurieren, verwenden Sie die Lambda-API, um die Richtlinie zu aktualisieren. Sie können auch die Lambda-API verwenden, um einem anderen Konto Berechtigungen zu erteilen oder die Berechtigung auf einen bestimmten Alias zu beschränken.

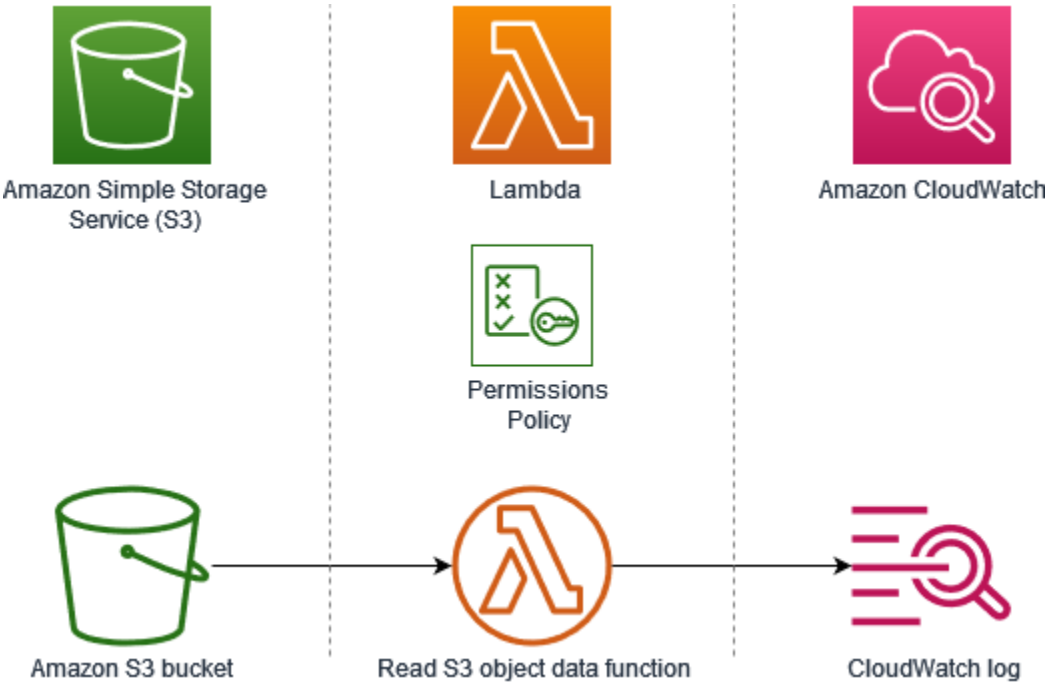
Wenn Ihre Funktion das AWS SDK zur Verwaltung von Amazon S3 S3-Ressourcen verwendet, benötigt sie in ihrer Ausführungsrolle auch Amazon S3 S3-Berechtigungen.

Themen

- Tutorial: Verwenden eines Amazon-S3-Auslösers zum Aufrufen einer Lambda-Funktion
- Tutorial: Verwenden eines Amazon-S3-Auslösers zum Erstellen von Miniaturbildern

Tutorial: Verwenden eines Amazon-S3-Auslösers zum Aufrufen einer Lambda-Funktion

In diesem Tutorial verwenden Sie die Konsole, um eine Lambda-Funktion zu erstellen und einen Auslöser für einen Amazon-Simple-Storage-Service-Bucket (Amazon-S3-Bucket) zu konfigurieren. Jedes Mal, wenn Sie Ihrem Amazon S3 S3-Bucket ein Objekt hinzufügen, wird Ihre Funktion ausgeführt und der Objekttyp wird in Amazon CloudWatch Logs ausgegeben.



Dieses Tutorial zeigt, wie Sie:

1. Erstellen Sie einen Amazon-S3-Bucket.
2. Erstellen Sie eine Lambda-Funktion, die den Objekttyp von Objekten in einem Amazon-S3-Bucket ausgibt.
3. Konfigurieren Sie einen Lambda-Auslöser, der Ihre Funktion aufruft, wenn Objekte in Ihren Bucket hochgeladen werden.
4. Testen Sie Ihre Funktion, zuerst mit einem Dummy-Ereignis und dann mit dem Auslöser.

Durch das Ausführen dieser Schritte erfahren Sie, wie Sie eine Lambda-Funktion so konfigurieren, dass sie ausgeführt wird, wenn Objekte einem Amazon-S3-Bucket hinzugefügt oder daraus gelöscht werden. Sie können dieses Tutorial abschließen, indem Sie nur die AWS Management Console verwenden.

Voraussetzungen

Melde dich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

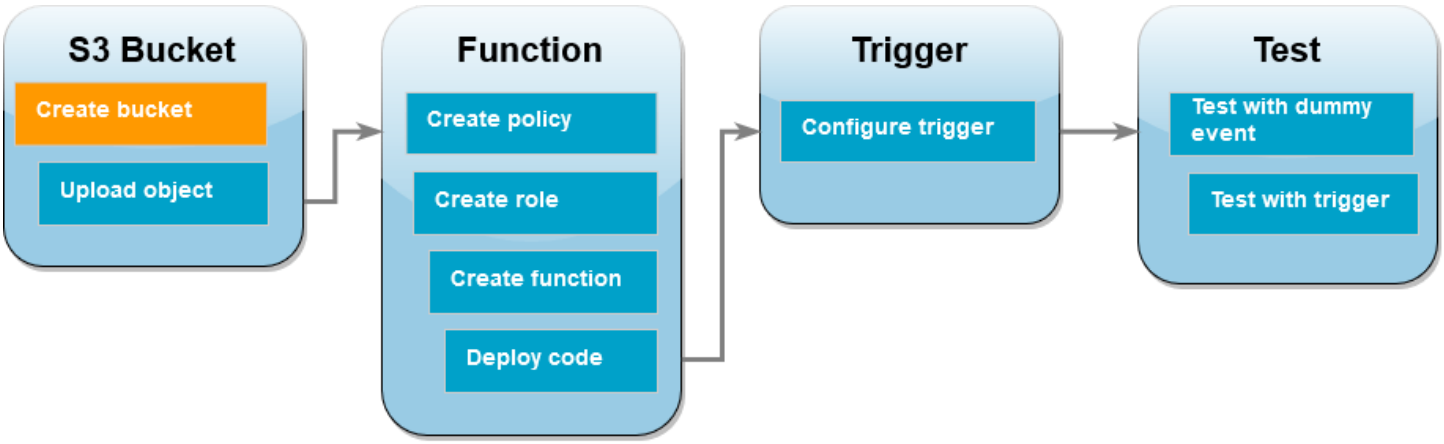
Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Erstellen eines Amazon-S3-Buckets



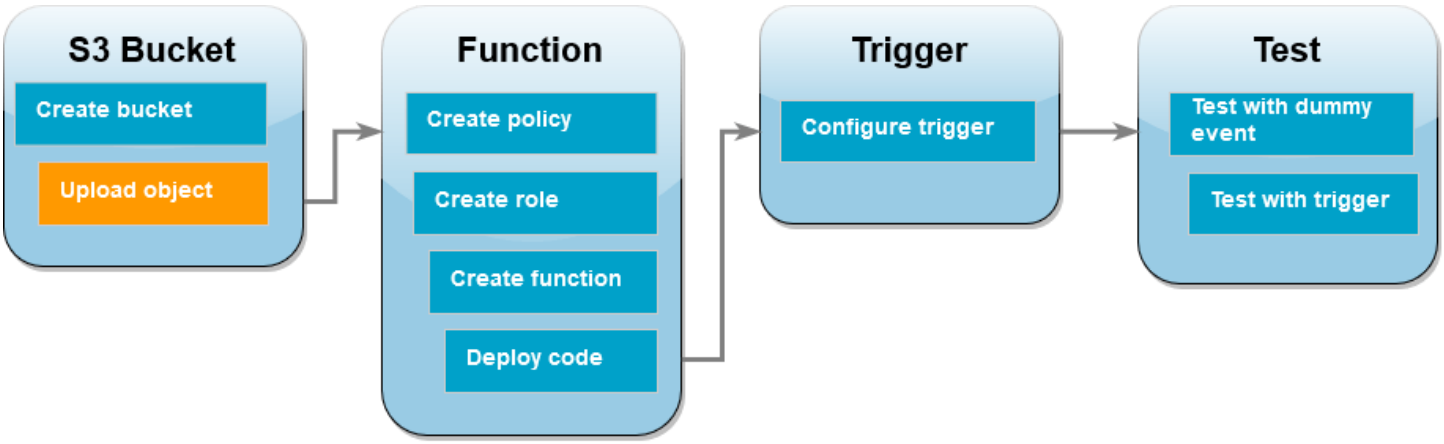
So erstellen Sie einen Amazon-S3-Bucket

1. Öffnen Sie die Amazon-S3-Konsole und wählen Sie die Seite Buckets aus.
2. Wählen Sie Bucket erstellen aus.
3. Führen Sie unter Allgemeine Konfiguration die folgenden Schritte aus:

   a. Geben Sie für den Bucket-Namen einen global eindeutigen Namen ein, der den Regeln für die Bucket-Benennung von Amazon S3 entspricht. Bucket-Namen dürfen nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen.

   b. Wählen Sie unter AWS -Region eine Region aus. Später im Tutorial müssen Sie eine Lambda-Funktion in derselben Region erstellen.
4. Belassen Sie alle anderen Optionen auf ihren Standardwerten und wählen Sie Bucket erstellen aus.

Hochladen eines Testobjekts in Ihren Bucket

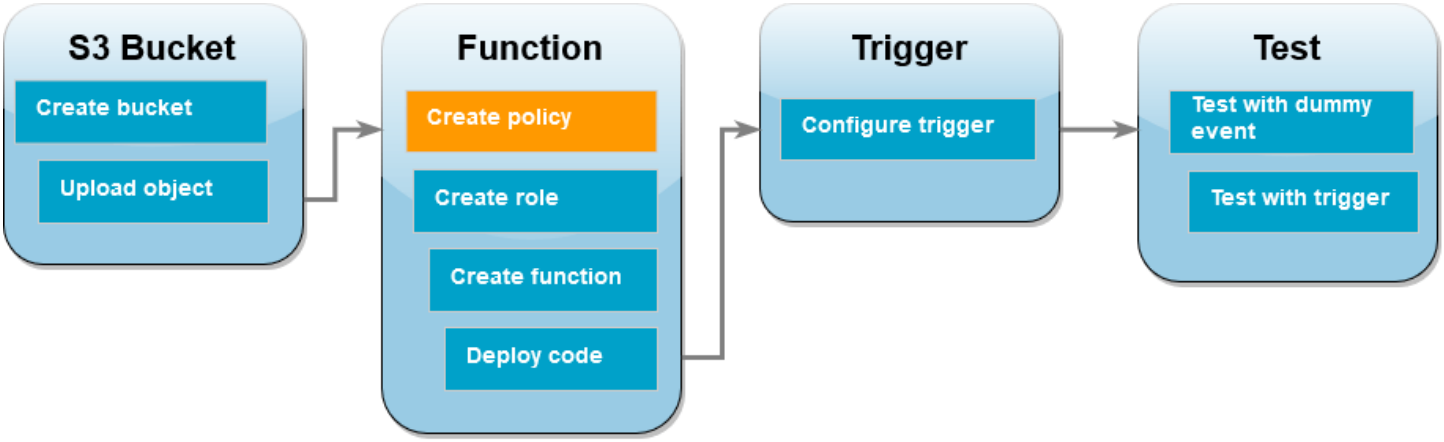


Hochladen eines Testobjekts

1. Öffnen Sie die Buckets-Seite der Amazon-S3-Konsole und wählen Sie den Bucket aus, den Sie im vorherigen Schritt erstellt haben.
2. Klicken Sie auf Hochladen.
3. Wählen Sie Dateien hinzufügen und wählen Sie das Objekt aus, das Sie hochladen möchten. Sie können eine beliebige Datei auswählen (z. B. `HappyFace.jpg`).
4. Wählen Sie Öffnen und anschließend Hochladen aus.

Später im Tutorial testen Sie Ihre Lambda-Funktion mit diesem Objekt.

Erstellen einer Berechtigungsrichtlinie



Erstellen Sie eine Berechtigungsrichtlinie, die es Lambda ermöglicht, Objekte aus einem Amazon S3 S3-Bucket abzurufen und in Amazon CloudWatch Logs zu schreiben.

So erstellen Sie die Richtlinie

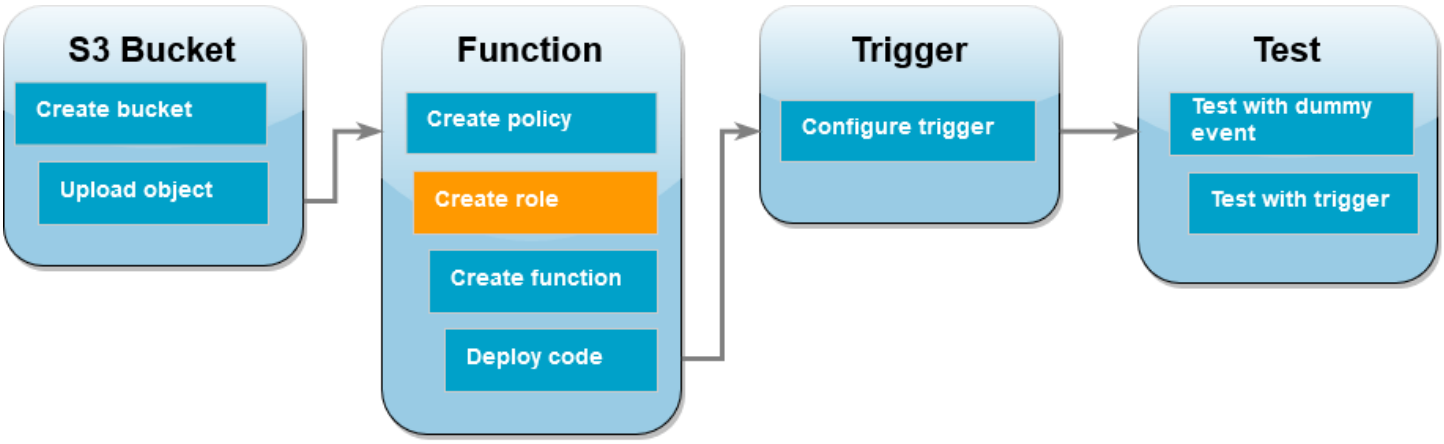
1. Öffnen Sie die Seite Richtlinien in der IAM-Konsole.
2. Wählen Sie Richtlinie erstellen aus.
3. Wählen Sie die Registerkarte JSON aus und kopieren Sie dann die folgende benutzerdefinierte JSON-Richtlinie in den JSON-Editor.

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

```
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

4. Wählen Sie Next: Tags (Weiter: Tags) aus.
5. Klicken Sie auf Weiter: Prüfen.
6. Geben Sie unter Review policy (Richtlinie prüfen) für den Richtlinien-Namen **`s3-trigger-tutorial`** ein.
7. Wählen Sie Richtlinie erstellen aus.

Erstellen einer Ausführungsrolle

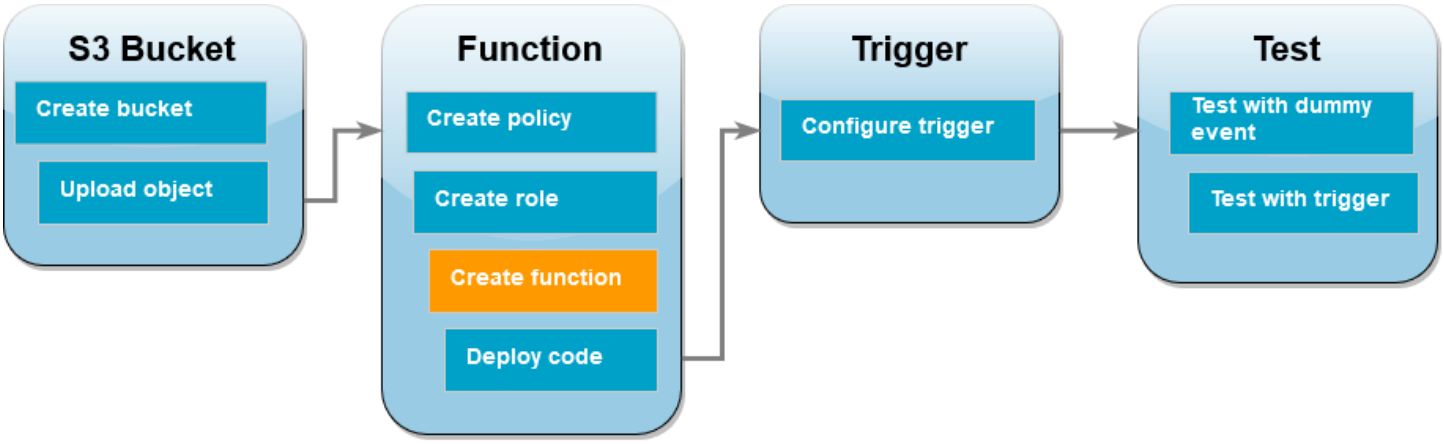


Eine Ausführungsrolle ist eine AWS Identity and Access Management (IAM-) Rolle, die einer Lambda-Funktion die Berechtigung zum Zugriff auf AWS Dienste und Ressourcen gewährt. Erstellen Sie in diesem Schritt eine Ausführungsrolle mithilfe der Berechtigungsrichtlinie, die Sie im vorherigen Schritt erstellt haben.

So erstellen Sie eine Ausführungsrolle und fügen Ihre benutzerdefinierte Berechtigungsrichtlinie hinzu

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie als Typ der vertrauenswürdigen Entität AWS -Service und dann als Anwendungsfall Lambda aus.
4. Wählen Sie Weiter aus.
5. Geben Sie im Feld für die Richtliniensuche **`s3-trigger-tutorial`** ein.
6. Wählen Sie in den Suchergebnissen die von Ihnen erstellte Richtlinie (`s3-trigger-tutorial`) und dann die Option Next (Weiter) aus.
7. Geben Sie unter Role details (Rollendetails) für den Role name (Rollennamen) **`lambda-s3-trigger-role`** ein und wählen Sie dann Create role (Rolle erstellen) aus.

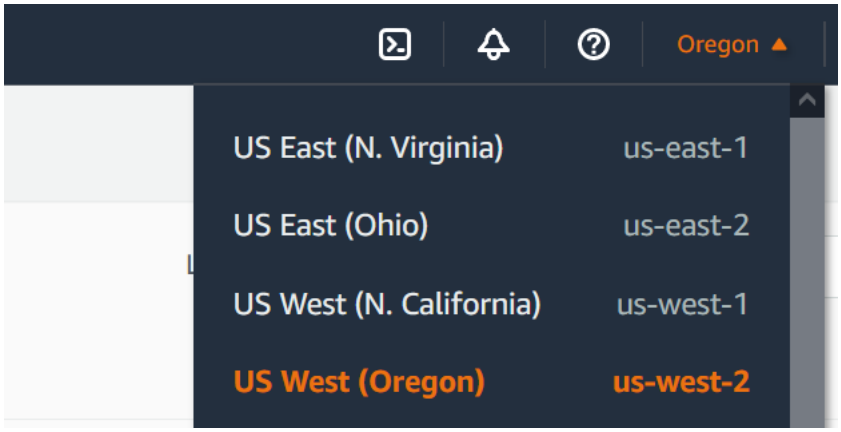
So erstellen Sie die Lambda-Funktion:



Erstellen Sie mit der Python 3.12-Laufzeit eine Lambda-Funktion in der Konsole.

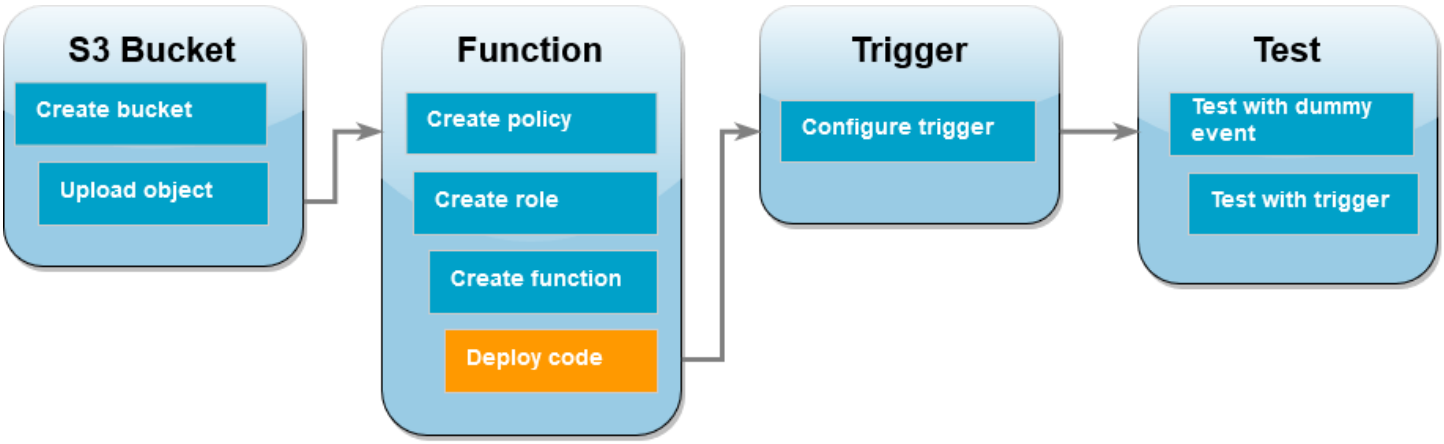
So erstellen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Stellen Sie sicher, dass Sie in demselben Modus arbeiten, in dem AWS-Region Sie Ihren Amazon S3 S3-Bucket erstellt haben. Sie können Ihre Region mithilfe der Dropdown-Liste oben auf dem Bildschirm ändern.



3. Wählen Sie Funktion erstellen.
4. Wählen Sie Ohne Vorgabe erstellen aus.
5. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie unter Funktionsname `s3-trigger-tutorial` ein.
   b. Wählen Sie für Runtime Python 3.12.
   c. Wählen Sie für Architektur x86_64 aus.
6. Gehen Sie auf der Registerkarte Standard-Ausführungsrolle ändern wie folgt vor:
   a. Erweitern Sie die Registerkarte und wählen Sie dann Verwenden einer vorhandenen Rolle aus.
   b. Wählen Sie die zuvor erstellte `lambda-s3-trigger-role` aus.
7. Wählen Sie Funktion erstellen.

Bereitstellen des Funktionscodes



Dieses Tutorial verwendet die Python 3.12-Laufzeit, aber wir haben auch Beispielcodedateien für andere Laufzeiten bereitgestellt. Sie können die Registerkarte im folgenden Feld auswählen, um den Code für die gewünschte Laufzeit anzusehen.

Die Lambda-Funktion ruft den Schlüsselnamen des hochgeladenen Objekts und den Namen des Buckets aus dem `event` Parameter ab, den sie von Amazon S3 erhält. Die Funktion verwendet dann die Methode get_object von, AWS SDK for Python (Boto3) um die Metadaten des Objekts abzurufen, einschließlich des Inhaltstyps (MIME-Typ) des hochgeladenen Objekts.

So stellen Sie den Funktionscode bereit

1. Wählen Sie im folgenden Feld die Registerkarte Python und kopieren Sie den Code.

   .NET

   AWS SDK for .NET

   > **Note**
   >
   > Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

   Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von .NET

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be
 converted into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJson

namespace S3Integration
{
```

```
   public class Function
   {
       private static AmazonS3Client _s3Client;
       public Function() : this(null)
       {
       }

       internal Function(AmazonS3Client s3Client)
       {
           _s3Client = s3Client ?? new AmazonS3Client();
       }

       public async Task<string> Handler(S3Event evt, ILambdaContext
context)
       {
           try
           {
               if (evt.Records.Count <= 0)
               {
                   context.Logger.LogLine("Empty S3 Event received");
                   return string.Empty;
               }

               var bucket = evt.Records[0].S3.Bucket.Name;
               var key =
HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

               context.Logger.LogLine($"Request is for {bucket} and {key}");

               var objectResult = await _s3Client.GetObjectAsync(bucket,
key);

               context.Logger.LogLine($"Returning {objectResult.Key}");

               return objectResult.Key;
           }
           catch (Exception e)
           {
               context.Logger.LogLine($"Error processing request -
{e.Message}");

               return string.Empty;
           }
       }
```

```
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Go

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)

func handler(ctx context.Context, s3Event events.S3Event) error {
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Printf("failed to load default config: %s", err)
  return err
 }
 s3Client := s3.NewFromConfig(sdkConfig)

 for _, record := range s3Event.Records {
  bucket := record.S3.Bucket.Name
  key := record.S3.Object.URLDecodedKey
  headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
```

```
   Bucket: &bucket,
   Key:    &key,
  })
  if err != nil {
   log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
   return err
  }
  log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
 *headOutput.ContentType)
 }

 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Java

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
```

```
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
 com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNo

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger =
 LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
          S3EventNotificationRecord record = s3event.getRecords().get(0);
          String srcBucket = record.getS3().getBucket().getName();
          String srcKey = record.getS3().getObject().getUrlDecodedKey();

          S3Client s3Client = S3Client.builder().build();
          HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
 srcKey);

          logger.info("Successfully retrieved " + srcBucket + "/" + srcKey +
 " of type " + headObject.contentType());

          return "Ok";
        } catch (Exception e) {
          throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String
 bucket, String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
                .bucket(bucket)
                .key(key)
                .build();
        return s3Client.headObject(headObjectRequest);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines S3-Ereignisses mit Lambda unter Verwendung JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

exports.handler = async (event, context) => {

    // Get the object from the event and show its content type
    const bucket = event.Records[0].s3.bucket.name;
    const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\
+/g, ' '));

    try {
        const { ContentType } = await client.send(new HeadObjectCommand({
            Bucket: bucket,
            Key: key,
        }));

        console.log('CONTENT TYPE:', ContentType);
        return ContentType;

    } catch (err) {
        console.log(err);
        const message = `Error getting object ${key} from bucket ${bucket}.
 Make sure they exist and your bucket is in the same region as this
 function.`;
        console.log(message);
        throw new Error(message);
```

```
    }
};
```

Konsumieren eines S3-Ereignisses mit Lambda unter Verwendung TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> =>
 {
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/
g, ' '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make
 sure they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein S3-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';


class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
```

```
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());

            try {
                $fileSize = urldecode($record->getObject()->getSize());
                echo "File Size: " . $fileSize . "\n";
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                echo $e->getMessage() . "\n";
                echo 'Error getting object ' . $key . ' from bucket ' .
 $bucket . '. Make sure they exist and your bucket is in the same region as
 this function.' . "\n";
                throw $e;
            }
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Python

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')
```

```
s3 = boto3.client('s3')


def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']
['key'], encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they
 exist and your bucket is in the same region as this function.'.format(key,
 bucket))
        raise e
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein S3-Ereignis mit Lambda mithilfe von Ruby konsumieren.

```
require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'
```

```
def lambda_handler(event:, context:)
  s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
  # puts "Received event: #{JSON.dump(event)}"

  # Get the object from the event and show its content type
  bucket = event['Records'][0]['s3']['bucket']['name']
  key = URI.decode_www_form_component(event['Records'][0]['s3']['object']
['key'], Encoding::UTF_8)
  begin
    response = s3.get_object(bucket: bucket, key: key)
    puts "CONTENT TYPE: #{response.content_type}"
    return response.content_type
  rescue StandardError => e
    puts e.message
    puts "Error getting object #{key} from bucket #{bucket}. Make sure they
 exist and your bucket is in the same region as this function."
    raise e
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

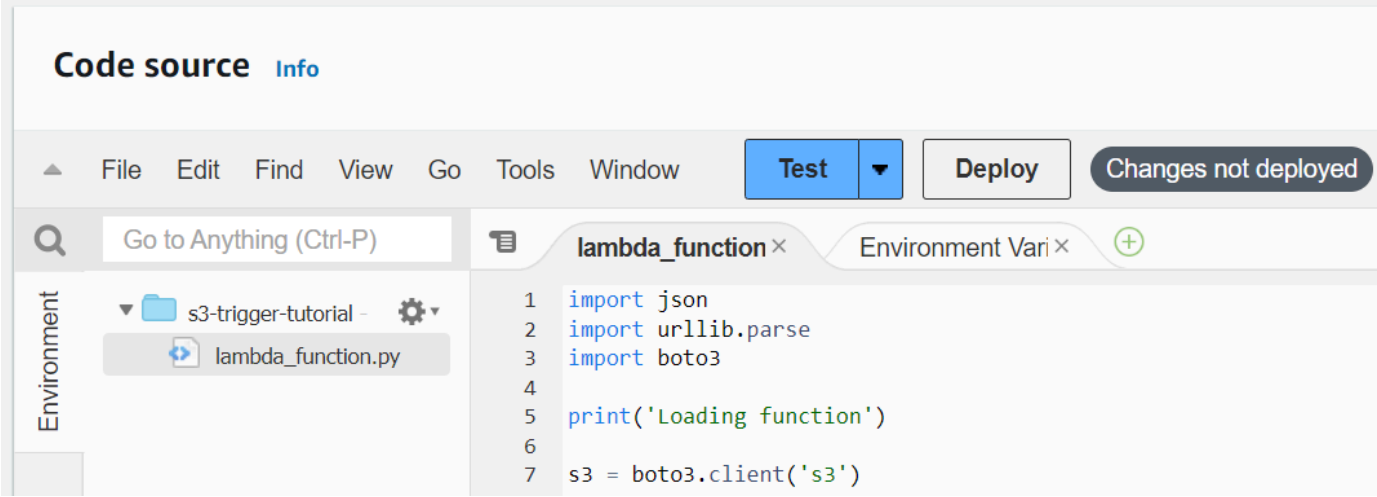
Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Rust

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};


/// Main function
```

```
#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    // Initialize the AWS SDK for Rust
    let config = aws_config::load_from_env().await;
    let s3_client = Client::new(&config);

    let res = run(service_fn(|request: LambdaEvent<S3Event>| {
        function_handler(&s3_client, request)
    })).await;

    res
}

async fn function_handler(
    s3_client: &Client,
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request
 from SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket =
 evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket name to
 exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object
 key to exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;
```

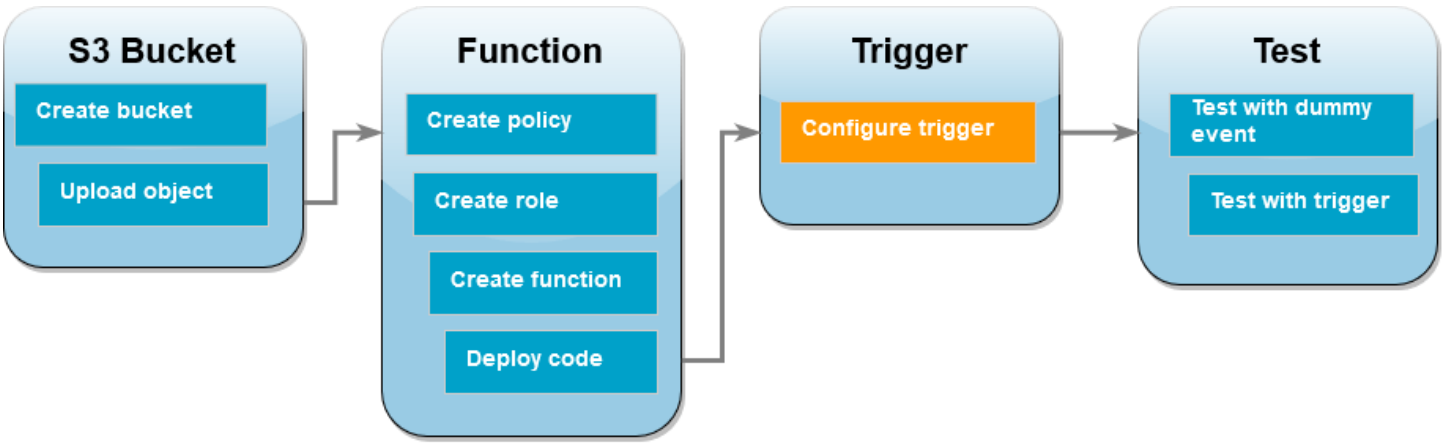
```
    match s3_get_object_result {
        Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
 contains a 'body' property of type ByteStream"),
        Err(_) => tracing::info!("Failure with S3 Get Object request")
    }

    Ok(())
}
```

2. Fügen Sie den Code im Bereich Codequelle der Lambda-Konsole in die Datei lambda_function.py ein.



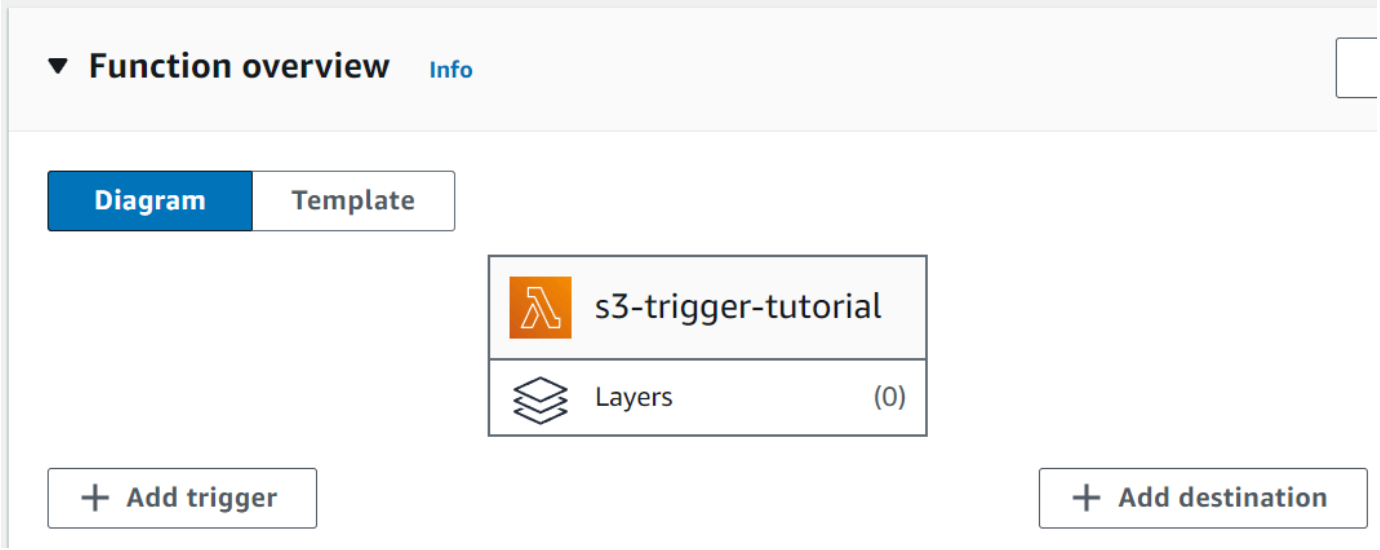
3. Wählen Sie Bereitstellen.

Erstellen des Amazon-S3-Auslösers



Erstellen des Amazon-S3-Auslösers

1. Wählen Sie im Bereich Function overview (Funktionsübersicht) die Option Add trigger (Auslöser hinzufügen).



2. Wählen Sie S3 aus.
3. Wählen Sie unter Bucket den Bucket aus, den Sie zuvor im Tutorial erstellt haben.
4. Vergewissern Sie sich, dass unter Ereignistypen die Option Alle Ereignisse zur Objekterstellung ausgewählt ist.
5. Aktivieren Sie unter Rekursiver Aufruf das Kontrollkästchen, um zu bestätigen, dass die Verwendung desselben Amazon-S3-Buckets für die Ein- und Ausgabe nicht empfohlen wird.
6. Wählen Sie Hinzufügen aus.

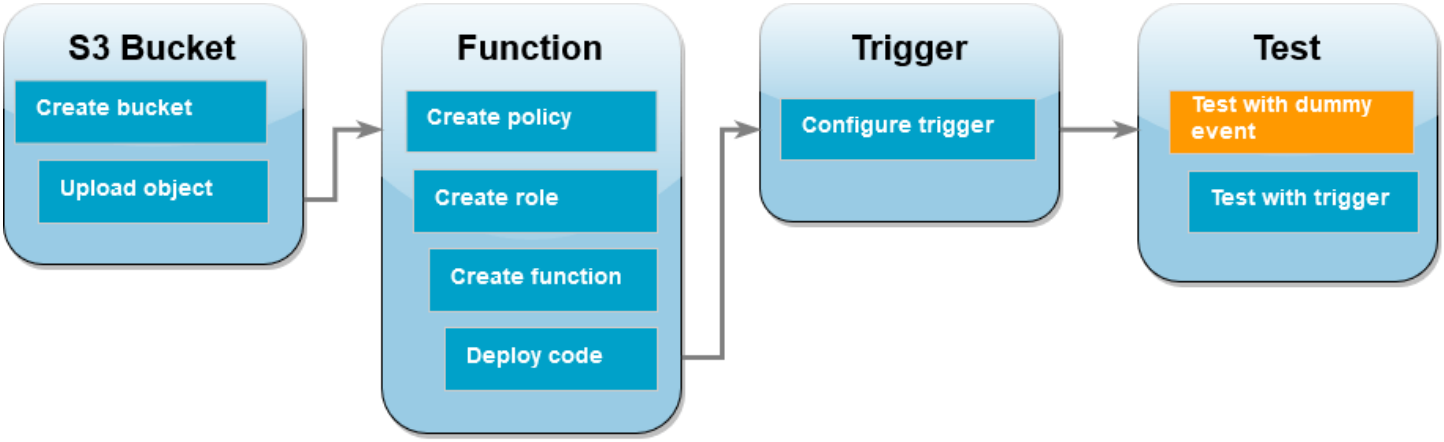
> **Note**
>
> Wenn Sie mit der Lambda-Konsole einen Amazon S3-Trigger für eine Lambda-Funktion erstellen, konfiguriert Amazon S3 eine Ereignisbenachrichtigung für den von Ihnen angegebenen Bucket. Vor der Konfiguration dieser Ereignisbenachrichtigung führt Amazon S3 eine Reihe von Prüfungen durch, um sicherzustellen, dass das Ereignisziel existiert und über die erforderlichen IAM-Richtlinien verfügt. Amazon S3 führt diese Tests auch für alle anderen Ereignisbenachrichtigungen durch, die für diesen Bucket konfiguriert sind. Aufgrund dieser Prüfung kann Amazon S3 die neue Ereignisbenachrichtigung nicht erstellen, wenn der Bucket zuvor Ereignisziele für Ressourcen konfiguriert hat, die nicht mehr existieren, oder für Ressourcen, die nicht über die erforderlichen Berechtigungsrichtlinien

verfügen. Es wird die folgende Fehlermeldung angezeigt, die darauf hinweist, dass Ihr Trigger nicht erstellt werden konnte:

```
An error occurred when creating the trigger: Unable to validate the following
 destination configurations.
```

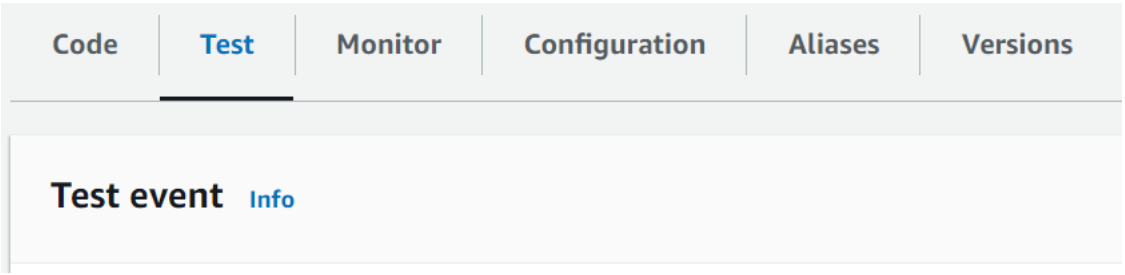
Sie können diesen Fehler sehen, wenn Sie zuvor einen Trigger für eine andere Lambda-Funktion konfiguriert haben, die denselben Bucket verwendet, und Sie die Funktion inzwischen gelöscht oder ihre Berechtigungsrichtlinien geändert haben.

Testen Ihrer Lambda-Funktion mit einem Dummy-Ereignis



So testen Sie die Lambda-Funktion mit einem Dummy-Ereignis

1. Wählen Sie auf der Lambda-Konsolenseite für Ihre Funktion die Registerkarte Test aus.



2. Geben Sie für Event name (Ereignisname) `MyTestEvent` ein.
3. Fügen Sie im Event-JSON das folgende Testereignis ein. Achten Sie darauf, diese Werte zu ersetzen:

   - Ersetzen Sie `us-east-1` durch die Region, in der Sie den Amazon-S3-Bucket erstellt haben.

- Ersetzen Sie beide Vorkommen von `DOC-EXAMPLE-BUCKET` durch den Namen Ihres eigenen Amazon-S3-Buckets.
- Ersetzen Sie `test%2FKey` durch den Namen des Testobjekts, das Sie zuvor in Ihren Bucket hochgeladen haben (z. B.`HappyFace.jpg`).

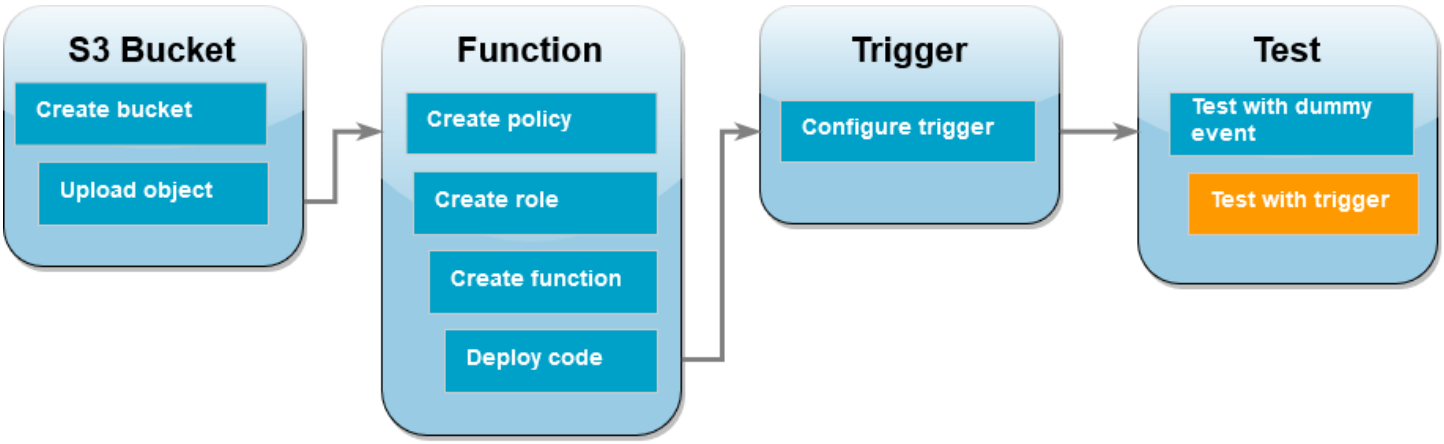
```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "DOC-EXAMPLE-BUCKET",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
          "eTag": "0123456789abcdef0123456789abcdef",
          "sequencer": "0A1B2C3D4E5F678901"
        }
      }
```

```
    }
  ]
}
```

4. Wählen Sie Save (Speichern) aus.
5. Wählen Sie Test aus.
6. Wenn Ihre Funktion erfolgreich ausgeführt wird, wird auf der Registerkarte Ausführungsergebnisse eine Ausgabe angezeigt, die der folgenden ähnelt.

```
Response
"image/jpeg"

Function Logs
START RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6 Version: $LATEST
2021-02-18T21:40:59.280Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    INPUT
 BUCKET AND KEY:  { Bucket: 'DOC-EXAMPLE-BUCKET', Key: 'HappyFace.jpg' }
2021-02-18T21:41:00.215Z    12b3cae7-5f4e-415e-93e6-416b8f8b66e6    INFO    CONTENT
 TYPE: image/jpeg
END RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6
REPORT RequestId: 12b3cae7-5f4e-415e-93e6-416b8f8b66e6    Duration: 976.25 ms
 Billed Duration: 977 ms    Memory Size: 128 MB    Max Memory Used: 90 MB    Init
 Duration: 430.47 ms

Request ID
12b3cae7-5f4e-415e-93e6-416b8f8b66e6
```

Testen der Lambda-Funktion mit dem Amazon-S3-Auslöser



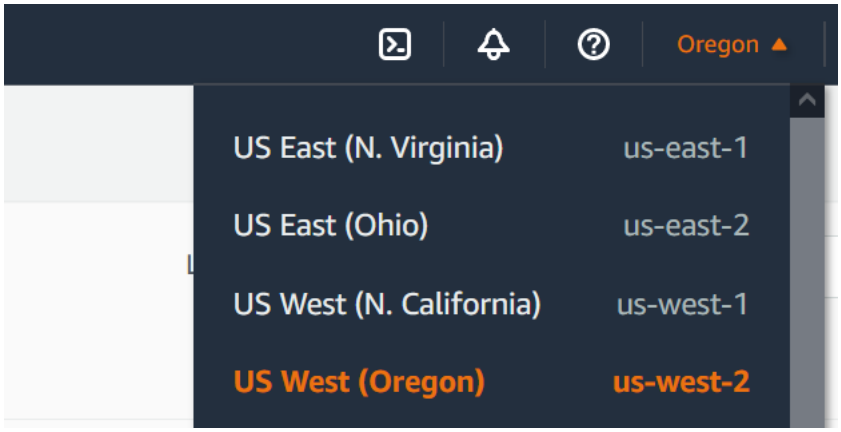
Um Ihre Funktion mit dem konfigurierten Trigger zu testen, laden Sie über die Konsole ein Objekt in Ihren Amazon S3 S3-Bucket hoch. Um zu überprüfen, ob Ihre Lambda-Funktion wie erwartet ausgeführt wurde, verwenden Sie CloudWatch Logs, um die Ausgabe Ihrer Funktion einzusehen.

So laden Sie Objekte in Ihren Amazon-S3-Bucket hoch

1. Öffnen Sie die Buckets-Seite der Amazon S3 S3-Konsole und wählen Sie den Bucket aus, den Sie zuvor erstellt haben.
2. Klicken Sie auf Hochladen.
3. Wählen Sie Dateien hinzufügen aus und wählen Sie mit der Dateiauswahl ein Objekt aus, das Sie hochladen möchten. Bei diesem Objekt kann es sich um eine beliebige von Ihnen ausgewählte Datei handeln.
4. Wählen Sie Öffnen und anschließend Hochladen aus.

Um den Funktionsaufruf mithilfe von Logs zu überprüfen CloudWatch

1. Öffnen Sie die CloudWatch-Konsole.
2. Stellen Sie sicher, dass Sie in derselben Umgebung arbeiten, in der AWS-Region Sie Ihre Lambda-Funktion erstellt haben. Sie können Ihre Region mithilfe der Dropdown-Liste oben auf dem Bildschirm ändern.



3. Wählen Sie Protokolle und anschließend Protokollgruppen aus.
4. Wählen Sie die Protokollgruppe für Ihre Funktion (`/aws/lambda/s3-trigger-tutorial`) aus.
5. Wählen Sie im Bereich Protokollstreams den neuesten Protokollstream aus.

6. Wenn Ihre Funktion als Reaktion auf Ihren Amazon S3 S3-Trigger korrekt aufgerufen wurde, erhalten Sie eine Ausgabe, die der folgenden ähnelt. Welchen `CONTENT TYPE` Sie sehen, hängt von der Art der Datei ab, die Sie in Ihren Bucket hochgeladen haben.

```
2022-05-09T23:17:28.702Z 0cae7f5a-b0af-4c73-8563-a3430333cc10 INFO CONTENT
 TYPE: image/jpeg
```

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, verhindern Sie unnötige Gebühren für Ihre AWS-Konto.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie den S3-Bucket:

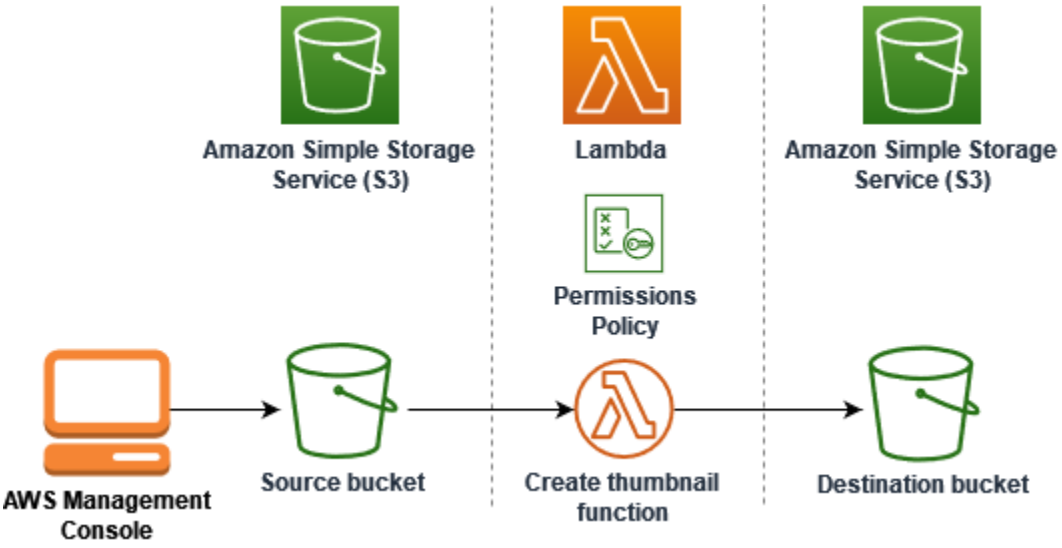
1. Öffnen Sie die Amazon S3-Konsole.
2. Wählen Sie den Bucket aus, den Sie erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen des Buckets in das Texteingabefeld ein.
5. Wählen Sie Bucket löschen aus.

Nächste Schritte

In Tutorial: Verwenden eines Amazon-S3-Auslösers zum Erstellen von Miniaturbildern ruft der Amazon S3 S3-Trigger eine Funktion auf, die für jede Bilddatei, die in einen Bucket hochgeladen wird, ein Miniaturbild erstellt. Dieses Tutorial erfordert ein gewisses Maß AWS an Wissen über Lambda-Domänen. Es zeigt, wie Ressourcen mithilfe von AWS Command Line Interface (AWS CLI) erstellt werden und wie ein Bereitstellungspaket für das ZIP-Dateiarchiv für die Funktion und ihre Abhängigkeiten erstellt wird.

Tutorial: Verwenden eines Amazon-S3-Auslösers zum Erstellen von Miniaturbildern

In diesem Tutorial wird eine Lambda-Funktion erstellt und konfiguriert, die die Größe von Bildern anpasst, die einem Amazon Simple Storage Service (Amazon S3)-Bucket hinzugefügt werden. Wenn Sie Ihrem Bucket eine Bilddatei hinzufügen, ruft Amazon S3 Ihre Lambda-Funktion auf. Die Funktion erstellt daraufhin eine Miniaturversion des Bilds und gibt sie an einen anderen Amazon-S3-Bucket aus.



Führen Sie für dieses Tutorial die folgenden Schritte aus:

1. Erstellen Sie Quell- und Ziel-Buckets für Amazon S3 und laden Sie ein Beispielbild hoch.
2. Erstellen Sie eine Lambda-Funktion, die die Größe eines Bildes anpasst und eine Miniaturansicht an einen Amazon-S3-Bucket ausgibt.
3. Konfigurieren Sie einen Lambda-Auslöser, der Ihre Funktion aufruft, wenn Objekte in Ihren Quell-Bucket hochgeladen werden.

4. Testen Sie Ihre Funktion zunächst mit einem Dummy-Ereignis und anschließend durch Hochladen eines Bilds in Ihren Quell-Bucket.

Diese Schritte zeigen, wie Sie Lambda verwenden, um eine Dateiverarbeitungsaufgabe für Objekte auszuführen, die einem Amazon-S3-Bucket hinzugefügt werden. Sie können dieses Tutorial mit dem AWS Command Line Interface (AWS CLI) oder dem abschließen AWS Management Console.

Ein einfacheres Beispiel, das zeigt, wie Sie einen Amazon-S3-Auslöser für Lambda konfigurieren, finden Sie unter Tutorial: Verwenden eines Amazon-S3-Auslösers zum Aufrufen einer Lambda-Funktion.

Themen

Voraussetzungen

Melde dich an für eine AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

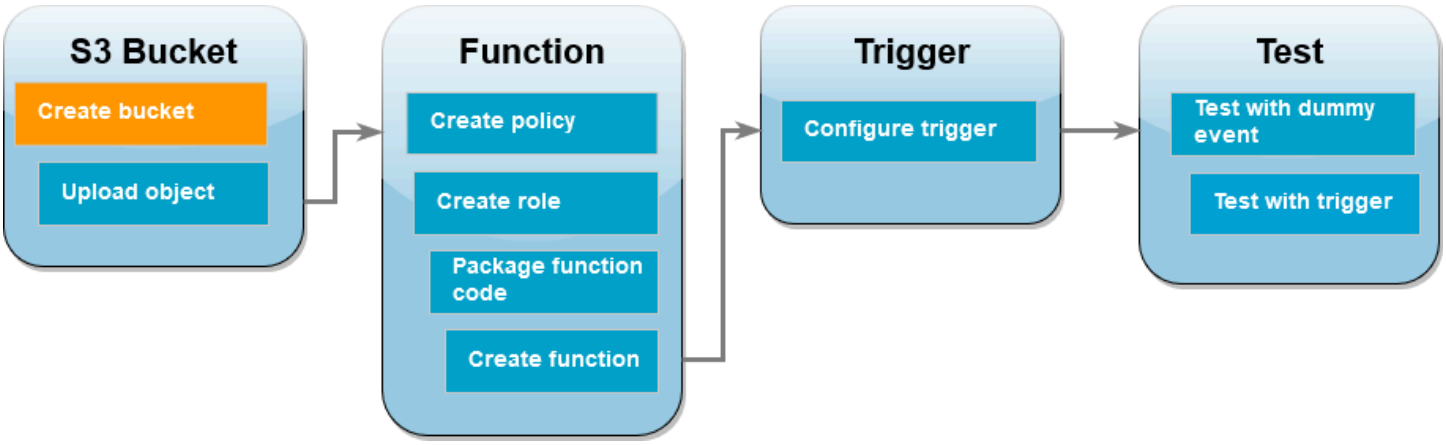
   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Wenn Sie den verwenden möchten, AWS CLI um das Tutorial abzuschließen, installieren Sie die neueste Version von. AWS Command Line Interface

Für Ihren Lambda-Funktionscode können Sie Python, Node.js oder Java verwenden. Installieren Sie die Tools zur Sprachunterstützung und einen Paketmanager für die gewünschte Sprache.

Erstellen von zwei Amazon-S3-Buckets



Erstellen Sie zunächst zwei Amazon-S3-Buckets. Der erste Bucket ist der Quell-Bucket, in den Sie Ihre Bilder hochladen. Der zweite Bucket wird von Lambda verwendet, um das verkleinerte Miniaturbild zu speichern, wenn Sie Ihre Funktion aufrufen.

AWS Management Console

So erstellen Sie die Amazon-S3-Buckets (Konsole)

1. Öffnen Sie die Seite Buckets der Amazon-S3-Konsole.
2. Wählen Sie Bucket erstellen aus.
3. Führen Sie unter Allgemeine Konfiguration die folgenden Schritte aus:
   a. Geben Sie für den Bucket-Namen einen global eindeutigen Namen ein, der den Regeln für die Bucket-Benennung von Amazon S3 entspricht. Bucket-Namen dürfen nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen.
   b. Wählen Sie unter AWS-Region die AWS-Region aus, die Ihrem geografischen Standort am nächsten ist. Später im Tutorial müssen Sie Ihre Lambda-Funktion in derselben erstellen. Notieren Sie sich also die Region AWS-Region, die Sie ausgewählt haben.
4. Belassen Sie alle anderen Optionen auf ihren Standardwerten und wählen Sie Bucket erstellen aus.
5. Wiederholen Sie die Schritte 1 bis 4, um Ihren Ziel-Bucket zu erstellen. Geben Sie unter Bucket-Name den Namen **`DOC-EXAMPLE-SOURCE-BUCKET-resized`** ein. **`DOC-EXAMPLE-SOURCE-BUCKET`** ist hierbei der Name des Quell-Buckets, den Sie soeben erstellt haben.

AWS CLI

So erstellen Sie die Amazon-S3-Buckets (AWS CLI)

1. Führen Sie den folgenden CLI-Befehl aus, um Ihren Quell-Bucket zu erstellen. Der gewählte Name für Ihren Bucket muss global eindeutig sein und den Regeln für die Benennung von Buckets für Amazon S3 entsprechen. Namen dürfen nur Kleinbuchstaben, Zahlen, Punkte (.) und Bindestriche (-) enthalten. Wählen Sie für `region` und `LocationConstraint` die AWS-Region aus, die Ihrem geografischen Standort am nächsten ist.

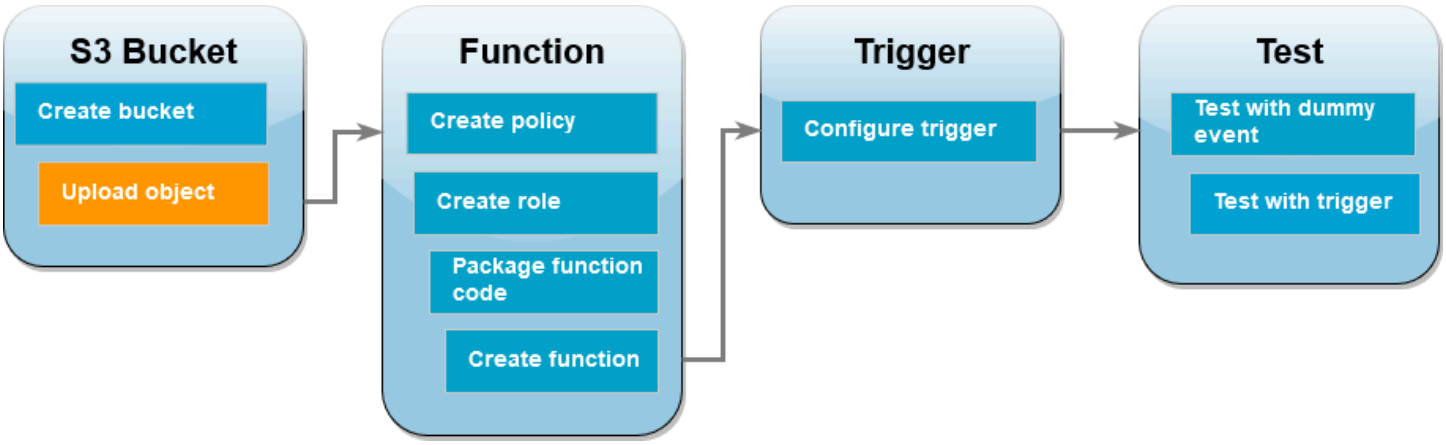
   ```
   aws s3api create-bucket --bucket DOC-EXAMPLE-SOURCE-BUCKET --region us-west-2 \
   --create-bucket-configuration LocationConstraint=us-west-2
   ```

   Später im Tutorial müssen Sie Ihre Lambda-Funktion im selben Verzeichnis AWS-Region wie in Ihrem Quell-Bucket erstellen. Notieren Sie sich also die Region, die Sie ausgewählt haben.

2. Führen Sie den folgenden Befehl aus, um Ihren Ziel-Bucket zu erstellen. Verwenden Sie für den Bucket-Namen **`DOC-EXAMPLE-SOURCE-BUCKET-resized`**. **`DOC-EXAMPLE-SOURCE-BUCKET`** ist hierbei der Name des Quell-Buckets, den Sie in Schritt 1 erstellt haben. Wählen Sie für `region` und dasselbe aus`LocationConstraint`, das AWS-Region Sie zur Erstellung Ihres Quell-Buckets verwendet haben.

   ```
   aws s3api create-bucket --bucket DOC-EXAMPLE-SOURCE-BUCKET-resized --region us-
   west-2 \
   --create-bucket-configuration LocationConstraint=us-west-2
   ```

Hochladen eines Testbilds in Ihren Quell-Bucket



Später im Tutorial testen Sie Ihre Lambda-Funktion, indem Sie sie mit der AWS CLI oder der Lambda-Konsole aufrufen. Damit Sie sich vergewissern können, dass Ihre Funktion ordnungsgemäß funktioniert, muss Ihr Quell-Bucket ein Testbild enthalten. Bei diesem Bild kann es sich um eine beliebige JPG- oder PNG-Datei handeln.

AWS Management Console

So laden Sie ein Testbild in Ihren Quell-Bucket hoch (Konsole)

1. Öffnen Sie die Seite Buckets der Amazon-S3-Konsole.
2. Wählen Sie den Quell-Bucket aus, den Sie im vorherigen Schritt erstellt haben.
3. Klicken Sie auf Hochladen.
4. Wählen Sie Dateien hinzufügen aus und wählen Sie mit der Dateiauswahl das Objekt aus, das Sie hochladen möchten.
5. Wählen Sie Öffnen und anschließend Hochladen aus.

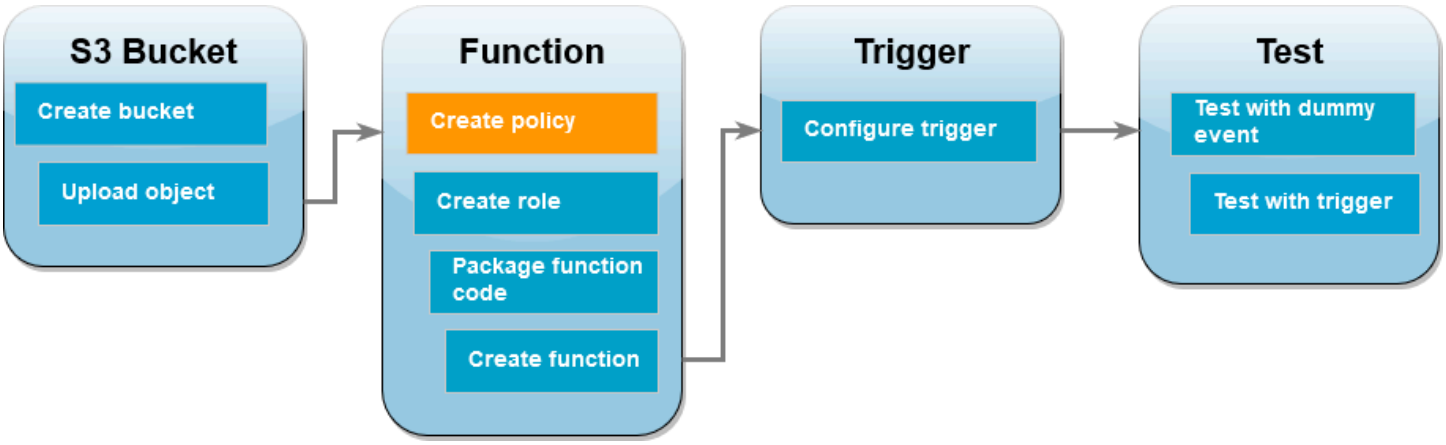
AWS CLI

So laden Sie ein Testbild in Ihren Quell-Bucket hoch (AWS CLI)

- Führen Sie in dem Verzeichnis, das das hochzuladende Bild enthält, den folgenden CLI-Befehl aus. Ersetzen Sie dabei den Parameter `--bucket` durch den Namen Ihres Quell-Buckets. Verwenden Sie für die Parameter `--key` und `--body` den Dateinamen Ihres Testbilds.

```
aws s3api put-object --bucket DOC-EXAMPLE-SOURCE-BUCKET --key HappyFace.jpg --
body ./HappyFace.jpg
```

Erstellen einer Berechtigungsrichtlinie



Im ersten Schritt der Erstellung Ihrer Lambda-Funktion wird eine Berechtigungsrichtlinie erstellt. Diese Richtlinie gibt Ihrer Funktion die Berechtigungen, die sie für den Zugriff auf andere Ressourcen benötigt. AWS In diesem Tutorial gewährt die Richtlinie Lambda Lese- und Schreibberechtigungen für Amazon S3 S3-Buckets und ermöglicht es ihm, in Amazon CloudWatch Logs zu schreiben.

AWS Management Console

So erstellen Sie die Richtlinie (Konsole)

1. Öffnen Sie die Seite Richtlinien der AWS Identity and Access Management (IAM-) Konsole.
2. Wählen Sie Richtlinie erstellen aus.
3. Wählen Sie die Registerkarte JSON aus und kopieren Sie dann die folgende benutzerdefinierte JSON-Richtlinie in den JSON-Editor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

4. Wählen Sie Weiter aus.
5. Geben Sie unter Richtliniendetails für den Richtliniennamen **`LambdaS3Policy`** ein.
6. Wählen Sie Richtlinie erstellen aus.

AWS CLI

So erstellen Sie die Richtlinie (AWS CLI)

1. Speichern Sie den folgenden JSON-Code in einer Datei mit dem Namen `policy.json`:

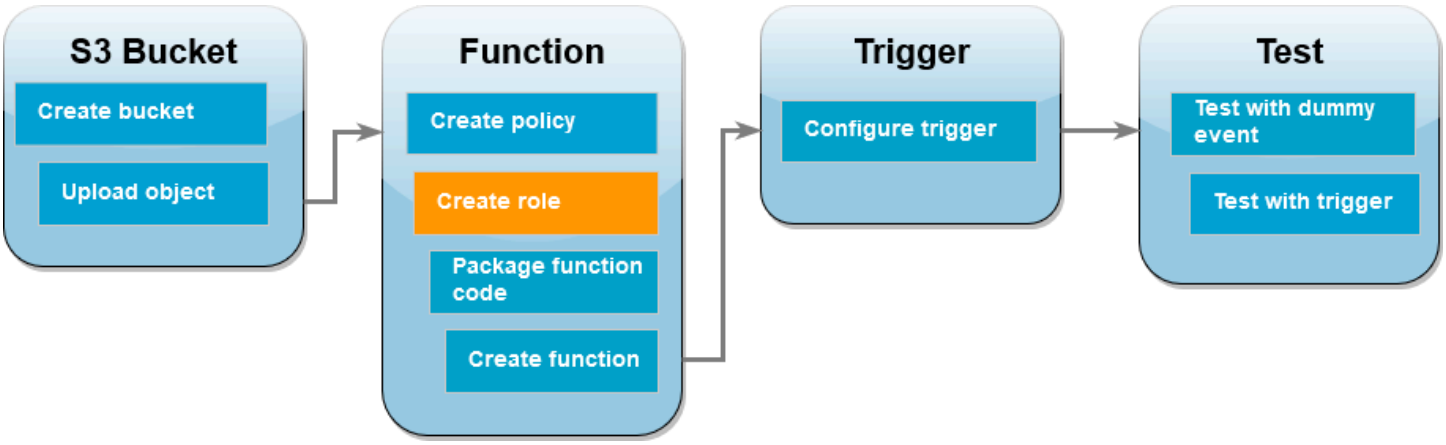
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
```

```
            "Resource": "arn:aws:s3:::*/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::*/*"
        }
    ]
}
```

2. Führen Sie in dem Verzeichnis, in dem Sie das JSON-Richtliniendokument gespeichert haben, den folgenden CLI-Befehl aus:

```
aws iam create-policy --policy-name LambdaS3Policy --policy-document file://
policy.json
```

Erstellen einer Ausführungsrolle



Eine Ausführungsrolle ist eine IAM-Rolle, die einer Lambda-Funktion Zugriff AWS-Services und Ressourcen gewährt. Um Ihrer Funktion Lese- und Schreibzugriff auf einen Amazon-S3-Bucket zu erteilen, fügen Sie die Berechtigungsrichtlinie an, die Sie im vorherigen Schritt erstellt haben.

AWS Management Console

So erstellen Sie eine Ausführungsrolle und fügen Ihre Berechtigungsrichtlinie hinzu (Konsole)

1. Öffnen Sie die Seite Rollen der (IAM-)Konsole.
2. Wählen Sie Rolle erstellen aus.

3. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS-Service und unter Anwendungsfall die Option Lambda aus.
4. Wählen Sie Weiter aus.
5. Fügen Sie die Berechtigungsrichtlinie hinzu, die Sie im vorherigen Schritt erstellt haben:
   a. Geben Sie im Feld für die Richtliniensuche **`LambdaS3Policy`** ein.
   b. Aktivieren Sie in den Suchergebnissen das Kontrollkästchen für `LambdaS3Policy`.
   c. Wählen Sie Weiter aus.
6. Geben Sie unter Rollendetails im Feld Rollenname den Namen **`LambdaS3Role`** ein.
7. Wählen Sie Rolle erstellen aus.

AWS CLI

So erstellen Sie eine Ausführungsrolle und fügen Ihre Berechtigungsrichtlinie an (AWS CLI)

1. Speichern Sie den folgenden JSON-Code in einer Datei mit dem Namen `trust-policy.json`: Diese Vertrauensrichtlinie ermöglicht es Lambda, die Berechtigungen der Rolle zu verwenden, indem dem Dienstprinzipal die `lambda.amazonaws.com` Erlaubnis erteilt wird, die `AssumeRole` Aktion AWS Security Token Service (AWS STS) aufzurufen.

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

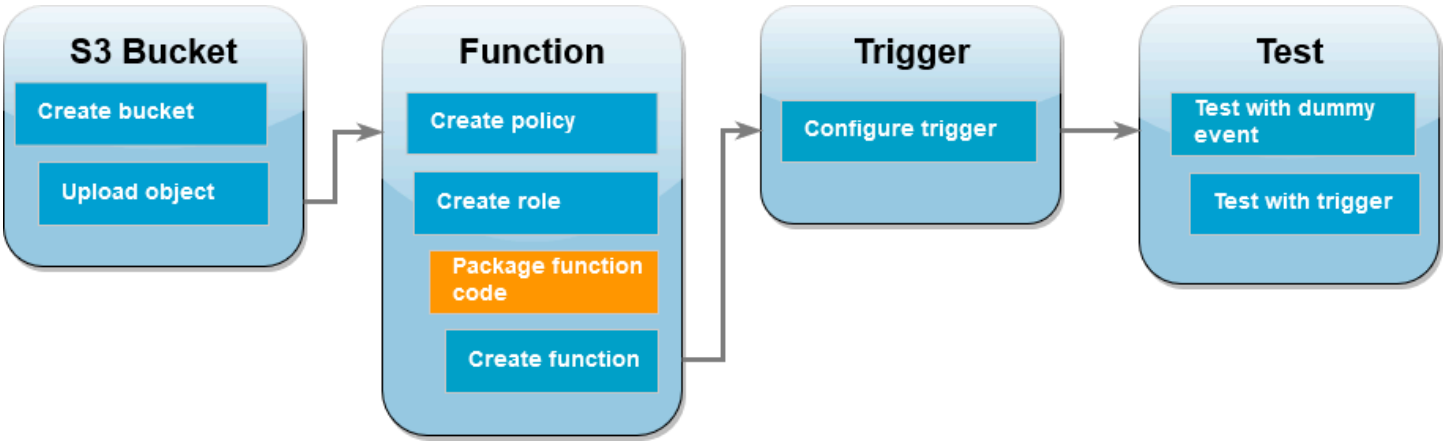
2. Führen Sie in dem Verzeichnis, in dem Sie das JSON-Vertrauensrichtliniendokument gespeichert haben, den folgenden CLI-Befehl aus, um die Ausführungsrolle zu erstellen:

```
aws iam create-role --role-name LambdaS3Role --assume-role-policy-document
 file://trust-policy.json
```

3. Führen Sie den folgenden CLI-Befehl aus, um die im vorherigen Schritt erstellte Berechtigungsrolle anzufügen. Ersetzen Sie die AWS-Konto Nummer im ARN der Police durch Ihre eigene Kontonummer.

```
aws iam attach-role-policy --role-name LambdaS3Role --policy-arn
 arn:aws:iam::123456789012:policy/LambdaS3Policy
```

Erstellen des Bereitstellungspakets für die Funktion



Um Ihre Funktion zu erstellen, erstellen Sie ein Bereitstellungspaket, das Ihren Funktionscode und die zugehörigen Abhängigkeiten enthält. Bei der hier verwendeten Funktion `CreateThumbnail` verwendet Ihr Funktionscode eine separate Bibliothek für die Anpassung der Bildgröße. Folgen Sie den Anweisungen für die von Ihnen gewählte Sprache, um ein Bereitstellungspaket zu erstellen, das die erforderliche Bibliothek enthält.

Node.js

So erstellen Sie das Bereitstellungspaket (Node.js)

1. Erstellen Sie ein Verzeichnis namens `lambda-s3` für Ihren Funktionscode und die Abhängigkeiten und navigieren Sie dorthin.

```
mkdir lambda-s3
cd lambda-s3
```

2. Speichern Sie den folgenden Funktionscode in einer lokalen Datei namens `index.mjs`: Stellen Sie sicher, dass Sie durch den Bucket `'us-west-2'` ersetzen, AWS-Region in dem Sie Ihre eigenen Quell- und Ziel-Buckets erstellt haben.

```
// dependencies
import { S3Client, GetObjectCommand, PutObjectCommand } from '@aws-sdk/client-
s3';

import { Readable } from 'stream';

import sharp from 'sharp';
import util from 'util';


// create S3 client
const s3 = new S3Client({region: 'us-west-2'});

// define the handler function
export const handler = async (event, context) => {

// Read options from the event parameter and get the source bucket
console.log("Reading options from event:\n", util.inspect(event, {depth: 5}));
  const srcBucket = event.Records[0].s3.bucket.name;

// Object key may have spaces or unicode non-ASCII characters
const srcKey    = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/
g, " "));
const dstBucket = srcBucket + "-resized";
const dstKey    = "resized-" + srcKey;

// Infer the image type from the file suffix
const typeMatch = srcKey.match(/\.([^.]*)$/);
if (!typeMatch) {
  console.log("Could not determine the image type.");
  return;
}

// Check that the image type is supported
const imageType = typeMatch[1].toLowerCase();
if (imageType != "jpg" && imageType != "png") {
  console.log(`Unsupported image type: ${imageType}`);
  return;
}

// Get the image from the source bucket. GetObjectCommand returns a stream.
try {
  const params = {
```

```
    Bucket: srcBucket,
    Key: srcKey
  };
  var response = await s3.send(new GetObjectCommand(params));
  var stream = response.Body;

// Convert stream to buffer to pass to sharp resize function.
  if (stream instanceof Readable) {
    var content_buffer = Buffer.concat(await stream.toArray());

  } else {
    throw new Error('Unknown object stream type');
  }


} catch (error) {
  console.log(error);
  return;
}


// set thumbnail width. Resize will set the height automatically to maintain
 aspect ratio.
const width  = 200;

// Use the sharp module to resize the image and save in a buffer.
try {
  var output_buffer = await sharp(content_buffer).resize(width).toBuffer();

} catch (error) {
  console.log(error);
  return;
}

// Upload the thumbnail image to the destination bucket
try {
  const destparams = {
    Bucket: dstBucket,
    Key: dstKey,
    Body: output_buffer,
    ContentType: "image"
  };

  const putResult = await s3.send(new PutObjectCommand(destparams));
```

```
  } catch (error) {
    console.log(error);
    return;
  }

  console.log('Successfully resized ' + srcBucket + '/' + srcKey +
    ' and uploaded to ' + dstBucket + '/' + dstKey);
  };
```

3. Installieren Sie die Sharp-Bibliothek mithilfe von npm im Verzeichnis `lambda-s3`. Beachten Sie, dass die neueste Version von Sharp (0.33) nicht mit Lambda kompatibel ist. Installieren Sie für dieses Tutorial daher Version 0.32.6.

   ```
   npm install sharp@0.32.6
   ```

   Der npm-Befehl `install` erstellt ein Verzeichnis namens `node_modules` für Ihre Module. Nach diesem Schritt sollte Ihre Verzeichnisstruktur wie folgt aussehen:

   ```
   lambda-s3
   |- index.mjs
   |- node_modules
   |  |- base64js
   |  |- bl
   |  |- buffer
   ...
   |- package-lock.json
   |- package.json
   ```

4. Erstellen Sie ein ZIP-Bereitstellungspaket, das Ihren Funktionscode und die zugehörigen Abhängigkeiten enthält. Führen Sie unter macOS oder Linux den folgenden Befehl aus:

   ```
   zip -r function.zip .
   ```

   Verwenden Sie unter Windows Ihr bevorzugtes ZIP-Programm, um eine ZIP-Datei zu erstellen. Achten Sie darauf, dass sich die Dateien `index.mjs`, `package.json` und `package-lock.json` und das Verzeichnis `node_modules` im Stammverzeichnis der ZIP-Datei befinden.

Python

So erstellen Sie das Bereitstellungspaket (Python)

1. Speichern Sie den Beispielcode als Datei mit dem Namen `lambda_function.py`.

```
import boto3
import os
import sys
import uuid
from urllib.parse import unquote_plus
from PIL import Image
import PIL.Image

s3_client = boto3.client('s3')

def resize_image(image_path, resized_path):
  with Image.open(image_path) as image:
    image.thumbnail(tuple(x / 2 for x in image.size))
    image.save(resized_path)

def lambda_handler(event, context):
  for record in event['Records']:
    bucket = record['s3']['bucket']['name']
    key = unquote_plus(record['s3']['object']['key'])
    tmpkey = key.replace('/', '')
    download_path = '/tmp/{}{}'.format(uuid.uuid4(), tmpkey)
    upload_path = '/tmp/resized-{}'.format(tmpkey)
    s3_client.download_file(bucket, key, download_path)
    resize_image(download_path, upload_path)
    s3_client.upload_file(upload_path, '{}-resized'.format(bucket), 'resized-
{}'.format(key))
```

2. Erstellen Sie in dem Verzeichnis, in dem Sie auch Ihre `lambda_function.py`-Datei erstellt haben, ein neues Verzeichnis mit dem Namen `package` und installieren Sie die Bibliothek Pillow (PIL) sowie das AWS SDK for Python (Boto3). Die Lambda-Python-Laufzeit enthält zwar eine Version des Boto3 SDK, es empfiehlt sich jedoch, dem Bereitstellungspaket alle Abhängigkeiten Ihrer Funktion hinzuzufügen, auch wenn sie in der Laufzeit enthalten sind. Weitere Informationen finden Sie in der Laufzeitabhängigkeiten in Python.

```
mkdir package
pip install \
```

```
--platform manylinux2014_x86_64 \
--target=package \
--implementation cp \
--python-version 3.9 \
--only-binary=:all: --upgrade \
pillow boto3
```

Die Pillow-Bibliothek enthält Code in C/C++. Mithilfe der Optionen `--platform manylinux_2014_x86_64` und `--only-binary=:all:` lädt pip eine Version von Pillow herunter und installiert sie, die vorkompilierte Binärdateien enthält, die mit dem Betriebssystem Amazon Linux 2 kompatibel sind. Dadurch wird sichergestellt, dass Ihr Bereitstellungspaket in der Lambda-Ausführungsumgebung funktioniert, unabhängig vom Betriebssystem und der Architektur Ihrer lokalen Build-Maschine.

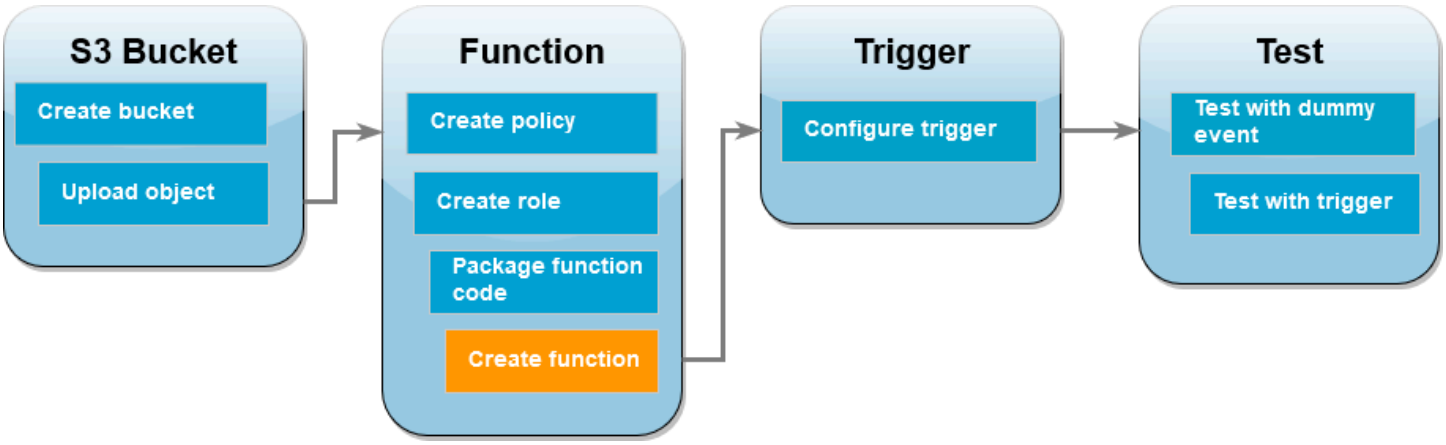
3. Erstellen Sie eine ZIP-Datei, die Ihren Anwendungscode sowie die Pillow- und die Boto3-Bibliothek enthält. Führen Sie unter Linux oder MacOS die folgenden Befehle über Ihre Befehlszeilenschnittstelle aus:

```
cd package
zip -r ../lambda_function.zip .
cd ..
zip lambda_function.zip lambda_function.py
```

Verwenden Sie unter Windows Ihr bevorzugtes ZIP-Tool, um die `lambda_function.zip`-Datei zu erstellen. Achten Sie darauf, dass sich die Datei `lambda_function.py` und die Ordner, die Ihre Abhängigkeiten enthalten, im Stammverzeichnis der ZIP-Datei befinden.

Sie können Ihr Bereitstellungspaket auch in einer virtuellen Python-Umgebung erstellen. Siehe Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen

So erstellen Sie die Lambda-Funktion:



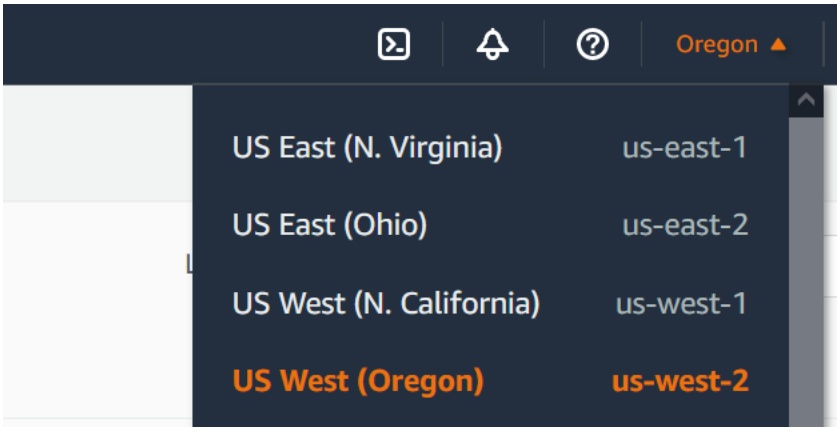
Sie können Ihre Lambda-Funktion entweder mit der AWS CLI oder der Lambda-Konsole erstellen. Folgen Sie den Anweisungen für die von Ihnen gewählte Sprache, um die Funktion zu erstellen.

AWS Management Console

So erstellen Sie die Funktion (Konsole)

Wenn Sie Ihre Lambda-Funktion über die Konsole erstellen möchten, erstellen Sie zunächst eine Basisfunktion, die etwas Hello-World-Code enthält. Anschließend ersetzen Sie diesen Code durch Ihren eigenen Funktionscode, indem Sie die im vorherigen Schritt erstellte ZIP- oder JAR-Datei hochladen.

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Stellen Sie sicher, dass Sie in demselben Modus arbeiten, in dem AWS-Region Sie Ihren Amazon S3 S3-Bucket erstellt haben. Sie können Ihre Region mithilfe der Dropdown-Liste am oberen Bildschirmrand ändern.



3. Wählen Sie Funktion erstellen.

4. Wählen Sie Author from scratch aus.
5. Führen Sie unter Basic information (Grundlegende Informationen) die folgenden Schritte aus:
   a. Geben Sie für Function name (Funktionsname) **`CreateThumbnail`** ein.
   b. Wählen Sie unter Laufzeit entweder Node.js 18.x oder Python 3.9 aus (je nachdem, welche Sprache Sie für Ihre Funktion gewählt haben).
   c. Wählen Sie für Architektur x86_64 aus.
6. Gehen Sie auf der Registerkarte Standard-Ausführungsrolle ändern wie folgt vor:
   a. Erweitern Sie die Registerkarte und wählen Sie dann Verwenden einer vorhandenen Rolle aus.
   b. Wählen Sie die zuvor erstellte `LambdaS3Role` aus.
7. Wählen Sie Funktion erstellen.

So laden Sie den Funktionscode hoch (Konsole)

1. Wählen Sie im Bereich Codequelle die Option Hochladen von aus.
2. Wählen Sie die ZIP-Datei aus.
3. Klicken Sie auf Hochladen.
4. Wählen Sie in der Dateiauswahl Ihre ZIP-Datei und anschließend Öffnen aus.
5. Wählen Sie Speichern.

AWS CLI

So erstellen Sie die Funktion (AWS CLI)

- Führen Sie den CLI-Befehl für die von Ihnen gewählte Sprache aus. Stellen Sie sicher, dass Sie den `role` Parameter durch Ihre eigene AWS-Konto ID `123456789012` ersetzen. Ersetzen Sie für den Parameter `region` den Wert `us-west-2` durch die Region, in der Sie Ihre Amazon-S3-Buckets erstellt haben.
  - Führen Sie für Node.js den folgenden Befehl in dem Verzeichnis aus, das die Datei `function.zip` enthält:

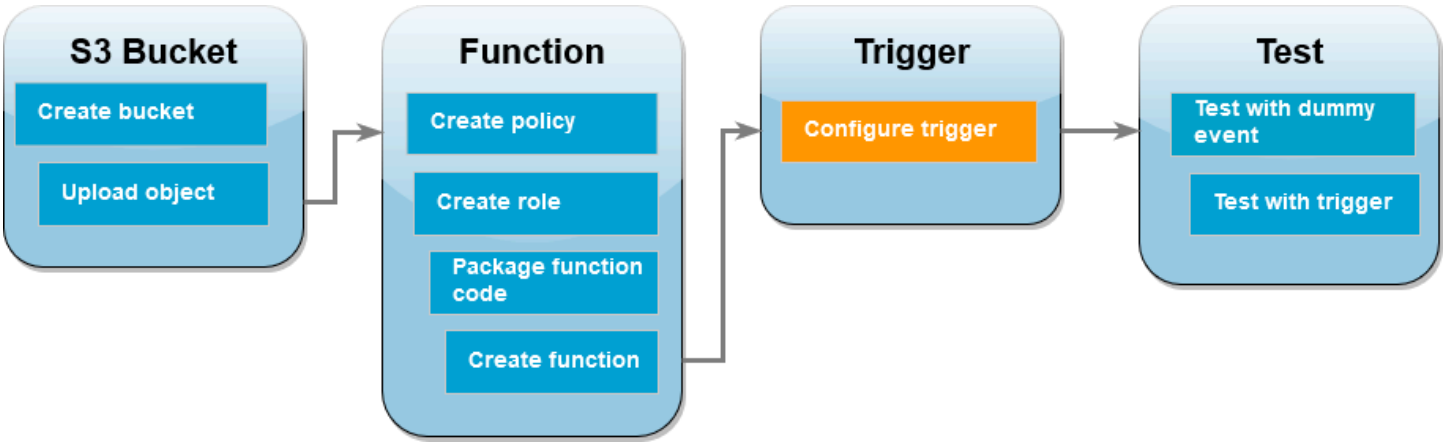
```
aws lambda create-function --function-name CreateThumbnail \
--zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
```

```
--timeout 10 --memory-size 1024 \
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-west-2
```

- Führen Sie für Python den folgenden Befehl in dem Verzeichnis aus, das die Datei `lambda_function.zip` enthält:

```
aws lambda create-function --function-name CreateThumbnail \
--zip-file fileb://lambda_function.zip --handler
 lambda_function.lambda_handler \
--runtime python3.9 --timeout 10 --memory-size 1024 \
--role arn:aws:iam::123456789012:role/LambdaS3Role --region us-west-2
```

Konfigurieren von Amazon S3 zum Aufrufen der Funktion



Damit Ihre Lambda-Funktion ausgeführt wird, wenn Sie ein Bild in Ihren Quell-Bucket hochladen, müssen Sie einen Auslöser für Ihre Funktion konfigurieren. Sie können den Amazon-S3-Auslöser entweder über die Konsole oder mithilfe der AWS CLI konfigurieren.

> **Important**
>
> Mit diesem Verfahren wird der Amazon-S3-Bucket so konfiguriert, dass die Funktion jedes Mal aufgerufen wird, wenn ein Objekt im Bucket erstellt wird. Konfigurieren Sie dieses Verhalten nur für den Quell-Bucket. Wenn Ihre Lambda-Funktion Objekte in dem Bucket erstellt, der sie aufruft, kann es passieren, dass Ihre Funktion kontinuierlich in einer Schleife aufgerufen wird. Dies kann dazu führen, dass Ihnen AWS-Konto unerwartete Gebühren in Rechnung gestellt werden.

AWS Management Console

So konfigurieren Sie den Amazon-S3-Auslöser (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole und wählen Sie Ihre Funktion (`CreateThumbnail`) aus.
2. Wählen Sie Add trigger.
3. Wählen Sie S3 aus.
4. Wählen Sie unter Bucket Ihren Quell-Bucket aus.
5. Wählen Sie unter Ereignistypen die Option Alle Objekterstellungsereignisse aus.
6. Aktivieren Sie unter Rekursiver Aufruf das Kontrollkästchen, um zu bestätigen, dass die Verwendung desselben Amazon-S3-Buckets für die Ein- und Ausgabe nicht empfohlen wird. Weitere Informationen zu rekursiven Aufrufmustern in Lambda finden Sie bei Serverless Land unter Recursive patterns that cause run-away Lambda functions.
7. Wählen Sie Hinzufügen aus.

   Wenn Sie einen Auslöser über die Lambda-Konsole erstellen, erstellt Lambda automatisch eine ressourcenbasierte Richtlinie, um dem von Ihnen ausgewählten Dienst die Berechtigung zum Aufrufen Ihrer Funktion zu erteilen.

AWS CLI

So konfigurieren Sie den Amazon-S3-Auslöser (AWS CLI)

1. Damit Ihr Amazon-S3-Quell-Bucket Ihre Funktion aufruft, wenn Sie eine Bilddatei hinzufügen, müssen Sie zunächst mithilfe einer ressourcenbasierten Richtlinie Berechtigungen für Ihre Funktion konfigurieren. Eine ressourcenbasierte Grundsatzerklärung erteilt anderen Personen die AWS-Services Erlaubnis, Ihre Funktion aufzurufen. Führen Sie den folgenden CLI-Befehl aus, um Amazon S3 die Berechtigung zum Aufrufen Ihrer Funktion zu erteilen. Achten Sie darauf, den `source-account` Parameter durch Ihre eigene AWS-Konto ID zu ersetzen und Ihren eigenen Quell-Bucket-Namen zu verwenden.

```
aws lambda add-permission --function-name CreateThumbnail \
--principal s3.amazonaws.com --statement-id s3invoke --action
 "lambda:InvokeFunction" \
--source-arn arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET \
--source-account 123456789012
```

Die mit diesem Befehl definierte Richtlinie ermöglicht es Amazon S3 nur, Ihre Funktion aufzurufen, wenn eine Aktion in Ihrem Quell-Bucket ausgeführt wird.

> **Note**
>
> Namen von Amazon-S3-Buckets sind zwar global eindeutig, trotzdem empfiehlt es sich, bei der Verwendung ressourcenbasierter Richtlinien anzugeben, dass der Bucket zu Ihrem Konto gehören muss. Denn wenn Sie einen Bucket löschen, kann ein anderer AWS-Konto Bucket einen Bucket mit demselben Amazon-Ressourcennamen (ARN) erstellen.

2. Speichern Sie den folgenden JSON-Code in einer Datei mit dem Namen `notification.json`: Wenn dieser JSON-Code auf Ihren Quell-Bucket angewendet wird, wird der Bucket so konfiguriert, dass er jedes Mal, wenn ein neues Objekt hinzugefügt wird, eine Benachrichtigung an Ihre Lambda-Funktion sendet. Ersetzen Sie die AWS-Konto Nummer und AWS-Region in der Lambda-Funktion ARN durch Ihre eigene Kontonummer und Region.

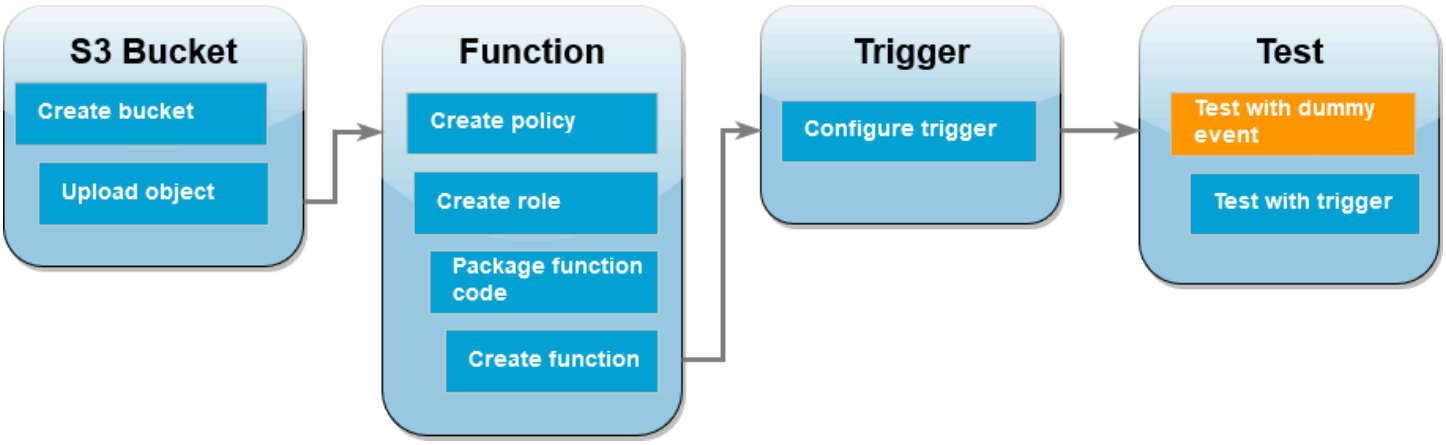
```
{
"LambdaFunctionConfigurations": [
    {
      "Id": "CreateThumbnailEventConfiguration",
      "LambdaFunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:CreateThumbnail",
      "Events": [ "s3:ObjectCreated:Put" ]
    }
  ]
}
```

3. Führen Sie den folgenden CLI-Befehl aus, um die Benachrichtigungseinstellungen in der von Ihnen erstellten JSON-Datei auf Ihren Quell-Bucket anzuwenden. Ersetzen Sie dabei `DOC-EXAMPLE-SOURCE-BUCKET` durch den Namen Ihres Quell-Buckets.

```
aws s3api put-bucket-notification-configuration --bucket DOC-EXAMPLE-SOURCE-
BUCKET \
--notification-configuration file://notification.json
```

Weitere Informationen zu dem `put-bucket-notification-configuration` Befehl und der `notification-configuration` Option finden Sie put-bucket-notification-configurationin der AWS CLI-Befehlsreferenz.

Testen Ihrer Lambda-Funktion mit einem Dummy-Ereignis



Bevor Sie Ihr gesamtes Setup testen, indem Sie Ihrem Amazon-S3-Quell-Bucket eine Bilddatei hinzufügen, testen Sie, ob Ihre Lambda-Funktion ordnungsgemäß funktioniert, indem Sie sie mit einem Dummy-Ereignis aufrufen. In Lambda ist ein Ereignis ein Dokument im JSON-Format, das Daten enthält, die von Ihrer Lambda-Funktion verarbeitet werden sollen. Wenn Ihre Funktion von Amazon S3 aufgerufen wird, enthält das an Ihre Funktion gesendete Ereignis Informationen wie den Bucket-Namen, den Bucket-ARN und den Objektschlüssel.

AWS Management Console

So testen Sie Ihre Lambda-Funktion mit einem Dummy-Ereignis (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole und wählen Sie Ihre Funktion (`CreateThumbnail`) aus.
2. Wählen Sie die Registerkarte Test.
3. Gehen Sie im Bereich Testereignis wie folgt vor, um Ihr Testereignis zu erstellen:
   a. Wählen Sie unter Testereignisaktion die Option Neues Ereignis erstellen aus.
   b. Geben Sie für Event name (Ereignisname) **`myTestEvent`** ein.
   c. Wählen Sie unter Vorlage die Option S3 Put aus.
   d. Ersetzen Sie die Werte für die folgenden Parameter durch Ihre eigenen Werte:

- Ersetzen Sie für durch den`awsRegion`, in `us-east-1` dem AWS-Region Sie Ihre Amazon S3 S3-Buckets erstellt haben.
- Ersetzen Sie für `name` den Wert `DOC-EXAMPLE-BUCKET` durch den Namen Ihres eigenen Amazon-S3-Quell-Buckets.
- Ersetzen Sie für `key` den Wert `test%2Fkey` durch den Dateinamen des Testobjekts, das Sie im Schritt Hochladen eines Testbilds in Ihren Quell-Bucket in Ihren Quell-Bucket hochgeladen haben.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "1970-01-01T00:00:00.000Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "EXAMPLE"
      },
      "requestParameters": {
        "sourceIPAddress": "127.0.0.1"
      },
      "responseElements": {
        "x-amz-request-id": "EXAMPLE123456789",
        "x-amz-id-2": "EXAMPLE123/5678abcdefghijklambdaisawesome/
mnopqrstuvwxyzABCDEFGH"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "testConfigRule",
        "bucket": {
          "name": "DOC-EXAMPLE-BUCKET",
          "ownerIdentity": {
            "principalId": "EXAMPLE"
          },
          "arn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        },
        "object": {
          "key": "test%2Fkey",
          "size": 1024,
```

```
            "eTag": "0123456789abcdef0123456789abcdef",
            "sequencer": "0A1B2C3D4E5F678901"
          }
        }
      }
    ]
}
```

e. Wählen Sie Speichern.

4. Wählen Sie im Bereich Testereignis die Option Testen aus.
5. Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Funktion eine verkleinerte Version Ihres Bilds erstellt und in Ihrem Amazon-S3-Ziel-Bucket gespeichert hat:

   a. Öffnen Sie die Seite Buckets der Amazon-S3-Konsole.

   b. Wählen Sie Ihren Ziel-Bucket aus und vergewissern Sie sich, dass die Datei, deren Größe angepasst wurde, im Bereich Objekte vorhanden ist.

AWS CLI

So testen Sie Ihre Lambda-Funktion mit einem Dummy-Ereignis (AWS CLI)

1. Speichern Sie den folgenden JSON-Code in einer Datei mit dem Namen `dummyS3Event.json`: Ersetzen Sie die Werte für die folgenden Parameter durch Ihre eigenen Werte:

   1. Ersetzen Sie für durch den`awsRegion`, in `us-west-2` dem AWS-Region Sie Ihre Amazon S3 S3-Buckets erstellt haben.
   2. Ersetzen Sie für `name` den Wert `DOC-EXAMPLE-SOURCE-BUCKET` durch den Namen Ihres eigenen Amazon-S3-Quell-Buckets.
   3. Ersetzen Sie für `key` den Wert `HappyFace.jpg` durch den Dateinamen des Testobjekts, das Sie im Schritt Hochladen eines Testbilds in Ihren Quell-Bucket in Ihren Quell-Bucket hochgeladen haben.

```
{
  "Records":[
    {
      "eventVersion":"2.0",
      "eventSource":"aws:s3",
```

```
      "awsRegion":"us-west-2",
      "eventTime":"1970-01-01T00:00:00.000Z",
      "eventName":"ObjectCreated:Put",
      "userIdentity":{
        "principalId":"AIDAJDPLRKLG7UEXAMPLE"
      },
      "requestParameters":{
        "sourceIPAddress":"127.0.0.1"
      },
      "responseElements":{
        "x-amz-request-id":"C3D13FE58DE4C810",
        "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
      },
      "s3":{
        "s3SchemaVersion":"1.0",
        "configurationId":"testConfigRule",
        "bucket":{
          "name":"DOC-EXAMPLE-SOURCE-BUCKET",
          "ownerIdentity":{
            "principalId":"A3NL1KOZZKExample"
          },
          "arn":"arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
        },
        "object":{
          "key":"HappyFace.jpg",
          "size":1024,
          "eTag":"d41d8cd98f00b204e9800998ecf8427e",
          "versionId":"096fKKXTRTtl3on89fVO.nfljtsv6qko"
        }
      }
    }
  ]
}
```

2. Rufen Sie die Funktion in dem Verzeichnis auf, in dem Sie die Datei `dummyS3Event.json` gespeichert haben, indem Sie den folgenden CLI-Befehl ausführen. Dieser Befehl ruft Ihre Lambda-Funktion synchron auf, indem `RequestResponse` als Wert des Parameters „invocation-type“ angegeben wird. Weitere Informationen zu synchronen und asynchronen Aufrufen finden Sie unter Aufrufen von Lambda-Funktionen.

```
aws lambda invoke --function-name CreateThumbnail \
--invocation-type RequestResponse --cli-binary-format raw-in-base64-out \
```

```
--payload file://dummyS3Event.json outputfile.txt
```

Die cli-binary-format Option ist erforderlich, wenn Sie Version 2 von verwenden. AWS CLI Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter AWS CLI - unterstützte globale Befehlszeilenoptionen.

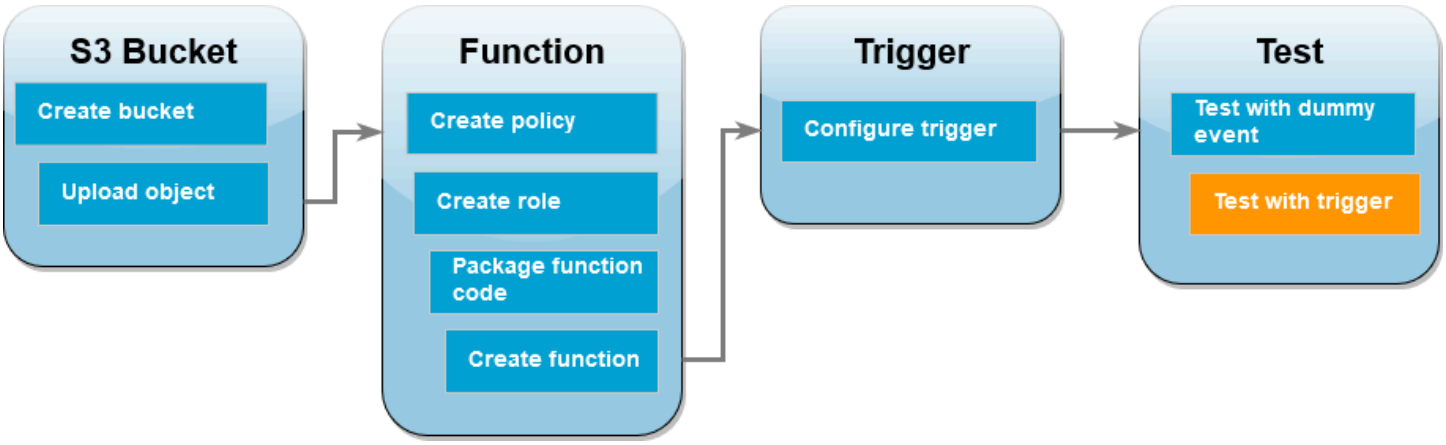
3. Vergewissern Sie sich, dass Ihre Funktion eine Miniaturversion Ihres Bilds erstellt und in Ihrem Amazon-S3-Ziel-Bucket gespeichert hat. Führen Sie den folgenden CLI-Befehl aus und ersetzen Sie dabei `DOC-EXAMPLE-SOURCE-BUCKET-resized` durch den Namen Ihres eigenen Ziel-Buckets:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-SOURCE-BUCKET-resized
```

Die Ausgabe sollte in etwa wie folgt aussehen: Der Parameter `Key` zeigt den Dateinamen Ihrer verkleinerten Bilddatei an.

```
{
    "Contents": [
        {
            "Key": "resized-HappyFace.jpg",
            "LastModified": "2023-06-06T21:40:07+00:00",
            "ETag": "\"d8ca652ffe83ba6b721ffc20d9d7174a\"",
            "Size": 2633,
            "StorageClass": "STANDARD"
        }
    ]
}
```

Testen Ihrer Funktion mit dem Amazon-S3-Auslöser



Nachdem Sie sich vergewissert haben, dass Ihre Lambda-Funktion ordnungsgemäß funktioniert, können Sie Ihr gesamtes Setup testen, indem Sie Ihrem Amazon-S3-Quell-Bucket eine Bilddatei hinzufügen. Wenn Sie Ihr Bild dem Quell-Bucket hinzufügen, sollte Ihre Lambda-Funktion automatisch aufgerufen werden. Ihre Funktion erstellt eine verkleinerte Version der Datei und speichert sie in Ihrem Ziel-Bucket.

AWS Management Console

So testen Sie Ihre Lambda-Funktion unter Verwendung des Amazon-S3-Auslösers (Konsole)

1. Gehen Sie wie folgt vor, um ein Bild in Ihren Amazon-S3-Bucket hochzuladen:
   a. Öffnen Sie die Seite Buckets der Amazon-S3-Konsole und wählen Sie Ihren Quell-Bucket aus.
   b. Klicken Sie auf Hochladen.
   c. Wählen Sie Dateien hinzufügen und anschließend über die Dateiauswahl die Bilddatei aus, die Sie hochladen möchten. Ihr Bildobjekt kann eine beliebige JPG- oder PNG-Datei sein.
   d. Wählen Sie Öffnen und anschließend Hochladen aus.
2. Vergewissern Sie sich, dass Lambda eine verkleinerte Version Ihrer Bilddatei in Ihrem Ziel-Bucket gespeichert hat:
   a. Navigieren Sie wieder zur Seite Buckets der Amazon-S3-Konsole und wählen Sie Ihren Ziel-Bucket aus.

b. Im Bereich Objekte sollten jetzt zwei verkleinerte Bilddateien angezeigt werden (jeweils eine aus den beiden Tests Ihrer Lambda-Funktion). Wählen Sie zum Herunterladen Ihres verkleinerten Bilds die Datei und anschließend Herunterladen aus.

AWS CLI

So testen Sie Ihre Lambda-Funktion unter Verwendung des Amazon-S3-Auslösers (AWS CLI)

1. Führen Sie in dem Verzeichnis, das das hochzuladende Bild enthält, den folgenden CLI-Befehl aus. Ersetzen Sie dabei den Parameter `--bucket` durch den Namen Ihres Quell-Buckets. Verwenden Sie für die Parameter `--key` und `--body` den Dateinamen Ihres Testbilds. Ihr Testbild kann eine beliebige JPG- oder PNG-Datei sein.

```
aws s3api put-object --bucket DOC-EXAMPLE-SOURCE-BUCKET --key SmileyFace.jpg --
body ./SmileyFace.jpg
```

2. Vergewissern Sie sich, dass Ihre Funktion eine Miniaturversion Ihres Bilds erstellt und in Ihrem Amazon-S3-Ziel-Bucket gespeichert hat. Führen Sie den folgenden CLI-Befehl aus und ersetzen Sie dabei `DOC-EXAMPLE-SOURCE-BUCKET-resized` durch den Namen Ihres eigenen Ziel-Buckets:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-SOURCE-BUCKET-resized
```

Wenn Ihre Funktion erfolgreich ausgeführt wird, erhalten Sie eine Ausgabe wie die folgende. Ihr Ziel-Bucket sollte jetzt zwei verkleinerte Dateien enthalten.

```
{
    "Contents": [
        {
            "Key": "resized-HappyFace.jpg",
            "LastModified": "2023-06-07T00:15:50+00:00",
            "ETag": "\"7781a43e765a8301713f533d70968a1e\"",
            "Size": 2763,
            "StorageClass": "STANDARD"
        },
        {
            "Key": "resized-SmileyFace.jpg",
            "LastModified": "2023-06-07T00:13:18+00:00",
            "ETag": "\"ca536e5a1b9e32b22cd549e18792cdbc\"",
            "Size": 1245,
```

```
            "StorageClass": "STANDARD"
        }
    ]
}
```

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die von Ihnen erstellte Richtlinie

1. Öffnen Sie die Seite Richtlinien in der IAM-Konsole.
2. Wählen Sie die Richtlinie aus, die Sie erstellt haben (AWSLambdaS3Policy).
3. Wählen Sie Policy actions (Richtlinienaktionen) und anschließend Delete (Löschen) aus.
4. Wählen Sie Löschen aus.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie den S3-Bucket:

1. Öffnen Sie die Amazon S3-Konsole.

2. Wählen Sie den Bucket aus, den Sie erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen des Buckets in das Texteingabefeld ein.
5. Wählen Sie Bucket löschen aus.

Verwendung AWS Lambda mit Amazon S3 S3-Batchoperationen

Sie können Amazon-S3-Batchvorgänge verwenden, um eine Lambda-Funktion für einen großen Satz von Amazon-S3-Objekten aufzurufen. Amazon S3 verfolgt den Fortschritt von Batchvorgängen, sendet Benachrichtigungen und speichert einen Abschlussbericht, der den Status jeder Aktion anzeigt.

Zum Ausführen eines Batchvorgangs erstellen Sie einen Amazon-S3-Batchvorgangsauftrag. Wenn Sie den Auftrag erstellen, stellen Sie ein Manifest (die Liste der Objekte) bereit und konfigurieren die Aktion für diese Objekte.

Wenn der Batchauftrag gestartet wird, ruft Amazon S3 die Lambda-Funktion synchron für jedes Objekt im Manifest auf. Der Ereignis-Parameter enthält die Namen des Buckets und des Objekts.

Das folgende Beispiel zeigt das Ereignis, das Amazon S3 an die Lambda-Funktion für ein Objekt mit dem Namen customerImage1.jpg im DOC-EXAMPLE-BUCKET-Bucket sendet.

Example Batch-Anforderungsereignis für Amazon S3

```
{
"invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
        }
    ]
}
```

Ihre Lambda-Funktion muss ein JSON-Objekt mit den Feldern zurückgeben, wie im folgenden Beispiel gezeigt. Sie können den Parameter `invocationId` und `taskId` aus dem Ereignisparameter kopieren. Sie können eine Zeichenfolge in `resultString` zurückgeben. Amazon S3 speichert die `resultString`-Werte im Abschlussbericht.

Example Batch-Anforderungantwort für Amazon S3

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Alice\", \"Bob\"]"
    }
  ]
}
```

Aufrufen von Lambda-Funktionen aus Amazon-S3-Batchvorägngen

Sie können die Lambda-Funktion mit einem nicht qualifizierten oder einem qualifizierten Funktions-ARN aufrufen. Wenn Sie dieselbe Funktionsversion für den gesamten Stapelauftrag verwenden möchten, konfigurieren Sie beim Erstellen des Auftrags eine bestimmte Funktionsversion im Parameter `FunctionARN`. Wenn Sie einen Alias oder den Qualifizierer $LATEST konfigurieren, beginnt der Stapelauftrag sofort, die neue Version der Funktion aufzurufen, wenn der Alias oder $LATEST während der Auftragsausführung aktualisiert wird.

Beachten Sie, dass Sie eine vorhandene ereignisbasierte Amazon-S3-Funktion nicht für Batchvorgänge verwenden können. Dies liegt daran, dass der Amazon-S3-Batchvorgang einen anderen Ereignisparameter an die Lambda-Funktion übergibt und eine Rückgabemeldung mit einer bestimmten JSON-Struktur erwartet.

Stellen Sie in der ressourcenbasierten Richtlinie, die Sie für den Amazon-S3-Batchauftrag erstellen, sicher, dass Sie die Berechtigung für den Auftrag zum Aufrufen der Lambda-Funktion festlegen.

Legen Sie in der Ausführungsrolle für die Funktion eine Vertrauensrichtlinie fest, damit Amazon S3 die Rolle übernimmt, wenn die Funktion ausgeführt wird.

Wenn Ihre Funktion das AWS SDK zur Verwaltung von Amazon S3 S3-Ressourcen verwendet, müssen Sie der Ausführungsrolle Amazon S3 S3-Berechtigungen hinzufügen.

Wenn der Auftrag ausgeführt wird, startet Amazon S3 mehrere Funktionsinstances, um die Amazon-S3-Objekte bis zur Parallelitätsgrenze der Funktion parallel zu verarbeiten. Amazon S3 begrenzt den anfänglichen Hochlauf von Instances, um Überkosten für kleinere Aufträge zu vermeiden.

Wenn die Lambda-Funktion den Antwortcode `TemporaryFailure` zurückgibt, wiederholt Amazon S3 den Vorgang.

Weitere Informationen zu Amazon-S3-Stapelvorgängen finden Sie unter Durchführen von Stapelvorgängen im Amazon-S3-Entwicklerhandbuch.

Ein Beispiel für die Verwendung einer Lambda-Funktion in Amazon-S3-Stapelvorgängen finden Sie unter Aufrufen einer Lambda-Funktion von Amazon-S3-Stapelvorgängen im Amazon-S3-Entwicklerhandbuch.

Transformieren von S3-Objekten mit S3 Objekt Lambda

Mit S3 Object Lambda können Sie Ihren eigenen Code zu Amazon S3 GET-, HEAD- und LIST-Anfragen hinzufügen, um Daten zu ändern und zu verarbeiten, bevor sie an eine Anwendung zurückgegeben werden. Sie können benutzerdefinierten Code verwenden, um die von Standard-S3-GET-, HEAD- oder LIST-Anfragen zurückgegebenen Daten zu ändern, um Zeilen zu filtern, die Größe von Images dynamisch anzupassen, vertrauliche Daten zu unterdrücken und vieles mehr. Unterstützt von AWS-Lambda-Funktionen wird Ihr Code in einer Infrastruktur ausgeführt, die vollständig von AWS verwaltet wird, sodass keine abgeleiteten Kopien Ihrer Daten erstellt und gespeichert oder Proxys ausgeführt werden müssen. Und all das ohne erforderliche Änderungen an den Anwendungen.

Weitere Informationen finden Sie unte rTransformieren von Objekten mit S3-Objekt Lambda.

Tutorials

- Umwandlung von Daten für Ihre Anwendung mit Amazon S3 Object Lambda
- Erkennen und Schwärzen von PII-Daten mit Amazon S3 Object Lambda und Amazon Comprehend
- Verwenden von Amazon S3 Object Lambda, um Bilder beim Abrufen dynamisch mit Wasserzeichen zu versehen

Verwendung von AWS Lambda mit Secrets Manager

Ihre AWS Lambda-Funktion kann mit AWS Secrets Manager mithilfe der Secrets-Manager-API oder einem der AWS Software Development Kits (SDKs) interagieren. Sie können die Lambda-Erweiterung von AWS-Parametern und Geheimnissen auch verwenden, um AWS Secrets Manager-Geheimnisse in Lambda-Funktionen abzurufen und im Cache zu speichern, ohne ein SDK zu verwenden. Weitere Informationen finden Sie unter Verwenden von AWS Secrets Manager-Geheimnissen inAWS Lambda-Funktionen.

Verwenden von AWS Lambda mit Amazon SES

Wenn Sie Amazon SES zum Empfangen von Nachrichten verwenden, können Sie Amazon SES so konfigurieren, dass Ihre Lambda-Funktion beim Eintreffen von Nachrichten aufgerufen wird. Der Service kann dann Ihre Lambda-Funktion aufrufen, indem das eingehende E-Mail-Ereignis, bei dem es sich um eine Amazon-SES-Nachricht in einem Amazon-SNS-Ereignis handelt, als Parameter übergeben wird.

Example Amazon-SES-Nachrichtenereignis

```
{
  "Records": [
    {
      "eventVersion": "1.0",
      "ses": {
        "mail": {
          "commonHeaders": {
            "from": [
              "Jane Doe <janedoe@example.com>"
            ],
            "to": [
              "johndoe@example.com"
            ],
            "returnPath": "janedoe@example.com",
            "messageId": "<0123456789example.com>",
            "date": "Wed, 7 Oct 2015 12:34:56 -0700",
            "subject": "Test Subject"
          },
          "source": "janedoe@example.com",
          "timestamp": "1970-01-01T00:00:00.000Z",
          "destination": [
            "johndoe@example.com"
          ],
          "headers": [
            {
              "name": "Return-Path",
              "value": "<janedoe@example.com>"
            },
            {
              "name": "Received",
```

```
            "value": "from mailer.example.com (mailer.example.com [203.0.113.1])
 by inbound-smtp.us-west-2.amazonaws.com with SMTP id o3vrnil0e2ic for
 johndoe@example.com; Wed, 07 Oct 2015 12:34:56 +0000 (UTC)"
          },
          {
            "name": "DKIM-Signature",
            "value": "v=1; a=rsa-sha256; c=relaxed/relaxed; d=example.com;
 s=example; h=mime-version:from:date:message-id:subject:to:content-type;
 bh=jX3F0bCAI7sIbkHyy3mLYO28ieDQz2R0P8HwQkklFj4=; b=sQwJ+LMe9RjkesGu
+vqU56asvMhrLRRYrWCbV"
          },
          {
            "name": "MIME-Version",
            "value": "1.0"
          },
          {
            "name": "From",
            "value": "Jane Doe <janedoe@example.com>"
          },
          {
            "name": "Date",
            "value": "Wed, 7 Oct 2015 12:34:56 -0700"
          },
          {
            "name": "Message-ID",
            "value": "<0123456789example.com>"
          },
          {
            "name": "Subject",
            "value": "Test Subject"
          },
          {
            "name": "To",
            "value": "johndoe@example.com"
          },
          {
            "name": "Content-Type",
            "value": "text/plain; charset=UTF-8"
          }
        ],
        "headersTruncated": false,
        "messageId": "o3vrnil0e2ic28tr"
      },
      "receipt": {
```

```
          "recipients": [
            "johndoe@example.com"
          ],
          "timestamp": "1970-01-01T00:00:00.000Z",
          "spamVerdict": {
            "status": "PASS"
          },
          "dkimVerdict": {
            "status": "PASS"
          },
          "processingTimeMillis": 574,
          "action": {
            "type": "Lambda",
            "invocationType": "Event",
            "functionArn": "arn:aws:lambda:us-west-2:111122223333:function:Example"
          },
          "spfVerdict": {
            "status": "PASS"
          },
          "virusVerdict": {
            "status": "PASS"
          }
        }
      },
      "eventSource": "aws:ses"
    }
  ]
}
```

Weitere Informationen finden Sie unter Lambda-Aktion im Amazon-SES-Entwicklerhandbuch.

Aufrufen von Lambda-Funktionen mit Amazon SNS SNS-Benachrichtigungen

Verwenden Sie eine Lambda-Funktion, um Amazon-Simple-Notification-Service-(Amazon-SNS)-Benachrichtigungen zu verarbeiten. Amazon SNS unterstützt Lambda-Funktionen als Ziel für Nachrichten, die an ein Thema gesendet werden. Sie können Ihre Funktion für Themen in demselben Konto oder in anderen AWS -Konten abonnieren. Eine ausführliche exemplarische Vorgehensweise finden Sie unter the section called “Tutorial”.

Lambda unterstützt SNS-Trigger nur für Standard-SNS-Themen. FIFO-Themen werden nicht unterstützt.

Bei asynchronen Aufrufe legt Lambda die Nachricht in eine Warteschlange und verarbeitet Wiederholungen. Wenn Amazon SNS Lambda nicht erreichen kann, oder die Nachricht abgelehnt wird, wiederholt Amazon SNS den Vorgang in zunehmenden Intervallen über mehrere Stunden. Weitere Details finden Sie unter Zuverlässigkeit in den häufig gestellten Fragen zu Amazon SNS.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

Themen

Hinzufügen eines Amazon SNS SNS-Themenauslösers für eine Lambda-Funktion mithilfe der Konsole

Um ein SNS-Thema als Auslöser für eine Lambda-Funktion hinzuzufügen, verwenden Sie am einfachsten die Lambda-Konsole. Wenn Sie den Trigger über die Konsole hinzufügen, richtet Lambda automatisch die erforderlichen Berechtigungen und Abonnements ein, um Ereignisse aus dem SNS-Thema zu empfangen.

Um ein SNS-Thema als Auslöser für eine Lambda-Funktion hinzuzufügen (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion, für die Sie den Auslöser hinzufügen möchten.
3. Wählen Sie Konfiguration und dann Trigger.
4. Wählen Sie Add trigger.
5. Wählen Sie im Dropdownmenü unter Trigger-Konfiguration die Option SNS aus.
6. Wählen Sie unter SNS-Thema das SNS-Thema aus, das Sie abonnieren möchten.

Manuelles Hinzufügen eines Amazon SNS SNS-Themenauslösers für eine Lambda-Funktion

Um einen SNS-Trigger für eine Lambda-Funktion manuell einzurichten, müssen Sie die folgenden Schritte ausführen:

- Definieren Sie eine ressourcenbasierte Richtlinie für Ihre Funktion, damit SNS sie aufrufen kann.
- Abonnieren Sie Ihre Lambda-Funktion für das Amazon SNS SNS-Thema.

> **Note**
>
> Wenn sich Ihr SNS-Thema und Ihre Lambda-Funktion in unterschiedlichen AWS Konten befinden, müssen Sie auch zusätzliche Berechtigungen gewähren, um kontoübergreifende Abonnements für das SNS-Thema zuzulassen. Weitere Informationen finden Sie unter Kontenübergreifende Berechtigungen für ein Amazon SNS SNS-Abonnement gewähren.

Sie können die Taste AWS Command Line Interface (AWS CLI) verwenden, um diese beiden Schritte abzuschließen. Verwenden Sie zunächst den folgenden Befehl, um eine ressourcenbasierte Richtlinie

für eine Lambda-Funktion zu definieren, die SNS-Aufrufe zulässt. AWS CLI Achten Sie darauf, den Wert von `--function-name` durch Ihren Lambda-Funktionsnamen und den Wert von `--source-arn` durch Ihren SNS-Thema-ARN zu ersetzen.

```
aws lambda add-permission --function-name example-function \
    --source-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \
    --statement-id function-with-sns --action "lambda:InvokeFunction" \
    --principal sns.amazonaws.com
```

Verwenden Sie den folgenden Befehl, um das SNS-Thema für Ihre Funktion zu abonnieren. AWS CLI Ersetzen Sie den Wert von `--topic-arn` durch Ihren SNS-Thema-ARN und den Wert von `--notification-endpoint` durch Ihren Lambda-Funktions-ARN.

```
aws sns subscribe --protocol lambda \
    --region us-east-1 \
    --topic-arn arn:aws:sns:us-east-1:123456789012:sns-topic-for-lambda \
    --notification-endpoint arn:aws:lambda:us-east-1:123456789012:function:example-
function
```

Beispiel für eine SNS-Ereignisform

Amazon SNS ruft Ihre Funktion asynchron mit einem Ereignis auf, das eine Nachricht und Metadaten enthält.

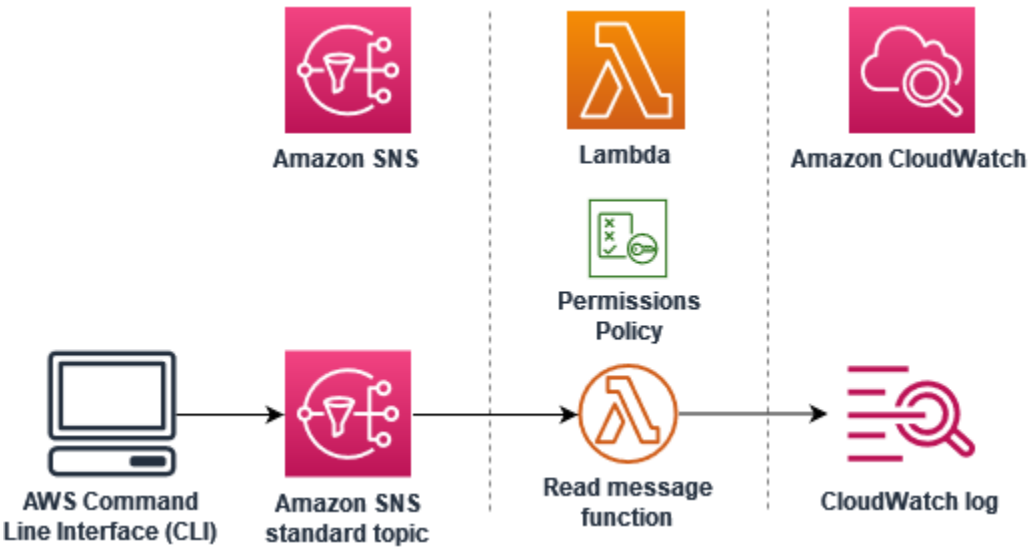
Example Amazon-SNS-Nachrichtenereignis

```
{
  "Records": [
    {
      "EventVersion": "1.0",
      "EventSubscriptionArn": "arn:aws:sns:us-east-1:123456789012:sns-lambda:21be56ed-
a058-49f5-8c98-aedd2564c486",
      "EventSource": "aws:sns",
      "Sns": {
        "SignatureVersion": "1",
        "Timestamp": "2019-01-02T12:45:07.000Z",
        "Signature": "tcc6faL2yUC6dgZdmrwh1Y4cGa/ebXEkAi6RibDsvpi+tE/1+82j...65r==",
        "SigningCertURL": "https://sns.us-east-1.amazonaws.com/
SimpleNotificationService-ac565b8b1a6c5d002d285f9598aa1d9b.pem",
        "MessageId": "95df01b4-ee98-5cb9-9903-4c221d41eb5e",
        "Message": "Hello from SNS!",
```

```
        "MessageAttributes": {
          "Test": {
            "Type": "String",
            "Value": "TestString"
          },
          "TestBinary": {
            "Type": "Binary",
            "Value": "TestBinary"
          }
        },
        "Type": "Notification",
        "UnsubscribeURL": "https://sns.us-east-1.amazonaws.com/?
Action=Unsubscribe&amp;SubscriptionArn=arn:aws:sns:us-east-1:123456789012:test-
lambda:21be56ed-a058-49f5-8c98-aedd2564c486",
        "TopicArn":"arn:aws:sns:us-east-1:123456789012:sns-lambda",
        "Subject": "TestInvoke"
      }
    }
  ]
}
```

Tutorial: Verwendung AWS Lambda mit Amazon Simple Notification Service

In diesem Tutorial verwenden Sie eine Lambda-Funktion in einem, AWS-Konto um ein Amazon Simple Notification Service (Amazon SNS) -Thema in einem separaten zu abonnieren. AWS-Konto Wenn Sie Nachrichten zu Ihrem Amazon SNS SNS-Thema veröffentlichen, liest Ihre Lambda-Funktion den Inhalt der Nachricht und gibt ihn in Amazon CloudWatch Logs aus. Um dieses Tutorial abzuschließen, verwenden Sie die AWS Command Line Interface ()AWS CLI.



Gehen Sie für dieses Tutorial wie folgt vor:

- Erstellen Sie in Konto A ein Amazon-SNS-Thema.
- Erstellen Sie in Konto B eine Lambda-Funktion, die Nachrichten aus dem Thema liest.
- Erstellen Sie in Konto B ein Abonnement für das Thema.
- Veröffentlichen Sie Nachrichten zum Amazon SNS SNS-Thema in Konto A und stellen Sie sicher, dass die Lambda-Funktion in Konto B sie in Logs ausgibt. CloudWatch

Anhand dieser Schritte lernen Sie, wie Sie ein Amazon-SNS-Thema konfigurieren, um eine Lambda-Funktion aufzurufen. Sie erfahren auch, wie Sie eine AWS Identity and Access Management (IAM-) Richtlinie erstellen, die einer Ressource in einer anderen die Erlaubnis erteilt AWS-Konto , Lambda aufzurufen.

In dem Tutorial werden zwei separate AWS-Konten verwendet. Die AWS CLI Befehle veranschaulichen dies anhand von zwei benannten Profilen`accountB`, die aufgerufen `accountA` und jeweils für die Verwendung mit einem anderen konfiguriert sind. AWS-Konto Informationen zur Konfiguration der AWS CLI Verwendung verschiedener Profile finden Sie unter Einstellungen für Konfiguration und Anmeldeinformationsdatei im AWS Command Line Interface Benutzerhandbuch für Version 2. Stellen Sie sicher, dass Sie AWS-Region für beide Profile dieselbe Standardeinstellung konfigurieren.

Wenn die AWS CLI Profile, die Sie für die beiden erstellen, unterschiedliche Namen AWS-Konten verwenden oder wenn Sie das Standardprofil und ein benanntes Profil verwenden, ändern Sie die AWS CLI Befehle in den folgenden Schritten nach Bedarf.

Voraussetzungen

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

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

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

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Installieren Sie das AWS Command Line Interface

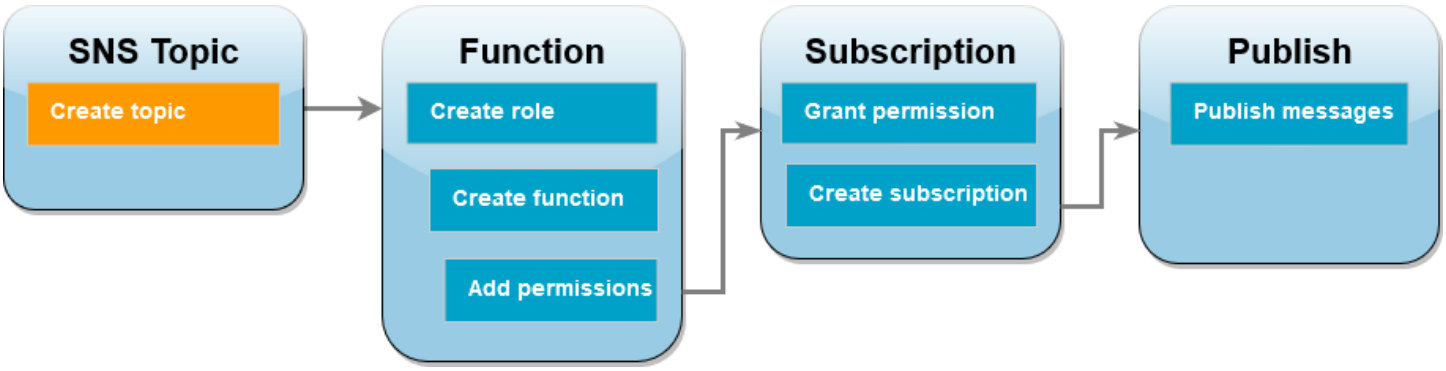
Wenn Sie das noch nicht installiert haben AWS Command Line Interface, folgen Sie den Schritten unter Installieren oder Aktualisieren der neuesten Version von AWS CLI, um es zu installieren.

Das Tutorial erfordert zum Ausführen von Befehlen ein Befehlszeilenterminal oder eine Shell. Verwenden Sie unter Linux und macOS Ihre bevorzugte Shell und Ihren bevorzugten Paketmanager.

> **Note**
>
> In Windows werden einige Bash-CLI-Befehle, die Sie häufig mit Lambda verwenden (z. B. `zip`), von den integrierten Terminals des Betriebssystems nicht unterstützt. Um eine in

Windows integrierte Version von Ubuntu und Bash zu erhalten, installieren Sie das Windows-Subsystem für Linux.

Erstellen eines Amazon-SNS-Themas (Konto A)



So erstellen Sie das -Thema

- Erstellen Sie in Konto A mit dem folgenden AWS CLI Befehl ein Amazon SNS SNS-Standardthema.

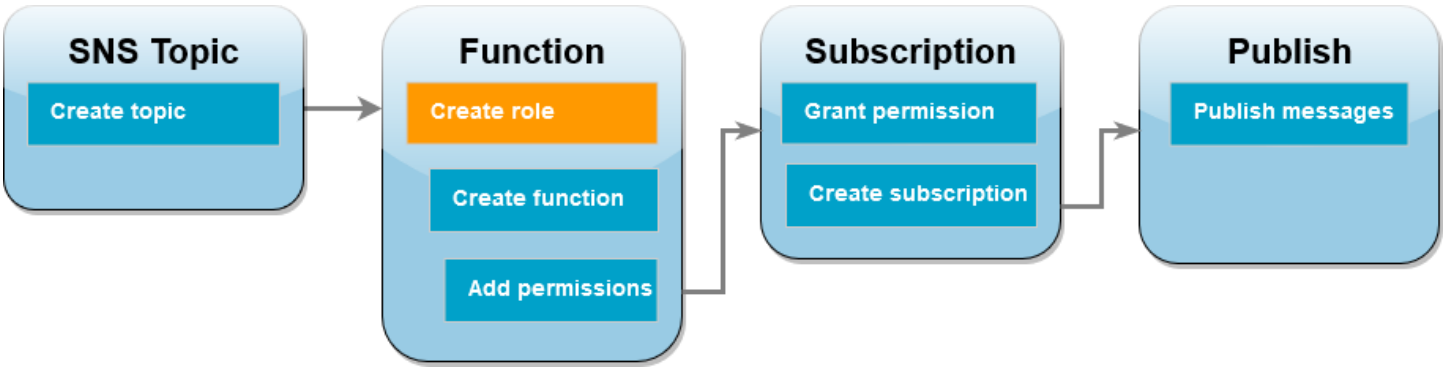
  ```
  aws sns create-topic --name sns-topic-for-lambda --profile accountA
  ```

  Die Ausgabe sollte in etwa wie folgt aussehen:

  ```
  {
      "TopicArn": "arn:aws:sns:us-west-2:123456789012:sns-topic-for-lambda"
  }
  ```

  Notieren Sie sich den Amazon-Ressourcennamen (ARN) Ihres Themas. Sie benötigen ihn im weiteren Verlauf des Tutorials, wenn Sie Ihrer Lambda-Funktion Berechtigungen zum Abonnieren des Themas hinzufügen.

Erstellen einer Funktionsausführungsrolle (Konto B)

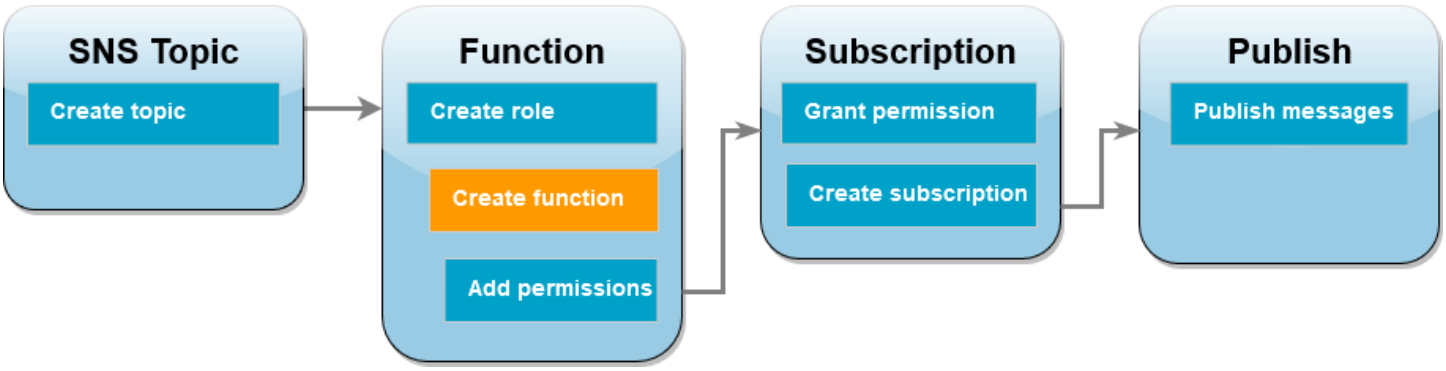


Eine Ausführungsrolle ist eine IAM-Rolle, die einer Lambda-Funktion die Berechtigung zum Zugriff auf AWS Dienste und Ressourcen gewährt. Bevor Sie Ihre Funktion in Konto B erstellen, erstellen Sie eine Rolle, die der Funktion grundlegende Berechtigungen zum Schreiben von Protokollen in Logs erteilt. CloudWatch Die Berechtigungen zum Lesen aus Ihrem Amazon-SNS-Thema werden in einem späteren Schritt hinzugefügt.

So erstellen Sie eine Ausführungsrolle

1. Öffnen Sie in Konto B die Seite Rollen in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
4. Wählen Sie unter Anwendungsfall die Option Lambda aus.
5. Wählen Sie Weiter aus.
6. Fügen Sie der Rolle wie folgt eine Richtlinie mit grundlegenden Berechtigungen hinzu:
    a. Geben Sie im Suchfeld Berechtigungsrichtlinien die Zeichenfolge **`AWSLambdaBasicExecutionRole`** ein.
    b. Wählen Sie Weiter aus.
7. Schließen Sie die Rollenerstellung ab:
    a. Geben Sie unter Rollendetails im Feld Rollenname den Namen **`lambda-sns-role`** ein.
    b. Wählen Sie Rolle erstellen aus.

Erstellen einer Lambda-Funktion (Konto B)



Erstellen Sie eine Lambda-Funktion, die Ihre Amazon-SNS-Nachrichten verarbeitet. Der Funktionscode protokolliert den Nachrichteninhalt jedes Datensatzes in Amazon CloudWatch Logs.

In diesem Tutorial wird die Node.js 18.x-Laufzeit verwendet. Es stehen aber auch Beispielcodes für andere Laufzeitensprachen zur Verfügung. Sie können die Registerkarte im folgenden Feld auswählen, um Code für die gewünschte Laufzeit anzusehen. Der JavaScript Code, den Sie in diesem Schritt verwenden, befindet sich im ersten Beispiel, das auf der JavaScriptRegisterkarte angezeigt wird.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
```

```
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SnsIntegration;

public class Function
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
        foreach (var record in evnt.Records)
        {
            await ProcessRecordAsync(record, context);
        }
        context.Logger.LogInformation("done");
    }

    private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed record
 {record.Sns.Message}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
 for _, record := range snsEvent.Records {
  processMessage(record)
 }
 fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
 message := record.SNS.Message
 fmt.Printf("Processed message: %s\n", message)
 // TODO: Process your record here
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines SNS-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;


import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }

    public void processRecord(SNSRecord record) {
```

```
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines SNS-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record) {
  try {
    const message = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
```

```
    throw err;
  }
}
```

Konsumieren eines SNS-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";

export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record: SNSEventRecord): Promise<any> {
  try {
    const message: string = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
 PHP functions runtime for AWS Lambda.
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-
lambda-custom-runtime-for-php-a-practical-example/
*/

// Additional composer packages may be required when using Bref or any other PHP
 functions runtime.
// require __DIR__ . '/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Sns\SnsEvent;
use Bref\Event\Sns\SnsHandler;

class Handler extends SnsHandler
{
    public function handleSns(SnsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $message = $record->getMessage();

            // TODO: Implement your custom processing logic here
            // Any exception thrown will be logged and the invocation will be
 marked as failed

            echo "Processed Message: $message" . PHP_EOL;
        }
    }
}

return new Handler();
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines SNS-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].map { |record| process_message(record) }
end

def process_message(record)
  message = record['Sns']['Message']
  puts("Processing message: #{message}")
rescue StandardError => e
  puts("Error processing message: #{e}")
  raise
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Rust

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
//  aws_lambda_events = { version = "0.10.0", default-features = false, features
 = ["sns"] }
//  lambda_runtime = "0.8.1"
//  tokio = { version = "1", features = ["macros"] }
```

```
//  tracing = { version = "0.1", features = ["log"] }
//  tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for event in event.payload.records {
        process_record(&event)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);

    // Implement your record handling code here.

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

So erstellen Sie die Funktion

1. Erstellen Sie ein Verzeichnis für das Projekt und wechseln Sie dann zu diesem Verzeichnis.

```
mkdir sns-tutorial
cd sns-tutorial
```

2. Kopieren Sie den JavaScript Beispielcode in eine neue Datei mit dem Namen`index.js`.
3. Erstellen Sie ein Bereitstellungspaket mit dem folgenden `zip`-Befehl.

```
zip function.zip index.js
```

4. Führen Sie den folgenden AWS CLI Befehl aus, um Ihre Lambda-Funktion in Konto B zu erstellen.

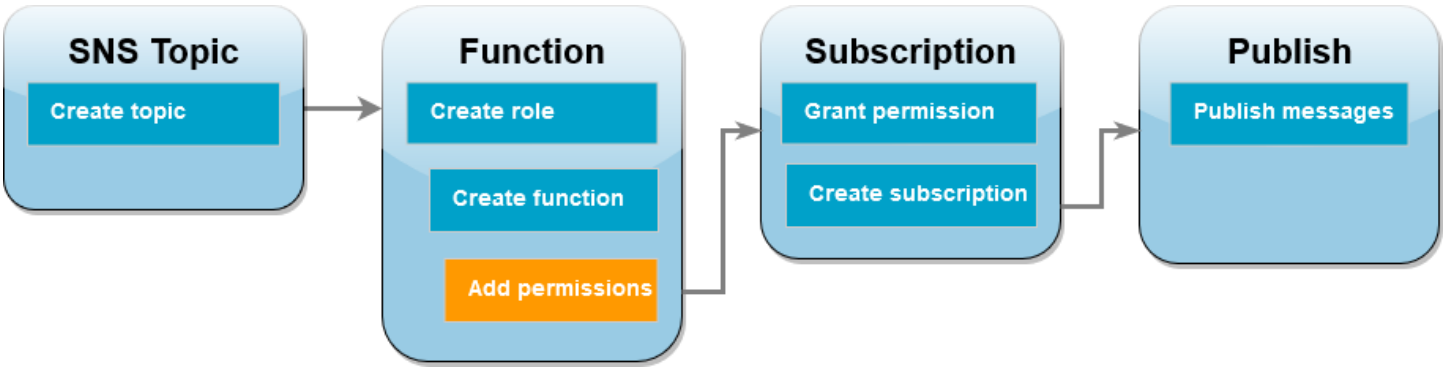
```
aws lambda create-function --function-name Function-With-SNS \
    --zip-file fileb://function.zip --handler index.handler --runtime nodejs18.x \
    --role arn:aws:iam::<AccountB_ID>:role/lambda-sns-role  \
    --timeout 60 --profile accountB
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "FunctionName": "Function-With-SNS",
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:Function-With-
SNS",
    "Runtime": "nodejs18.x",
    "Role": "arn:aws:iam::123456789012:role/lambda_basic_role",
    "Handler": "index.handler",
    ...
    "RuntimeVersionConfig": {
        "RuntimeVersionArn": "arn:aws:lambda:us-
west-2::runtime:7d5f06b69c951da8a48b926ce280a9daf2e8bb1a74fc4a2672580c787d608206"
    }
}
```

5. Notieren Sie sich den Amazon-Ressourcennamen (ARN) Ihrer Funktion. Sie benötigen ihn im weiteren Verlauf des Tutorials, wenn Sie Berechtigungen hinzufügen, um Amazon SNS das Aufrufen Ihrer Funktion zu ermöglichen.

Hinzufügen von Berechtigungen zur Funktion (Konto B)



Damit Amazon SNS Ihre Funktion aufrufen kann, muss die dafür notwendige Berechtigung in einer Anweisung einer ressourcenbasierten Richtlinie erteilt werden. Sie fügen diese Anweisung mit dem AWS CLI `add-permission` Befehl hinzu.

Erteilen der Berechtigung zum Aufrufen Ihrer Funktion durch Amazon SNS

- Führen Sie in Konto B den folgenden AWS CLI Befehl mit dem ARN für Ihr Amazon SNS SNS-Thema aus, das Sie zuvor aufgezeichnet haben.

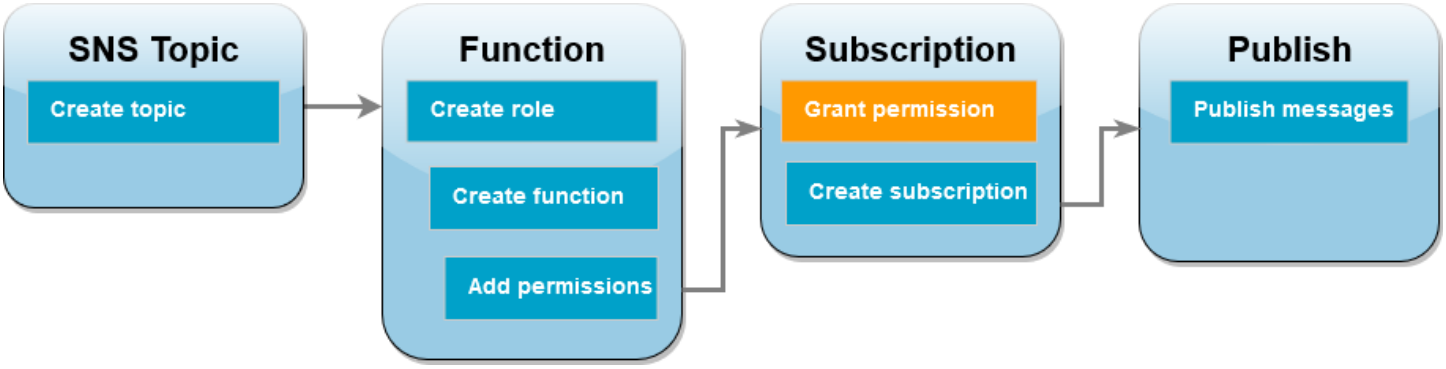
```
aws lambda add-permission --function-name Function-With-SNS \
    --source-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --statement-id function-with-sns --action "lambda:InvokeFunction" \
    --principal sns.amazonaws.com --profile accountB
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "Statement": "{\"Condition\":{\"ArnLike\":{\"AWS:SourceArn\":
      \"arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda\"}},
      \"Action\":[\"lambda:InvokeFunction\"],
      \"Resource\":\"arn:aws:lambda:us-east-1:<AccountB_ID>:function:Function-With-
SNS\",
      \"Effect\":\"Allow\",\"Principal\":{\"Service\":\"sns.amazonaws.com\"},
      \"Sid\":\"function-with-sns\"}"
}
```

> **Note**
>
> Wenn das Konto mit dem Amazon SNS SNS-Thema in einem Opt-In gehostet wird AWS-Region, müssen Sie die Region im Prinzipal angeben. Wenn Sie beispielsweise mit einem Amazon-SNS-Thema in der Region Asien-Pazifik (Hongkong) arbeiten, muss für den Prinzipal `sns.ap-east-1.amazonaws.com` anstelle von `sns.amazonaws.com` angegeben werden.

Erteilen einer kontoübergreifenden Berechtigung für das Amazon-SNS-Abonnement (Konto A)



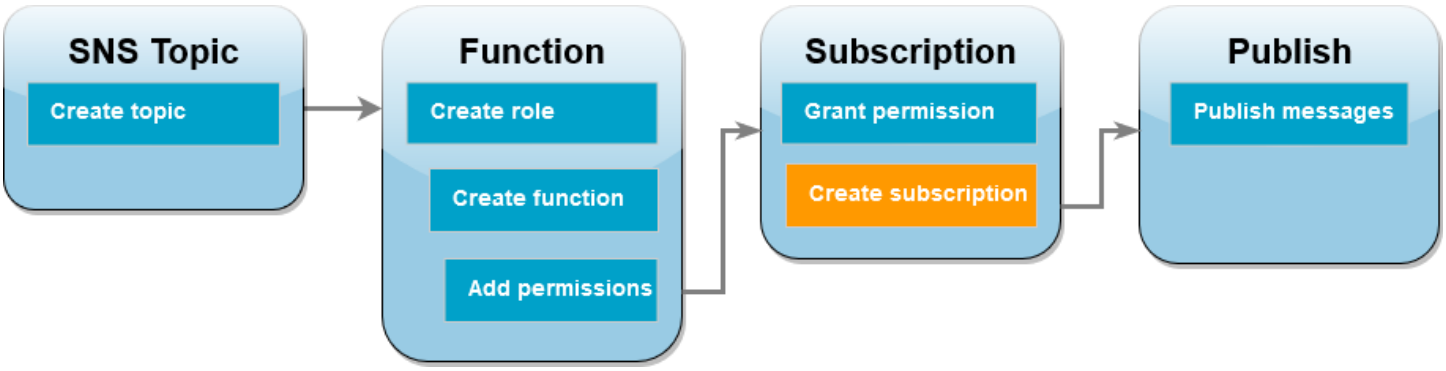
Damit Ihre Lambda-Funktion in Konto B das Amazon-SNS-Thema abonnieren kann, das Sie in Konto A erstellt haben, müssen Sie Konto B die Berechtigung zum Abonnieren Ihres Themas erteilen. Sie erteilen diese Berechtigung mit dem AWS CLI `add-permission` Befehl.

Erteilen der Berechtigung zum Abonnieren des Themas durch Konto B

- Führen Sie in Konto A den folgenden AWS CLI Befehl aus. Verwenden Sie den ARN für das Amazon-SNS-Thema, den Sie sich zuvor notiert haben.

```
aws sns add-permission --label lambda-access --aws-account-id <AccountB_ID> \
    --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --action-name Subscribe ListSubscriptionsByTopic --profile accountA
```

Erstellen eines Abonnements (Konto B)



In Konto B abonnieren Sie nun für Ihre Lambda-Funktion das Amazon-SNS-Thema, das Sie zu Beginn des Tutorials in Konto A erstellt haben. Wenn eine Nachricht an dieses Thema (`sns-topic-for-lambda`) gesendet wird, ruft Amazon SNS Ihre Lambda-Funktion `Function-With-SNS` in Konto B auf.

Erstellen eines Abonnements

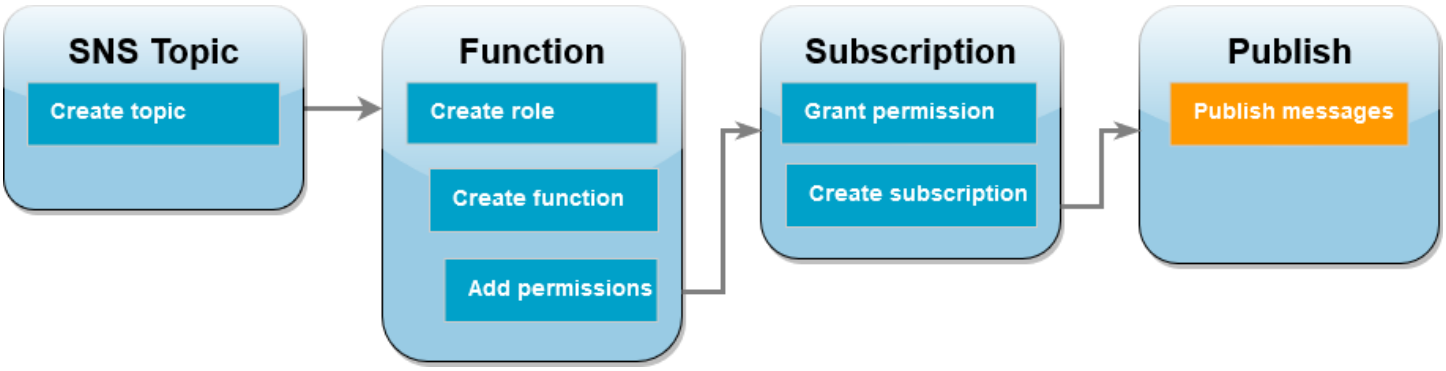
- Führen Sie in Konto B den folgenden AWS CLI Befehl aus. Verwenden Sie Ihre Standardregion, in der Sie Ihr Thema erstellt haben, sowie die ARNs für Ihr Thema und Ihre Lambda-Funktion.

```
aws sns subscribe --protocol lambda \
    --region us-east-1 \
    --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
    --notification-endpoint arn:aws:lambda:us-
east-1:<AccountB_ID>:function:Function-With-SNS \
    --profile accountB
```

  Die Ausgabe sollte in etwa wie folgt aussehen:

```
{
    "SubscriptionArn": "arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-
lambda:5d906xxxx-7c8x-45dx-a9dx-0484e31c98xx"
}
```

Veröffentlichen von Nachrichten für das Thema (Konto A und Konto B)



Ihre Lambda-Funktion in Konto B hat nun Ihr Amazon-SNS-Thema in Konto A abonniert und Sie können Ihr Setup testen, indem Sie Nachrichten für das Thema veröffentlichen. Um zu bestätigen, dass Amazon SNS Ihre Lambda-Funktion aufgerufen hat, verwenden Sie CloudWatch Logs, um die Ausgabe Ihrer Funktion anzusehen.

Veröffentlichen einer Nachricht für Ihr Thema und Anzeigen der Ausgabe Ihrer Funktion

1. Geben Sie `Hello World` in eine Textdatei ein und speichern Sie sie als `message.txt`.
2. Führen Sie aus demselben Verzeichnis, in dem Sie Ihre Textdatei gespeichert haben, den folgenden AWS CLI Befehl in Konto A aus. Verwenden Sie den ARN für Ihr eigenes Thema.

   ```
   aws sns publish --message file://message.txt --subject Test \
       --topic-arn arn:aws:sns:us-east-1:<AccountA_ID>:sns-topic-for-lambda \
       --profile accountA
   ```

   Dadurch wird eine eindeutige Nachrichten-ID zurückgegeben, die angibt, dass Amazon SNS die Nachricht akzeptiert hat. Anschließend versucht Amazon SNS, die Nachricht den Abonnenten des Themas zuzustellen. Um zu bestätigen, dass Amazon SNS Ihre Lambda-Funktion aufgerufen hat, verwenden Sie CloudWatch Logs, um die Ausgabe Ihrer Funktion einzusehen:
3. Öffnen Sie in Konto B die Seite Protokollgruppen der CloudWatch Amazon-Konsole.
4. Wählen Sie die Protokollgruppe für Ihre Funktion (`/aws/lambda/Function-With-SNS`) aus.
5. Wählen Sie den neuesten Protokollstreams aus.
6. Wenn Ihre Funktion korrekt aufgerufen wurde, sieht die Ausgabe in etwa wie folgt aus und enthält die Inhalte der Nachricht, die Sie für Ihr Thema veröffentlicht haben.

   ```
   2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO Processed
    message Hello World
   ```

```
2023-07-31T21:42:51.250Z c1cba6b8-ade9-4380-aa32-d1a225da0e48 INFO done
```

Bereinigen Ihrer Ressourcen

Sie können jetzt die Ressourcen, die Sie für dieses Tutorial erstellt haben, löschen, es sei denn, Sie möchten sie behalten. Durch das Löschen von AWS Ressourcen, die Sie nicht mehr verwenden, vermeiden Sie unnötige Kosten für Ihre AWS-Konto.

Bereinigen Sie über Konto A Ihr Amazon-SNS-Thema.

So löschen Sie das Amazon-SNS-Thema

1. Öffnen Sie die Seite Themen der Amazon-SNS-Konsole.
2. Wählen Sie das Thema aus, das Sie gerade erstellt haben.
3. Wählen Sie Löschen aus.
4. Geben Sie **`delete me`** in das Texteingabefeld ein.
5. Wählen Sie Löschen aus.

Bereinigen Sie über Konto B Ihre Ausführungsrolle, die Lambda-Funktion und das Amazon-SNS-Abonnement.

So löschen Sie die Ausführungsrolle

1. Öffnen Sie die Seite Roles in der IAM-Konsole.
2. Wählen Sie die von Ihnen erstellte Ausführungsrolle aus.
3. Wählen Sie Löschen aus.
4. Geben Sie den Namen der Rolle in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

So löschen Sie das Amazon-SNS-Abonnement

1. Öffnen Sie die Seite Abonnements der Amazon-SNS-Konsole.
2. Wählen Sie das von Ihnen erstellte Abonnement aus.
3. Wählen Sie Löschen, Löschen aus.

Bewährte Methoden für die Arbeit mit AWS Lambda Funktionen

Im Folgenden finden Sie einige bewährte Methoden für die Verwendung vo AWS Lambda:

Themen

Weitere Informationen zu bewährten Methoden für Lambda-Anwendungen finden Sie bei Serverless Land unter Application design. Sie können sich auch an Ihr AWS Account-Team wenden und eine Architekturprüfung beantragen.

Funktionscode

- Trennen Sie den Lambda-Handler von Ihrer Core-Logik. Auf diese Weise können Sie eine Funktion zur besseren Prüfbarkeit von Einheiten schaffen. In Node.js kann dies etwa wie folgt aussehen:

```
exports.myHandler = function(event, context, callback) {
 var foo = event.foo;
 var bar = event.bar;
 var result = MyLambdaFunction (foo, bar);

 callback(null, result);
}

function MyLambdaFunction (foo, bar) {
 // MyLambdaFunction logic here
}
```

- Nutzen Sie die Wiederverwendung der Ausführungsumgebung zur Verbesserung Ihrer Funktion. Initialisieren Sie SDK-Clients und Datenbankverbindungen außerhalb des Funktions-Handlers und

speichern Sie statische Komponenten lokal im `/tmp`-Verzeichnis. Nachfolgende Aufrufe, die von derselben Instance Ihrer Funktion verarbeitet werden, können diese Ressourcen wiederverwenden. Dies spart Kosten durch Reduzierung der Funktionslaufzeit.

Um potenzielle Datenlecks über Aufrufe hinweg zu vermeiden, verwenden Sie die Ausführungsumgebung nicht, um Benutzerdaten, Ereignisse oder andere Informationen mit Sicherheitsauswirkungen zu speichern. Wenn Ihre Funktion auf einem veränderbaren Zustand beruht, der nicht im Speicher innerhalb des Handlers gespeichert werden kann, sollten Sie für jeden Benutzer eine separate Funktion oder separate Versionen einer Funktion erstellen.

- Verwenden Sie eine Keep-Alive-Direktive, um dauerhafte Verbindungen zu pflegen. Lambda bereinigt Leerlaufverbindungen im Laufe der Zeit. Der Versuch, eine Leerlaufverbindung beim Aufruf einer Funktion wiederzuverwenden, führt zu einem Verbindungsfehler. Um Ihre persistente Verbindung aufrechtzuerhalten, verwenden Sie die Keep-Alive-Direktive, die Ihrer Laufzeit zugeordnet ist. Ein Beispiel finden Sie unter Wiederverwenden von Verbindungen mit Keep-Alive in Node.js.
- Verwenden Sie Umgebungsvariablen um Betriebsparameter an Ihre Funktion zu übergeben. Wenn Sie z. B. Daten in einen Amazon-S3-Bucket schreiben, anstatt den Bucket-Namen, in den Sie schreiben, hartzucodieren, konfigurieren Sie den Bucket-Namen als Umgebungsvariable.
- Kontrollieren Sie die Abhängigkeiten im Bereitstellungspaket Ihrer Funktion. Die AWS Lambda Ausführungsumgebung enthält eine Reihe von Bibliotheken wie das AWS SDK für die Node.js- und Python-Laufzeiten (eine vollständige Liste finden Sie hier:Lambda-Laufzeiten). Um die neuesten Funktionen und Sicherheitsupdates zu aktivieren, wird Lambda diese Bibliotheken regelmäßig aktualisieren. Diese Updates können das Verhalten Ihrer Lambda-Funktion geringfügig verändern. Um die Abhängigkeiten, die Ihre Funktion verwendet, vollständig zu kontrollieren, empfehlen wir, alle Abhängigkeiten mit Ihrem Bereitstellungspaket zu bündeln.
- Minimieren Sie die Größe Ihres Bereitstellungspakets auf die für die Laufzeit erforderliche Größe. Dadurch verkürzt sich die Zeit, die für das Herunterladen und Entpacken Ihres Bereitstellungspakets vor dem Aufruf benötigt wird. Vermeiden Sie es bei Funktionen, die in Java oder .NET Core verfasst wurden, die gesamte AWS SDK-Bibliothek als Teil Ihres Bereitstellungspakets hochzuladen. Stattdessen sollten Sie selektiv von den Modulen ausgehen, die Komponenten des SDK aufnehmen, die Sie benötigen (z. B. DynamoDB, Amazon-S3-SDK-Module und Lambda-Kernbibliotheken).
- Reduzieren Sie den Zeitaufwand, den Lambda für das Entpacken von Bereitstellungspaketen benötigt, die in Java erstellt wurden, indem Sie Ihre Abhängigkeitsdateien `.jar` in einem separaten /lib-Verzeichnis ablegen. Dies geht schneller, als den gesamten Code Ihrer Funktion in einem einzigen Jar mit einer großen Anzahl von `.class` Dateien zu speichern. Detaillierte

Anweisungen finden Sie unter Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven.

- Minimieren Sie die Komplexität Ihrer Abhängigkeiten. Ziehen Sie einfachere Frameworks vor, die sich schnell beim Start der Ausführungsumgebung laden lassen. Verwenden Sie beispielsweise einfachere Java Dependency Injection (IoC) Frameworks wie z. B. Dagger or Guice, als komplexere wie Spring Framework.
- Vermeiden Sie in Ihrer Lambda-Funktion rekursiven Code, bei dem sich die Funktion automatisch selbst aufruft, bis irgendein Kriterium erfüllt ist. Dies kann zu unvorhergesehenen Mengen an Funktionsaufrufen führen und höhere Kosten zur Folge haben. Wenn Sie dies versehentlich auslösen, legen Sie die reservierte gleichzeitige Ausführung der Funktion auf `0` fest, um sofort alle Aufrufe der Funktion zu drosseln, während Sie den Code aktualisieren.
- Verwenden Sie keine nicht dokumentierten, nicht öffentlichen APIs in Ihrem Lambda-Funktionscode. Für AWS Lambda verwaltete Laufzeiten führt Lambda regelmäßig Sicherheits- und Funktionsupdates für die internen APIs von Lambda durch. Diese internen API-Updates können abwärtskompatibel sein, was zu unbeabsichtigten Konsequenzen wie Aufruffehlern führt, wenn Ihre Funktion von diesen nicht öffentlichen APIs abhängig ist. Eine Liste öffentlich zugänglicher APIs finden Sie in der API-Referenz.
- Schreiben Sie idempotenten Code. Das Schreiben idempotenter Code für Ihre Funktionen stellt sicher, dass doppelte Ereignisse auf die gleiche Weise behandelt werden. Ihr Code sollte Ereignisse ordnungsgemäß validieren und doppelte Ereignisse ordnungsgemäß behandeln. Weitere Informationen finden Sie unter Wie mache ich meine Lambda-Funktion idempotent?.
- Vermeiden Sie die Verwendung des Java-DNS-Caches. Lambda-Funktionen speichern DNS-Antworten bereits im Cache. Wenn Sie einen anderen DNS-Cache verwenden, kann es zu Verbindungstimeouts kommen.

  Die `java.util.logging.Logger` Klasse kann indirekt den JVM-DNS-Cache aktivieren. Um die Standardeinstellungen zu überschreiben, setzen Sie networkaddress.cache.ttl vor der Initialisierung auf 0. `logger` Beispiel:

```
public class MyHandler {
  // first set TTL property
  static{
   java.security.Security.setProperty("networkaddress.cache.ttl" , "0");
  }
 // then instantiate logger
  var logger = org.apache.logging.log4j.LogManager.getLogger(MyHandler.class);
}
```

Um `UnknownHostException` Ausfälle zu vermeiden, empfehlen wir, den Wert auf 0 zu setzen. `networkaddress.cache.negative.ttl` Sie können diese Eigenschaft für eine Lambda-Funktion mit der `AWS_LAMBDA_JAVA_NETWORKADDRESS_CACHE_NEGATIVE_TTL=0` Umgebungsvariablen festlegen.

Durch die Deaktivierung des JVM-DNS-Caches wird das verwaltete DNS-Caching von Lambda nicht deaktiviert.

Funktionskonfiguration

- Die Leistungstests Ihrer Lambda-Funktion sind ein entscheidender Faktor, um sicherzustellen, dass Sie die optimale Speichergrößenkonfiguration auswählen. Jede Erhöhung des Arbeitsspeichers führt zu einer gleichwertigen Erhöhung der CPU-Verfügbarkeit Ihrer Funktion. Der Speicherverbrauch für Ihre Funktion wird pro Aufruf bestimmt und kann in Amazon eingesehen werden. CloudWatch Bei jedem Aufruf erfolgt ein `REPORT:` Eintrag, wie nachfolgend dargestellt:

  ```
  REPORT RequestId: 3604209a-e9a3-11e6-939a-754dd98c7be3 Duration: 12.34 ms Billed
   Duration: 100 ms Memory Size: 128 MB Max Memory Used: 18 MB
  ```

  Durch die Analyse `Max Memory Used:` des Feldes können Sie feststellen, ob Ihre Funktion mehr Speicher benötigt oder ob die Speichergröße Ihrer Funktion überdimensioniert ist.

  Um die richtige Speicherkonfiguration für Ihre Funktionen zu finden, empfehlen wir die Verwendung des Open-Source-Projekts AWS Lambda Power Tuning. Weitere Informationen finden Sie unter AWS Lambda Power Tuning on GitHub.

  Um die Funktionsleistung zu optimieren, empfehlen wir außerdem die Bereitstellung von Bibliotheken, die Advanced Vector Extensions 2 (AVX2) nutzen können. Auf diese Weise können Sie anspruchsvolle Workloads verarbeiten, einschließlich Inferencing für Machine Learning, Medienverarbeitung, High Performance Computing (HPC), wissenschaftliche Simulationen und Finanzmodellierung. Weitere Informationen finden Sie unter Schnellere AWS Lambda Funktionen mit AVX2 erstellen.
- Unterziehen Sie Ihre Lambda-Funktion zur Ermittlung der optimalen Zeitbeschränkung einem Belastungstest. Es sollte analysiert werden, wie lange Ihre Funktion ausgeführt wird, damit Sie Probleme mit einem Dependency-Service besser erkennen können, welche möglicherweise die Gleichzeitigkeit der Funktion über das hinaus erhöhen, was Sie erwarten. Dies ist

besonders wichtig, wenn Ihre Lambda-Funktion Netzwerkaufrufe an Ressourcen durchführt, die möglicherweise die Skalierung von Lambda nicht beherrschen.

- Verwenden Sie die strengsten Berechtigungen bei der Einrichtung von IAM-Richtlinien. Informieren Sie sich darüber, welche Ressourcen und Vorgänge Ihre Lambda-Funktion benötigt und beschränken Sie die Ausführungsrolle auf diese Berechtigungen. Weitere Informationen finden Sie unter Verwaltung von Berechtigungen in AWS Lambda.
- Machen Sie sich mit Lambda-Kontingente vertraut. Nutzlastgröße, Dateideskriptoren und /tmp space werden bei der Ermittlung von Laufzeit-Ressourcen-Limits oft übersehen.
- Löschen Sie nicht mehr benötigte Lambda-Funktionen. Auf diese Weise werden die nicht ungenutzten Funktionen nicht unnötigerweise auf die Größenbeschränkung Ihres Bereitstellungspakets angerechnet.
- Wenn Sie Amazon Simple Queue Service als Ereignisquelle verwenden, stellen Sie sicher, dass der Wert der erwarteten Aufrufzeit der Funktion nicht größer ist als der Wert der Zeitbeschränkung für die Sichtbarkeit in der Warteschlange. Dies gilt sowohl für als auch. CreateFunctionUpdateFunctionConfiguration
  - Im Fall von CreateFunctionschlägt der Prozess der Funktionserstellung fehl. AWS Lambda
  - Im Fall von UpdateFunctionConfigurationkönnte dies zu doppelten Aufrufen der Funktion führen.

Skalierbarkeit der Funktion

- Machen Sie sich mit Ihren vor- und nachgelagerten Durchsatzbeschränkungen vertraut. Lambda-Funktionen lassen sich zwar nahtlos abhängig von der Last skalieren, aber vor- und nachgelagerte Abhängigkeiten verfügen möglicherweise nicht über die gleichen Durchsatzfähigkeiten. Wenn Sie einschränken möchten, wie hoch Ihre Funktion skaliert werden kann, können Sie reservierte Parallelität für Ihre Funktion konfigurieren.
- Integrierte Drosselklappentoleranz. Wenn bei Ihrer synchronen Funktion eine Drosselung auftritt, weil der Datenverkehr die Skalierungsrate von Lambda überschreitet, können Sie die folgenden Strategien anwenden, um die Drosselungstoleranz zu verbessern:
  - Verwenden Sie Timeouts, Wiederholungsversuche und Backoffs mit Jitter. Durch die Implementierung dieser Strategien werden wiederholte Aufrufe vereinfacht und es wird sichergestellt, dass Lambda innerhalb von Sekunden skaliert werden kann, um die Drosselung durch Endbenutzer zu minimieren.
  - Verwenden Sie die bereitgestellte Parallelität. Bereitgestellte Parallelität ist die Anzahl der vorinitialisierten Ausführungsumgebungen, die Lambda Ihrer Funktion zuweist. Lambda

verarbeitet eingehende Anfragen mit bereitgestellter Parallelität, sofern verfügbar. Lambda kann Ihre Funktion bei Bedarf auch über Ihre bereitgestellte Parallelitätseinstellung hinaus skalieren. Durch die Konfiguration der bereitgestellten Parallelität fallen zusätzliche Gebühren für Ihr Konto an. AWS

Metriken und Alarme

- Verwenden Sie Arbeiten mit Lambda-Funktionsmetriken und CloudWatch Alarme, anstatt eine Metrik in Ihrem Lambda-Funktionscode zu erstellen oder zu aktualisieren. Es ist eine viel effizientere Art und Weise, die Zustandsprüfung Ihrer Lambda-Funktionen nachzuverfolgen, so dass Sie Probleme frühzeitig im Entwicklungsprozess erkennen können. Beispielsweise können Sie einen Alarm auf Basis der voraussichtlichen Dauer der Aufurfzeit Ihrer Lambda-Funktion konfigurieren, um Engpässe oder Latenzen zu beheben, die auf Ihren Funktionscode zurückzuführen sind.
- Nutzen Sie Ihre Protokollierungsbibliothek und AWS Lambda -Metriken und Dimensionen, um Anwendungsfehler (z. B. ERR, ERROR, WARNING usw.) zu erkennen.
- Verwenden Sie die AWS -Kostenanomalie-Erkennung, um ungewöhnliche Aktivitäten in Ihrem Konto zu erkennen. Die Kostenanomalie-Erkennung verwendet Machine Learning, um Ihre Kosten und Ihre Nutzung kontinuierlich zu überwachen und gleichzeitig falsch positive Warnungen zu minimieren. Die Erkennung von Kostenanomalien verwendet Daten von AWS Cost Explorer, was zu einer Verzögerung von bis zu 24 Stunden führt. Daher kann es nach der Nutzung bis zu 24 Stunden dauern, bis eine Anomalie erkannt wird. Um die Kostenanomalie-Erkennung verwenden zu können, müssen Sie sich zunächst bei Cost Explorer anmelden. Anschließend können Sie auf die Kostenanomalie-Erkennung zugreifen.

Arbeiten mit Streams

- Testen Sie mit unterschiedlichen Stapel- und Datensatzgrößen, so dass die Abfragefrequenz jeder Ereignisquelle darauf abgestimmt ist, wie schnell Ihre Funktion ihre Aufgabe erledigen kann. Der CreateEventSourceMapping BatchSize Parameter steuert die maximale Anzahl von Datensätzen, die bei jedem Aufruf an Ihre Funktion gesendet werden können. Eine höhere Stapelgröße kann den mit dem Aufruf-Overhead über eine größere Datensatzgruppe hinweg oft effizienter verarbeiten und Ihren Durchsatz erhöhen.

Standardmäßig ruft Lambda Ihre Funktion auf, sobald Datensätze verfügbar sind. Wenn der Batch, den Lambda aus der Ereignisquelle liest, nur einen Datensatz enthält, sendet Lambda nur einen Datensatz an die Funktion. Damit die Funktion nicht mit einer kleinen Anzahl von Datensätzen aufgerufen wird, können Sie die Ereignisquelle anweisen, Datensätze bis zu 5 Minuten lang zu puffern, indem Sie ein Batch-Fenster konfigurieren. Bevor die Funktion aufgerufen wird, liest Lambda so lange Datensätze aus der Ereignisquelle, bis es einen vollständigen Batch erfasst hat, das Batch-Verarbeitungsfenster abläuft oder der Batch die Nutzlastgrenze von 6 MB erreicht. Weitere Informationen finden Sie unter Batching-Verhalten.

> **Warning**
>
> Lambda-Ereignisquellenzuordnungen verarbeiten jedes Ereignis mindestens einmal, und es kann zu einer doppelten Verarbeitung von Datensätzen kommen. Um mögliche Probleme im Zusammenhang mit doppelten Ereignissen zu vermeiden, empfehlen wir Ihnen dringend, Ihren Funktionscode idempotent zu machen. Weitere Informationen finden Sie im Knowledge Center unter Wie mache ich meine Lambda-Funktion idempotent?. AWS

- Erhöhen Sie den Durchsatz bei der Verarbeitung des Kinesis-Streams durch Hinzufügen von Shards. Ein Kinesis Stream besteht aus einem oder mehreren Shards. Lambda fragt jeden Shard mit höchstens einem gleichzeitigen Aufruf ab. Wenn Ihr Stream z. B. 100 aktive Shards hat, werden maximal 100 Lambda-Funktionsaufrufe gleichzeitig ausgeführt. Eine Erhöhung der Anzahl der Shards erhöht direkt die Anzahl der maximalen gleichzeitigen Lambda-Funktionsaufrufe und kann den Durchsatz Ihrer Kinesis-Streamverarbeitung steigern. Wenn Sie die Anzahl der Shards in einem Kineses-Stream erhöhen, stellen Sie sicher, dass Sie für Ihre Daten einen guten Partitionsschlüssel ausgewählt haben, (siehe Partitionsschlüssel), so dass Bezugsdatensätze auf denselben Shards gespeichert werden und Ihre Daten gut verteilt sind.
- Verwenden Sie Amazon CloudWatch on IteratorAge , um festzustellen, ob Ihr Kinesis-Stream verarbeitet wird. Konfigurieren Sie beispielsweise einen CloudWatch Alarm mit einer Maximaleinstellung von 30000 (30 Sekunden).

Bewährte Methoden für die Gewährleistung der Sicherheit

- Überwachen Sie Ihre Nutzung von AWS Lambda in Bezug auf bewährte Sicherheitsmethoden, indem Sie AWS Security Hub Security Hub verwendet Sicherheitskontrollen für die Bewertung von Ressourcenkonfigurationen und Sicherheitsstandards, um Sie bei der Einhaltung verschiedener Compliance-Frameworks zu unterstützen. Weitere Informationen zur Verwendung von Security

Hub zur Evaluierung von Lambda-Ressourcen finden Sie unter AWS Lambda Kontrollen im AWS Security Hub Benutzerhandbuch.

- Überwachen Sie Lambda-Netzwerkaktivitätsprotokolle mit Amazon GuardDuty Lambda Protection. GuardDuty Lambda-Schutz hilft Ihnen dabei, potenzielle Sicherheitsbedrohungen zu identifizieren, wenn Lambda-Funktionen in Ihrem aufgerufen werden. AWS-Konto Dies ist beispielsweise der Fall, wenn eine Ihrer Funktionen eine IP-Adresse abfragt, die mit Aktivitäten im Zusammenhang mit Kryptowährungen verknüpft ist. GuardDuty überwacht die Netzwerkaktivitätsprotokolle, die generiert werden, wenn eine Lambda-Funktion aufgerufen wird. Weitere Informationen finden Sie unter Lambda-Schutz im GuardDuty Amazon-Benutzerhandbuch.

Verwaltung von Berechtigungen in AWS Lambda

Sie können AWS Identity and Access Management (IAM) verwenden, um Berechtigungen in AWS Lambda zu verwalten. Es gibt zwei Hauptkategorien von Berechtigungen, die Sie bei der Arbeit mit Lambda-Funktionen berücksichtigen müssen:

- Berechtigungen, die Ihre Lambda-Funktionen benötigen, um API-Aktionen auszuführen und auf andere AWS Ressourcen zuzugreifen
- Berechtigungen, die andere AWS Benutzer und Entitäten für den Zugriff auf Ihre Lambda-Funktionen benötigen

Lambda-Funktionen müssen häufig auf andere AWS Ressourcen zugreifen und verschiedene API-Operationen mit diesen Ressourcen ausführen. Möglicherweise haben Sie eine Lambda-Funktion, die auf ein Ereignis reagiert, indem sie Einträge in einer Amazon DynamoDB DynamoDB-Datenbank aktualisiert. In diesem Fall benötigt Ihre Funktion Berechtigungen für den Zugriff auf die Datenbank sowie Berechtigungen zum Ablegen oder Aktualisieren von Elementen in dieser Datenbank.

Sie definieren die Berechtigungen, die Ihre Lambda-Funktion benötigt, in einer speziellen IAM-Rolle, der sogenannten Ausführungsrolle. In dieser Rolle können Sie eine Richtlinie anhängen, die alle Berechtigungen definiert, die Ihre Funktion für den Zugriff auf andere AWS Ressourcen und das Lesen aus Ereignisquellen benötigt. Jede Lambda-Funktion muss eine Ausführungsrolle haben. Ihre Ausführungsrolle muss mindestens Zugriff auf Amazon haben, CloudWatch da Lambda-Funktionen standardmäßig in CloudWatch Logs protokolliert werden. Sie können die `AWSLambdaBasicExecutionRole`verwaltete Richtlinie an Ihre Ausführungsrolle anhängen, um diese Anforderung zu erfüllen.

Um anderen AWS Konten, Organisationen und Diensten Berechtigungen für den Zugriff auf Ihre Lambda-Ressourcen zu erteilen, haben Sie mehrere Möglichkeiten:

- Sie können identitätsbasierte Richtlinien verwenden, um anderen Benutzern Zugriff auf Ihre Lambda-Ressourcen zu gewähren. Identitätsbasierte Richtlinien können direkt auf Benutzer oder auf Gruppen und Rollen angewendet werden, die einem Benutzer zugeordnet sind.
- Sie können ressourcenbasierte Richtlinien verwenden, um anderen Konten und AWS Diensten Berechtigungen für den Zugriff auf Ihre Lambda-Ressourcen zu erteilen. Wenn ein Benutzer versucht, auf eine Lambda-Ressource zuzugreifen, berücksichtigt Lambda sowohl die identitätsbasierten Richtlinien des Benutzers als auch die ressourcenbasierte Richtlinie der

Ressource. Wenn ein AWS Service wie Amazon Simple Storage Service (Amazon S3) Ihre Lambda-Funktion aufruft, berücksichtigt Lambda nur die ressourcenbasierte Richtlinie.

- Sie können ein ABAC-Modell (attribute-based access control) verwenden, um den Zugriff auf Ihre Lambda-Funktionen zu steuern. Mit ABAC können Sie Tags an eine Lambda-Funktion anhängen, sie in bestimmten API-Anfragen übergeben oder sie an den IAM-Principal anhängen, der die Anfrage stellt. Geben Sie dieselben Tags im Bedingungselement einer IAM-Richtlinie an, um den Funktionszugriff zu kontrollieren.

In hat es sich bewährt AWS, nur die Berechtigungen zu gewähren, die für die Ausführung einer Aufgabe erforderlich sind (Berechtigungen mit den geringsten Rechten). Um dies in Lambda zu implementieren, empfehlen wir, mit einer AWS verwalteten Richtlinie zu beginnen. Sie können diese verwalteten Richtlinien unverändert oder als Ausgangspunkt zum Schreiben Ihrer eigenen restriktiveren Richtlinien verwenden.

Um Ihnen bei der Feinabstimmung Ihrer Berechtigungen für den Zugriff mit den geringsten Rechten zu helfen, bietet Lambda einige zusätzliche Bedingungen, die Sie in Ihre Richtlinien aufnehmen können. Weitere Informationen finden Sie unter the section called “Ressourcen und Bedingungen”.

Weitere Informationen zu IAM finden Sie im IAM-Benutzerhandbuch.

Definieren von Lambda-Funktionsberechtigungen mit einer Ausführungsrolle

Die Ausführungsrolle einer Lambda-Funktion ist eine AWS Identity and Access Management (IAM-) Rolle, die der Funktion die Erlaubnis erteilt, auf AWS Dienste und Ressourcen zuzugreifen. Sie könnten beispielsweise eine Ausführungsrolle erstellen, die berechtigt ist, Protokolle an Amazon zu senden CloudWatch und Trace-Daten hochzuladen AWS X-Ray. Diese Seite enthält Informationen zum Erstellen, Anzeigen und Verwalten der Ausführungsrolle einer Lambda-Funktion.

Lambda übernimmt automatisch Ihre Ausführungsrolle an, wenn Sie Ihre Funktion aufrufen. Sie sollten es vermeiden, manuell aufzurufen`sts:AssumeRole`, um die Ausführungsrolle in Ihrem Funktionscode zu übernehmen. Wenn Ihr Anwendungsfall erfordert, dass die Rolle sich selbst annimmt, müssen Sie die Rolle selbst als vertrauenswürdigen Prinzipal in die Vertrauensrichtlinie Ihrer Rolle aufnehmen. Weitere Informationen zum Ändern einer Rollenvertrauensrichtlinie finden Sie unter Ändern einer Rollenvertrauensrichtlinie (Konsole) im IAM-Benutzerhandbuch.

Damit Lambda Ihre Ausführungsrolle ordnungsgemäß übernehmen kann, muss die Vertrauensrichtlinie der Rolle den Lambda-Serviceprinzipal (`lambda.amazonaws.com`) als vertrauenswürdigen Dienst angeben.

Themen

- Erstellen einer Ausführungsrolle in der IAM-Konsole
- Rollen erstellen und verwalten mit AWS CLI
- Gewähren Sie den Zugriff auf Ihre Lambda-Ausführungsrolle mit den geringsten Berechtigungen
- Berechtigungen in der Ausführungsrolle anzeigen und aktualisieren
- Arbeiten mit AWS verwalteten Richtlinien in der Ausführungsrolle
- Verwendung der Quellfunktion ARN zur Steuerung des Funktionszugriffsverhaltens

Erstellen einer Ausführungsrolle in der IAM-Konsole

Standardmäßig erstellt Lambda beim Erstellen einer Funktion in der Lambda-Konsole eine Ausführungsrolle mit minimalen Berechtigungen. Insbesondere umfasst diese Ausführungsrolle die `AWSLambdaBasicExecutionRole`verwaltete Richtlinie, die Ihrer Funktion grundlegende Berechtigungen zum Protokollieren von Ereignissen in Amazon CloudWatch Logs erteilt.

Ihre Funktionen benötigen in der Regel zusätzliche Berechtigungen, um sinnvollere Aufgaben ausführen zu können. Beispielsweise könnten Sie über eine Lambda-Funktion verfügen, die auf ein Ereignis reagiert, indem sie Einträge in einer Amazon DynamoDB DynamoDB-Datenbank aktualisiert. Mithilfe der IAM-Konsole können Sie eine Ausführungsrolle mit den erforderlichen Berechtigungen erstellen.

So erstellen Sie eine Ausführungsrolle in der IAM-Konsole

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Typ der vertrauenswürdigen Entität die Option AWS -Service aus.
4. Wählen Sie unter Anwendungsfall Lambda aus.
5. Wählen Sie Weiter aus.
6. Wählen Sie die AWS verwalteten Richtlinien aus, die Sie Ihrer Rolle zuordnen möchten. Wenn Ihre Funktion beispielsweise auf DynamoDB zugreifen muss, wählen Sie die AWSLambdaDynamoDBExecutionRoleverwaltete Richtlinie aus.
7. Wählen Sie Weiter aus.
8. Geben Sie einen Role name (Rollennamen) ein und klicken Sie auf Create Role (Rolle erstellen).

Ausführliche Anweisungen finden Sie unter Erstellen einer Rolle für einen AWS Dienst (Konsole) im IAM-Benutzerhandbuch.

Nachdem Sie Ihre Ausführungsrolle erstellt haben, fügen Sie sie Ihrer Funktion hinzu. Wenn Sie eine Funktion in der Lambda-Konsole erstellen, können Sie der Funktion jede Ausführungsrolle zuordnen, die Sie zuvor erstellt haben. Wenn Sie einer vorhandenen Funktion eine neue Ausführungsrolle zuordnen möchten, folgen Sie den Schritten unter.

Rollen erstellen und verwalten mit AWS CLI

Um eine Ausführungsrolle mit dem AWS Command Line Interface (AWS CLI) zu erstellen, verwenden Sie den create-role Befehl. Wenn Sie diesen Befehl verwenden, können Sie die Vertrauensrichtlinie angeben. Über die Vertrauensrichtlinie einer Rolle wird den angegebenen Prinzipalen die Berechtigung gegeben, die Rolle zu übernehmen. Im folgenden Beispiel erteilen Sie dem Lambda-Serviceprinzipal die Berechtigung, Ihre Rolle zu übernehmen. Die Anforderungen für Escape-Anführungszeichen in der JSON-Zeichenfolge können je nach Shell variieren.

```
aws iam create-role --role-name lambda-ex --assume-role-policy-document '{"Version":
 "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service":
 "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}'
```

Sie können die Vertrauensrichtlinie für die Rolle auch mithilfe einer separaten JSON-Datei definieren. Im folgenden Beispiel ist `trust-policy.json` eine Datei im aktuellen Verzeichnis.

Example trust-policy.json

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

```
aws iam create-role --role-name lambda-ex --assume-role-policy-document file://trust-
policy.json
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "Role": {
        "Path": "/",
        "RoleName": "lambda-ex",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/lambda-ex",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "lambda.amazonaws.com"
                    },
```

```
                "Action": "sts:AssumeRole"
            }
        ]
    }
  }
}
```

Um der Rolle Berechtigungen hinzuzufügen, verwenden Sie den attach-policy-to-role-Befehl. Mit dem folgenden Befehl `AWSLambdaBasicExecutionRole` wird die verwaltete Richtlinie zur `lambda-ex` Ausführungsrolle hinzugefügt.

```
aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole
```

Nachdem Sie Ihre Ausführungsrolle erstellt haben, fügen Sie sie Ihrer Funktion hinzu. Wenn Sie eine Funktion in der Lambda-Konsole erstellen, können Sie der Funktion jede Ausführungsrolle zuordnen, die Sie zuvor erstellt haben. Wenn Sie einer vorhandenen Funktion eine neue Ausführungsrolle zuordnen möchten, folgen Sie den Schritten unter.

Gewähren Sie den Zugriff auf Ihre Lambda-Ausführungsrolle mit den geringsten Berechtigungen

Wenn Sie während der Entwicklungsphase zum ersten Mal eine IAM-Rolle für Ihre Lambda-Funktion erstellen, können Sie manchmal Berechtigungen erteilen, die über das erforderliche Maß hinausgehen. Bevor Sie Ihre Funktion in der Produktionsumgebung veröffentlichen, sollten Sie als bewährte Methode die Richtlinie so anpassen, dass sie nur die erforderlichen Berechtigungen enthält. Weitere Informationen finden Sie unter Anwenden von Berechtigungen mit geringsten Berechtigungen im IAM-Benutzerhandbuch.

Verwenden Sie IAM Access Analyzer, um die erforderlichen Berechtigungen für die IAM-Ausführungsrollenrichtlinie zu identifizieren. IAM Access Analyzer überprüft Ihre AWS CloudTrail Protokolle über den von Ihnen angegebenen Zeitraum und generiert eine Richtlinienvorlage mit nur den Berechtigungen, die die Funktion in diesem Zeitraum verwendet hat. Sie können die Vorlage verwenden, um eine verwaltete Richtlinie mit definierten Berechtigungen zu erstellen und sie dann an die IAM-Rolle anzuhängen. Auf diese Weise gewähren Sie nur die Berechtigungen, die die Rolle für die Interaktion mit AWS Ressourcen für Ihren speziellen Anwendungsfall benötigt.

Weitere Informationen finden Sie unter Generieren von Richtlinien basierend auf Zugriffsaktivitäten im IAM-Benutzerhandbuch.

Berechtigungen in der Ausführungsrolle anzeigen und aktualisieren

In diesem Thema wird beschrieben, wie Sie die Ausführungsrolle Ihrer Funktion anzeigen und aktualisieren können.

Themen

Die Ausführungsrolle einer Funktion anzeigen

Verwenden Sie die Lambda-Konsole, um die Ausführungsrolle einer Funktion anzuzeigen.

Um die Ausführungsrolle einer Funktion (Konsole) anzuzeigen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und anschließend Permissions (Berechtigungen) aus.
4. Unter Ausführungsrolle können Sie die Rolle anzeigen, die derzeit als Ausführungsrolle der Funktion verwendet wird. Der Einfachheit halber können Sie im Abschnitt Ressourcenübersicht alle Ressourcen und Aktionen anzeigen, auf die die Funktion zugreifen kann. Sie können auch einen Dienst aus der Dropdownliste auswählen, um alle Berechtigungen für diesen Dienst anzuzeigen.

Aktualisierung der Ausführungsrolle einer Funktion

Sie können Berechtigungen jederzeit zur Ausführungsrolle einer Funktion hinzufügen bzw. daraus entfernen oder Ihre Funktion so konfigurieren, dass sie eine andere Rolle verwendet. Wenn Ihre Funktion Zugriff auf andere Dienste oder Ressourcen benötigt, müssen Sie der Ausführungsrolle die erforderlichen Berechtigungen hinzufügen.

Wenn Sie Ihrer Funktion Berechtigungen hinzufügen, führen Sie auch eine einfache Aktualisierung des Codes oder der Konfiguration durch. Dies zwingt ausgeführte Instances Ihrer Funktion, die veraltete Anmeldeinformationen haben, anzuhalten und ersetzt zu werden.

Um die Ausführungsrolle einer Funktion zu aktualisieren, können Sie die Lambda-Konsole verwenden.

Um die Ausführungsrolle einer Funktion (Konsole) zu aktualisieren

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie den Namen einer Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und anschließend Permissions (Berechtigungen) aus.
4. Wählen Sie unter Ausführungsrolle die Option Bearbeiten aus.
5. Wenn Sie Ihre Funktion so aktualisieren möchten, dass sie eine andere Rolle als Ausführungsrolle verwendet, wählen Sie die neue Rolle im Dropdownmenü unter Bestehende Rolle aus.

   > **Note**
   >
   > Wenn Sie die Berechtigungen innerhalb einer vorhandenen Ausführungsrolle aktualisieren möchten, können Sie dies nur in der AWS Identity and Access Management (IAM-) Konsole tun.

   Wenn Sie eine neue Rolle zur Verwendung als Ausführungsrolle erstellen möchten, wählen Sie unter Ausführungsrolle die Option Neue Rolle aus AWS Richtlinienvorlagen erstellen aus. Geben Sie dann unter Rollenname einen Namen für Ihre neue Rolle ein und geben Sie unter Richtlinienvorlagen alle Richtlinien an, die Sie der neuen Rolle zuordnen möchten.
6. Klicken Sie auf Speichern.

Arbeiten mit AWS verwalteten Richtlinien in der Ausführungsrolle

Die folgenden AWS verwalteten Richtlinien bieten Berechtigungen, die für die Verwendung von Lambda-Funktionen erforderlich sind.

Änderung	Beschreibung	Datum
AWSLambdaMSKExecutionRole— Lambda hat dieser Richtlinie die Berechtigung kafka: DescribeCluster V2 hinzugefügt.	`AWSLambdaMSKExecutionRole` gewährt Berechtigungen zum Lesen und Zugreifen auf Datensätze aus einem Amazon Managed Streaming for Apache Kafka	17. Juni 2022

Änderung	Beschreibung	Datum
	(Amazon MSK) -Cluster, zum Verwalten von Elastic Network Interfaces (ENIs) und zum Schreiben in Protokolle. CloudWatch	
AWSLambdaBasicExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaBasicExecutionRole` erteilt Berechtigungen, um Protokolle auf CloudWatch hochzuladen.	14. Februar 2022
AWSLambdaDynamoDBExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaDynamoDBExecutionRole` gewährt Berechtigungen zum Lesen von Datensätzen aus einem Amazon DynamoDB DynamoDB-Stream und zum CloudWatch Schreiben in Logs.	14. Februar 2022
AWSLambdaKinesisExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaKinesisExecutionRole` gewährt Berechtigungen zum Lesen von Ereignissen aus einem Amazon Kinesis Kinesis-Datenstream und zum Schreiben in CloudWatch Protokolle.	14. Februar 2022

Änderung	Beschreibung	Datum
AWSLambdaMSKExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaMSKExecutionRole` gewährt Berechtigungen zum Lesen und Zugreifen auf Datensätze aus einem Amazon Managed Streaming for Apache Kafka (Amazon MSK) -Cluster, zum Verwalten von Elastic Network Interfaces (ENIs) und zum Schreiben in Protokolle. CloudWatch	14. Februar 2022
AWSLambdaSQSQueueExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaSQSQueueExecutionRole` gewährt Berechtigungen zum Lesen einer Nachricht aus einer Amazon Simple Queue Service (Amazon SQS) -Warteschlange und zum Schreiben in CloudWatch Protokolle.	14. Februar 2022
AWSLambdaVPCAccessExecutionRole— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSLambdaVPCAccessExecutionRole` gewährt Berechtigungen zur Verwaltung von ENIs innerhalb einer Amazon VPC und zum CloudWatch Schreiben in Logs.	14. Februar 2022
AWSXRayDaemonWriteAccess— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AWSXRayDaemonWriteAccess` erteilt Berechtigungen zum Hochladen von Nachverfolgungsdaten auf X-Ray.	14. Februar 2022

Änderung	Beschreibung	Datum
CloudWatchLambdaInsightsExecutionRolePolicy— Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`CloudWatchLambdaInsightsExecutionRolePolicy` gewährt Berechtigungen zum Schreiben von Laufzeitmetriken in CloudWatch Lambda Insights.	14. Februar 2022
ObjectLambdaExecutionRoleAmazonS3-Richtlinie — Lambda hat damit begonnen, Änderungen an dieser Richtlinie nachzuverfolgen.	`AmazonS3ObjectLambdaExecutionRolePolicy` gewährt Berechtigungen zur Interaktion mit dem Amazon Simple Storage Service (Amazon S3) -Objekt Lambda und zum Schreiben in CloudWatch Logs.	14. Februar 2022

Bei einigen Funktionen versucht die Lambda-Konsole, Ihrer Ausführungsrolle in einer vom Kunden verwalteten Richtlinie fehlende Berechtigungen hinzuzufügen. Diese Politiken können zahlreich werden. Fügen Sie der Ausführungsrolle die relevanten AWS -verwalteten Richtlinien hinzu, bevor Sie Funktionen aktivieren, um das Erstellen zusätzlicher Richtlinien zu vermeiden.

Wenn Sie eine Ereignisquellen-Zuweisung zum Aufrufen Ihrer Funktion verwenden, verwendet Lambda die Ausführungsrolle zum Lesen von Ereignisdaten. Zum Beispiel liest eine Ereignisquellen-Zuweisung für Kinesis-Ereignisse aus einem Datenstrom und sendet diese in Batches an Ihre Funktion.

Wenn ein Dienst eine Rolle in Ihrem Konto übernimmt, können Sie die globalen Bedingungskontextschlüssel `aws:SourceAccount` und `aws:SourceArn` in Ihrer Rollenvertrauensrichtlinie übernehmen, um den Zugriff auf die Rolle nur auf Anforderungen zu beschränken, die von erwarteten Ressourcen generiert werden. Weitere Informationen finden Sie unter Vermeidung des Problems des verwirrten Stellvertreters im dienstübergreifenden Szenario für AWS Security Token Service.

Zusätzlich zu den AWS verwalteten Richtlinien bietet die Lambda-Konsole Vorlagen für die Erstellung einer benutzerdefinierten Richtlinie mit Berechtigungen für zusätzliche Anwendungsfälle. Wenn Sie

eine Funktion in der Lambda-Konsole erstellen, haben Sie die Wahl, eine neue Ausführungsrolle mit Berechtigungen aus einer oder mehreren Vorlagen zu erstellen. Diese Vorlagen werden auch automatisch angewendet, wenn Sie eine Funktion von einer Vorlage erstellen oder wenn Sie Optionen konfigurieren, die Zugriff auf andere Services erfordern. Beispielvorlagen sind im GitHubRepository dieses Handbuchs verfügbar.

Verwendung der Quellfunktion ARN zur Steuerung des Funktionszugriffsverhaltens

Es ist üblich, dass Ihr Lambda-Funktionscode API-Anfragen an andere AWS Dienste stellt. Um diese Anforderungen zu stellen, generiert Lambda einen kurzlebigen Satz von Anmeldeinformationen, indem es die Ausführungsrolle Ihrer Funktion übernimmt. Diese Anmeldeinformationen sind während des Aufrufs Ihrer Funktion als Umgebungsvariablen verfügbar. Wenn Sie mit AWS -SDKs arbeiten, müssen Sie die Anmeldeinformationen für das SDK nicht direkt im Code angeben. Standardmäßig überprüft die Kette der Anbieter von Anmeldeinformationen nacheinander jeden Ort, an dem Sie Anmeldeinformationen festlegen können, und wählt die erste verfügbare aus – in der Regel die Umgebungsvariablen (`AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` und `AWS_SESSION_TOKEN`).

Lambda fügt die Quellfunktion ARN in den Anmeldeinformationskontext ein, wenn es sich bei der Anfrage um eine AWS API-Anforderung handelt, die aus Ihrer Ausführungsumgebung stammt. Lambda fügt auch den Quellfunktions-ARN für die folgenden AWS -API-Anfragen ein, die Lambda in Ihrem Namen außerhalb Ihrer Ausführungsumgebung durchführt:

Service	Aktion	Grund
CloudWatch Logs	`CreateLogGroup` , `CreateLogStream` , `PutLogEvents`	Um Logs in einer CloudWatch Logs-Protokollgruppe zu speichern
X-Ray	`PutTraceSegments`	So senden Sie Verfolgungsdaten an X-Ray
Amazon EFS	`ClientMount`	So stellen Sie eine Verbindung zwischen Ihrer Funktion und einem Amazon Elastic File System (Amazon EFS) Dateisystem her

Andere AWS API-Aufrufe, die Lambda außerhalb Ihrer Ausführungsumgebung in Ihrem Namen mit derselben Ausführungsrolle durchführt, enthalten nicht die Quellfunktion ARN. Beispiele für solche API-Aufrufe außerhalb der Ausführungsumgebung sind:

- Ruft AWS Key Management Service (AWS KMS) auf, um Ihre Umgebungsvariablen automatisch zu verschlüsseln und zu entschlüsseln.
- Aufrufe von Amazon Elastic Compute Cloud (Amazon EC2) zum Erstellen von Elastic-Network-Schnittstellen (ENIs) für eine VPC-fähige Funktion.
- Ruft AWS Dienste wie Amazon Simple Queue Service (Amazon SQS) auf, um aus einer Ereignisquelle zu lesen, die als Ereignisquellen-Mapping eingerichtet ist.

Mit dem ARN der Quellfunktion im Kontext der Anmeldeinformationen können Sie überprüfen, ob ein Aufruf Ihrer Ressource aus dem Code einer bestimmten Lambda-Funktion stammt. Um dies zu überprüfen, verwenden Sie den `lambda:SourceFunctionArn` Bedingungsschlüssel in einer identitätsbasierten IAM-Richtlinie oder Service Control Policy (SCP).

> **Note**
>
> Sie können den `lambda:SourceFunctionArn`-Bedingungsschlüssel nicht in ressourcenbasierten Richtlinien verwenden.

Mit diesem Bedingungsschlüssel in Ihren identitätsbasierten Richtlinien oder SCPs können Sie Sicherheitskontrollen für die API-Aktionen implementieren, die Ihr Funktionscode für andere Dienste vornimmt. AWS Dies hat einige wichtige Sicherheitsanwendungen, z. B. um Ihnen zu helfen, die Quelle eines Anmeldeinformationslecks zu identifizieren.

> **Note**
>
> Der `lambda:SourceFunctionArn`-Bedingungsschlüssel unterscheidet sich von den `lambda:FunctionArn` und `aws:SourceArn`-Bedingungsschlüsseln. Der `lambda:FunctionArn`-Bedingungsschlüssel gilt nur für Ereignisquellenzuordnungen und hilft bei der Definition der Funktionen, die Ihre Ereignisquelle aufrufen kann. Der `aws:SourceArn` Bedingungsschlüssel gilt nur für Richtlinien, bei denen Ihre Lambda-Funktion die Zielressource ist, und hilft zu definieren, welche anderen AWS Dienste und Ressourcen diese Funktion aufrufen können. Der `lambda:SourceFunctionArn` Bedingungsschlüssel kann für jede identitätsbasierte Richtlinie oder jeden SCP gelten, um

die spezifischen Lambda-Funktionen zu definieren, die berechtigt sind, bestimmte AWS API-Aufrufe an andere Ressourcen zu tätigen.

Um `lambda:SourceFunctionArn` in Ihrer Richtlinie zu verwenden, fügen Sie es als Bedingung mit einem der ARN-Bedingungsoperatoren ein. Der Wert des Schlüssels muss ein gültiger ARN sein.

Angenommen, Ihr Lambda-Funktionscode macht einen `s3:PutObject`-Aufruf, der auf einen bestimmten Amazon-S3-Bucket abzielt. Möglicherweise möchten Sie nur einer bestimmten Lambda-Funktion erlauben, dass `s3:PutObject` auf diesen Bucket zugreift. In diesem Fall sollte der Ausführungsrolle Ihrer Funktion eine Richtlinie angefügt sein, die wie folgt aussieht:

Example Richtlinie, die einer bestimmten Lambda-Funktion Zugriff auf eine Amazon-S3-Ressource gewährt

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ExampleSourceFunctionArn",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::lambda_bucket/*",
            "Condition": {
                "ArnEquals": {
                    "lambda:SourceFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:source_lambda"
                }
            }
        }
    ]
}
```

Diese Richtlinie erlaubt nur `s3:PutObject` Zugriff wenn die Quelle die Lambda-Funktion mit ARN `arn:aws:lambda:us-east-1:123456789012:function:source_lambda` ist. Diese Richtlinie erlaubt `s3:PutObject` keinen Zugriff auf jede andere aufrufende Identität. Dies gilt auch dann, wenn eine andere Funktion oder Entität einen `s3:PutObject`-Aufruf mit der gleichen Ausführungsrolle tätigt.

> **Note**
>
> Der Bedingungsschlüssel `lambda:SourceFunctionARN` unterstützt keine Lambda-Funktionsversionen oder -Funktionsaliase. Wenn Sie den ARN für eine bestimmte Funktionsversion oder einen bestimmten Alias verwenden, ist Ihre Funktion nicht berechtigt, die von Ihnen angegebene Aktion auszuführen. Achten Sie darauf, den unqualifizierten ARN für Ihre Funktion ohne Versions- oder Alias-Suffix zu verwenden.

Sie können ihn auch in SCPs verwenden. `lambda:SourceFunctionArn` Angenommen, Sie möchten den Zugriff auf Ihren Bucket entweder auf den Code einer einzelnen Lambda-Funktion oder auf Aufrufe aus einer bestimmten Amazon Virtual Private Cloud (VPC) beschränken. Das folgende SCP illustriert dies.

Example Richtlinie, die den Zugriff auf Amazon S3 unter bestimmten Bedingungen verweigert

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::lambda_bucket/*",
            "Effect": "Deny",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": [
                        "vpc-12345678"
                    ]
                }
            }
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": "arn:aws:s3:::lambda_bucket/*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotEqualsIfExists": {
```

```
                    "lambda:SourceFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:source_lambda"
                }
            }
        }
    ]
}
```

Diese Richtlinie verweigert alle S3-Aktionen, sofern sie nicht von einer bestimmten Lambda-Funktion mit ARN `arn:aws:lambda:*:123456789012:function:source_lambda` stammen, oder sofern sie nicht aus dem angegebenen VPC stammen. Der `StringNotEqualsIfExists`-Operator weist IAM an, diese Bedingung nur zu verarbeiten, wenn der `aws:SourceVpc`-Schlüssel in der Anfrage vorhanden ist. In ähnlicher Weise berücksichtigt IAM den `ArnNotEqualsIfExists`-Operator nur, wenn `lambda:SourceFunctionArn` vorhanden ist.

Anderen AWS Entitäten Zugriff auf Ihre Lambda-Funktionen gewähren

Um anderen AWS Konten, Organisationen und Diensten Berechtigungen für den Zugriff auf Ihre Lambda-Ressourcen zu erteilen, haben Sie mehrere Möglichkeiten:

- Sie können identitätsbasierte Richtlinien verwenden, um anderen Benutzern Zugriff auf Ihre Lambda-Ressourcen zu gewähren. Identitätsbasierte Richtlinien können direkt auf Benutzer oder auf Gruppen und Rollen angewendet werden, die einem Benutzer zugeordnet sind.
- Sie können ressourcenbasierte Richtlinien verwenden, um anderen Konten und AWS Diensten Berechtigungen für den Zugriff auf Ihre Lambda-Ressourcen zu erteilen. Wenn ein Benutzer versucht, auf eine Lambda-Ressource zuzugreifen, berücksichtigt Lambda sowohl die identitätsbasierten Richtlinien des Benutzers als auch die ressourcenbasierte Richtlinie der Ressource. Wenn ein AWS Service wie Amazon Simple Storage Service (Amazon S3) Ihre Lambda-Funktion aufruft, berücksichtigt Lambda nur die ressourcenbasierte Richtlinie.
- Sie können ein ABAC-Modell (attribute-based access control) verwenden, um den Zugriff auf Ihre Lambda-Funktionen zu steuern. Mit ABAC können Sie Tags an eine Lambda-Funktion anhängen, sie in bestimmten API-Anfragen übergeben oder sie an den IAM-Principal anhängen, der die Anfrage stellt. Geben Sie dieselben Tags im Bedingungselement einer IAM-Richtlinie an, um den Funktionszugriff zu kontrollieren.

Um Ihnen bei der Feinabstimmung Ihrer Berechtigungen für den Zugriff mit den geringsten Rechten zu helfen, bietet Lambda einige zusätzliche Bedingungen, die Sie in Ihre Richtlinien aufnehmen können. Weitere Informationen finden Sie unter the section called “Ressourcen und Bedingungen”.

Arbeiten mit identitätsbasierten IAM-Richtlinien in Lambda

Sie können identitätsbasierte Richtlinien in AWS Identity and Access Management (IAM) verwenden, um Benutzern in Ihrem Konto Zugriff auf Lambda zu gewähren. Identitätsbasierte Richtlinien können direkt auf Benutzer oder auf Gruppen und Rollen angewendet werden, die einem Benutzer zugeordnet sind. Sie können auch Benutzern in einem anderen Konto die Berechtigung erteilen, eine Rolle in Ihrem Konto zu übernehmen und auf Ihre Lambda-Ressourcen zuzugreifen. Diese Seite zeigt ein Beispiel dafür, wie identitätsbasierte Richtlinien für die Funktionsentwicklung verwendet werden können.

Lambda bietet AWS verwaltete Richtlinien, die Zugriff auf Lambda-API-Aktionen und in einigen Fällen Zugriff auf andere AWS Dienste gewähren, die zur Entwicklung und Verwaltung von Lambda-

Ressourcen verwendet werden. Lambda aktualisiert je nach Bedarf die verwalteten Richtlinien, um sicherzustellen, dass Ihre Benutzer Zugriff auf neue Funktionen haben, sobald diese veröffentlicht werden.

- AWSLambda_FullAccess— Gewährt vollen Zugriff auf Lambda-Aktionen und andere AWS Dienste, die zur Entwicklung und Wartung von Lambda-Ressourcen verwendet werden. Diese Richtlinie wurde erstellt, indem der Geltungsbereich der vorherigen Richtlinie eingeschränkt wurde. AWSLambdaFullAccess
- AWSLambda_ReadOnlyAccess— Gewährt schreibgeschützten Zugriff auf Lambda-Ressourcen. Diese Richtlinie wurde erstellt, indem der Geltungsbereich der vorherigen Richtlinie eingeschränkt wurde. AWSLambdaReadOnlyAccess
- AWSLambdaRole— Erteilt Berechtigungen zum Aufrufen von Lambda-Funktionen.

AWS verwaltete Richtlinien gewähren Berechtigungen für API-Aktionen, ohne die Lambda-Funktionen oder -Layer einzuschränken, die ein Benutzer ändern kann. Für eine feinere Steuerung können Sie eigene Richtlinien erstellen, die den Umfang der Berechtigungen eines Benutzers einschränken.

Sections

Schreiben einer Beispielrichtlinie, die Benutzerberechtigungen für eine Funktion gewährt

Verwenden Sie identitätsbasierte Richtlinien, um Benutzern das Ausführen von Operationen für Lambda-Funktionen zu erlauben.

> **Note**
>
> Für eine als Container-Image definierte Funktion MUSS die Benutzerberechtigung für den Zugriff auf das Image in der Amazon Elastic Container Registry konfiguriert werden. Ein Beispiel finden Sie unter Amazon-ECR-Berechtigungen.

Im Folgenden finden Sie ein Beispiel für eine Berechtigungsrichtlinie mit eingeschränktem Umfang. Sie ermöglicht Benutzern das Erstellen und Verwalten von Lambda-Funktionen mit einem bestimmten Präfix (`intern-`), die mit einer bestimmten Ausführungsrolle konfiguriert sind.

Example Richtlinie für die Funktionsentwicklung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:GetAccountSettings",
                "lambda:GetEventSourceMapping",
                "lambda:GetFunction",
                "lambda:GetFunctionConfiguration",
                "lambda:GetFunctionCodeSigningConfig",
                "lambda:GetFunctionConcurrency",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctions",
                "lambda:ListTags",
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DevelopFunctions",
            "Effect": "Allow",
            "NotAction": [
                "lambda:AddPermission",
                "lambda:PutFunctionConcurrency"
            ],
            "Resource": "arn:aws:lambda:*:*:function:intern-*"
        },
        {
            "Sid": "DevelopEventSourceMappings",
            "Effect": "Allow",
            "Action": [
                "lambda:DeleteEventSourceMapping",
                "lambda:UpdateEventSourceMapping",
                "lambda:CreateEventSourceMapping"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
                }
            }
        },
        {
            "Sid": "PassExecutionRole",
            "Effect": "Allow",
            "Action": [
                "iam:ListRolePolicies",
                "iam:ListAttachedRolePolicies",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:PassRole",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "arn:aws:iam::*:role/intern-lambda-execution-role"
        },
        {
            "Sid": "ViewLogs",
            "Effect": "Allow",
            "Action": [
                "logs:*"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*"
        }
    ]
}
```

Die Berechtigungen in der Richtlinie sind in Anweisungen basierend auf den Ressourcen und Bedingungen organisiert, die sie unterstützen.

- `ReadOnlyPermissions` – Die Lambda-Konsole verwendet diese Berechtigungen, wenn Sie Funktionen durchsuchen und anzeigen. Sie unterstützen keine Ressourcenmuster oder -bedingungen.

```
            "Action": [
                "lambda:GetAccountSettings",
                "lambda:GetEventSourceMapping",
                "lambda:GetFunction",
```

```
            "lambda:GetFunctionConfiguration",
            "lambda:GetFunctionCodeSigningConfig",
            "lambda:GetFunctionConcurrency",
            "lambda:ListEventSourceMappings",
            "lambda:ListFunctions",
            "lambda:ListTags",
            "iam:ListRoles"
        ],
        "Resource": "*"
```

- `DevelopFunctions` – Verwendet eine beliebige Lambda-Aktion, die auf Funktionen mit dem Präfix `intern-` ausgeführt wird, ausgenommen`AddPermission` und `PutFunctionConcurrency`. `AddPermission` ändert die ressourcenbasierte Richtlinie der Funktion und kann mögliche Sicherheitsprobleme darstellen. `PutFunctionConcurrency` reserviert Skalierungskapazitäten für eine Funktion und kann anderen Funktionen Kapazitäten wegnehmen.

```
        "NotAction": [
            "lambda:AddPermission",
            "lambda:PutFunctionConcurrency"
        ],
        "Resource": "arn:aws:lambda:*:*:function:intern-*"
```

- `DevelopEventSourceMappings` – Verwaltet Ereignis-Quellzuweisungen für Funktionen mit dem Präfix `intern-`. Diese Aktionen werden für Ereignis-Quellzuweisungen angewendet. Sie können sie jedoch mit einer Bedingung nach Funktion einschränken.

```
        "Action": [
            "lambda:DeleteEventSourceMapping",
            "lambda:UpdateEventSourceMapping",
            "lambda:CreateEventSourceMapping"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "lambda:FunctionArn": "arn:aws:lambda:*:*:function:intern-*"
            }
        }
```

- `PassExecutionRole` – Zeigt und übergibt nur eine Rolle namens `intern-lambda-execution-role`, die von einem Benutzer mit IAM-Berechtigungen erstellt und verwaltet werden muss. `PassRole` wird verwendet, wenn Sie eine Ausführungsrolle einer Funktion zuweisen.

```
        "Action": [
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies",
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:PassRole",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "arn:aws:iam::*:role/intern-lambda-execution-role"
```

- `ViewLogs`— Verwenden Sie CloudWatch Logs, um Logs für Funktionen anzuzeigen, denen das Präfix vorangestellt ist. `intern-`

```
        "Action": [
            "logs:*"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/intern-*"
```

Diese Richtlinie erlaubt es einem Benutzer, Lambda zu verwenden, ohne die Ressourcen anderer Benutzer zu gefährden. Es erlaubt einem Benutzer nicht, eine Funktion so zu konfigurieren, dass sie von anderen AWS Diensten ausgelöst wird oder diese aufruft, wofür umfassendere IAM-Berechtigungen erforderlich sind. Es beinhaltet auch keine Genehmigung für Dienste, die keine Richtlinien mit begrenztem Geltungsbereich unterstützen, wie X-Ray CloudWatch . Verwenden Sie die schreibgeschützten Richtlinien für diese Services, um dem Benutzer Zugriff auf Metriken und Ablaufverfolgungsdaten zu gewähren.

Wenn Sie Auslöser für Ihre Funktion konfigurieren, benötigen Sie Zugriff, um den AWS Dienst verwenden zu können, der Ihre Funktion aufruft. Wenn Sie z. B. einen Amazon-S3-Auslöser konfigurieren, müssen Sie zur Verwendung der Amazon-S3-Aktionen berechtigt sein, mit denen Bucket-Benachrichtigungen verwaltet werden. Viele dieser Berechtigungen sind in der AWSLambdaFullAccessverwalteten Richtlinie enthalten. Beispielrichtlinien sind im GitHubRepository dieses Handbuchs verfügbar.

Schreiben Sie eine Beispielrichtlinie, die Berechtigungen zur Verwendung von Ebenen gewährt

Die folgende Richtlinie erteilt einem Benutzer die Berechtigung, Ebenen zu erstellen und sie mit Funktionen zu verwenden. Die Ressourcenmuster ermöglichen es dem Benutzer, in jeder AWS Region und mit jeder Layer-Version zu arbeiten, sofern der Name der Ebene mit beginnt`test-`.

Example Richtlinie für die Ebenenentwicklung

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublishLayers",
            "Effect": "Allow",
            "Action": [
                "lambda:PublishLayerVersion"
            ],
            "Resource": "arn:aws:lambda:*:*:layer:test-*"
        },
        {
            "Sid": "ManageLayerVersions",
            "Effect": "Allow",
            "Action": [
                "lambda:GetLayerVersion",
                "lambda:DeleteLayerVersion"
            ],
            "Resource": "arn:aws:lambda:*:*:layer:test-*:*"
        }
    ]
}
```

Sie können die Ebenenverwendung auch bei der Erstellung und Konfiguration von Funktionen mit der `lambda:Layer`-Bedingung erzwingen. Sie können beispielsweise Benutzer daran hindern, Ebenen zu verwenden, die von anderen Konten veröffentlicht wurden. Die folgende Richtlinie fügt eine Bedingung zu den Aktionen `CreateFunction` und `UpdateFunctionConfiguration` hinzu, um zu verlangen, dass alle angegebenen Ebenen vom Konto `123456789012` stammen.

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

```
            "Sid": "ConfigureFunctions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:UpdateFunctionConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringLike": {
                    "lambda:Layer": [
                        "arn:aws:lambda:*:123456789012:layer:*:*"
                    ]
                }
            }
        }
    ]
}
```

Um sicherzustellen, dass die Bedingung angewendet wird, stellen Sie sicher, dass keine anderen Anweisungen dem Benutzer die Berechtigung für diese Aktionen erteilen.

Implementierung eines kontenübergreifenden Zugriffs mit identitätsbasierten Richtlinien

Sie können die vorherigen Richtlinien und Anweisungen auf eine Rolle anwenden, die Sie dann für ein anderes Konto freigeben können, um diesem Zugriff auf Ihre Lambda-Ressourcen zu gewähren. Im Gegensatz zu einem Benutzer hat eine Rolle keine Anmeldeinformationen für die Authentifizierung. Stattdessen verfügt sie über eine Vertrauensrichtlinie, die angibt, wer die Rolle übernehmen und ihre Berechtigungen verwenden darf.

Sie können kontoübergreifende Rollen verwenden, um Konten, denen Sie vertrauen, Zugriff auf Lambda-Aktionen und -Ressourcen zu gewähren. Wenn Sie nur die Berechtigung erteilen möchten, eine Funktion aufzurufen oder eine Ebene zu verwenden, nutzen Sie stattdessen ressourcenbasierte Richtlinien.

Weitere Informationen finden Sie unter IAM-Rollen im IAM-Benutzerhandbuch.

Arbeiten mit ressourcenbasierten Richtlinien in Lambda

Lambda unterstützt ressourcenbasierte Berechtigungsrichtlinien für Lambda-Funktionen und -Ebenen. Mit ressourcenbasierten Richtlinien können Sie anderen AWS Konten oder Organisationen

Nutzungsberechtigungen pro Ressource erteilen. Sie verwenden auch eine ressourcenbasierte Richtlinie, um einem AWS Dienst zu ermöglichen, Ihre Funktion in Ihrem Namen aufzurufen.

Für Lambda-Funktionen können Sie eine Kontoberechtigung erteilen, um eine Funktion aufzurufen oder zu verwalten. Außerdem können Sie eine einzelne ressourcenbasierte Richtlinie verwenden, um einer gesamten Organisation Berechtigungen in AWS Organizations zu erteilen. Sie können ressourcenbasierte Richtlinien auch verwenden, um einem AWS Dienst, der eine Funktion als Reaktion auf Aktivitäten in Ihrem Konto aufruft, die Aufrufberechtigung zu erteilen.

So zeigen Sie die ressourcenbasierte Richtlinie einer Funktion an

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Konfiguration und anschließend Berechtigungen aus.
4. Scrollen Sie nach unten zu Ressourcenbasierte Richtlinie und wählen Sie dann Richtliniendokument anzeigen aus. Die ressourcenbasierte Richtlinie zeigt die Berechtigungen, die angewendet werden, wenn ein anderes Konto oder ein anderer AWS Dienst versucht, auf die Funktion zuzugreifen. Das folgende Beispiel zeigt eine Anweisung, mit der Amazon S3 eine Funktion mit dem Namen `my-function` für einen Bucket mit dem Namen `DOC-EXAMPLE-BUCKET` im Konto `123456789012` aufrufen kann.

   Example Ressourcenbasierte Richtlinie

```
{
    "Version": "2012-10-17",
    "Id": "default",
    "Statement": [
        {
            "Sid": "lambda-allow-s3-my-function",
            "Effect": "Allow",
            "Principal": {
              "Service": "s3.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource":  "arn:aws:lambda:us-east-2:123456789012:function:my-
function",
            "Condition": {
              "StringEquals": {
                "AWS:SourceAccount": "123456789012"
              },
```

```
                "ArnLike": {
                  "AWS:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-BUCKET"
                }
              }
            }
        ]
}
```

Für Lambda-Ebenen können Sie nur eine ressourcenbasierte Richtlinie für eine bestimmte Ebenen-Version anstelle der gesamten Ebene verwenden. Zusätzlich zu den Richtlinien, die Berechtigungen für ein einzelnes Konto oder alle Konten erteilen, können Sie für Ebenen auch die Berechtigung für alle Konten in einer Organisation erteilen.

> **Note**
>
> Sie können ressourcenbasierte Richtlinien für Lambda-Ressourcen nur im Rahmen der AddPermissionund AddLayerVersionPermissionAPI-Aktionen aktualisieren. Derzeit können Sie keine Richtlinien für Ihre Lambda-Ressourcen in JSON erstellen oder Bedingungen verwenden, die mit keinen Parametern für diese Aktionen verknüpft sind.

Ressourcenbasierte Richtlinien gelten für einzelne Funktionen, Versionen, Aliasnamen oder Ebenenversionen. Sie gewähren die Berechtigung für einen oder mehrere Services bzw. Konten. Bei vertrauenswürdigen Konten, die Zugriff auf mehrere Ressourcen haben sollen, oder für die Verwendung von API-Aktionen, die ressourcenbasierte Richtlinien nicht unterstützen, können Sie kontoübergreifenden Rollen verwenden.

Themen

- Unterstützte API-Aktionen
- Funktionszugriff auf AWS Dienste gewähren
- Gewähren des Funktionszugriffs auf eine Organisation
- Gewähren des Funktionszugriffs für andere Konten
- Gewähren des Ebenenzugriffs für andere Konten
- Bereinigen von ressourcenbasierten Richtlinien

Unterstützte API-Aktionen

Die folgenden Lambda-API-Aktionen unterstützen ressourcenbasierte Richtlinien:

- CreateAlias
- DeleteAlias
- DeleteFunction
- DeleteFunctionParallelität
- DeleteFunctionEventInvokeConfig
- DeleteProvisionedConcurrencyConfig
- GetAlias
- GetFunction
- GetFunctionParallelität
- GetFunctionKonfiguration
- GetFunctionEventInvokeConfig
- GetPolicy
- GetProvisionedConcurrencyConfig
- Aufrufen
- ListAliases
- ListFunctionEventInvokeKonfigurationen
- ListProvisionedConcurrencyConfigs
- ListTags
- ListVersionsByFunction
- PublishVersion
- PutFunctionParallelität
- PutFunctionEventInvokeConfig
- PutProvisionedConcurrencyConfig
- TagResource
- UntagResource
- UpdateAlias
- UpdateFunctionKode
- UpdateFunctionEventInvokeConfig

Funktionszugriff auf AWS Dienste gewähren

Wenn Sie einen AWS Dienst verwenden, um Ihre Funktion aufzurufen, erteilen Sie die Erlaubnis in einer Erklärung zu einer ressourcenbasierten Richtlinie. Sie können die Anweisung auf die gesamte Funktion anwenden, die aufgerufen oder verwaltet werden soll, oder die Anweisung auf eine einzelne Version oder einen einzelnen Alias beschränken.

> **Note**
>
> Wenn Sie Ihrer Funktion mit der Lambda-Konsole einen Auslöser hinzufügen, aktualisiert die Konsole die ressourcenbasierte Richtlinie der Funktion, damit der Service sie aufrufen kann. Um Berechtigungen für andere Konten oder Services zu erteilen, die in der Lambda-Konsole nicht verfügbar sind, verwenden Sie die AWS CLI-CLI.

Fügen Sie eine Anweisung mit dem Befehl `add-permission` hinzu. Die einfachste ressourcenbasierte Richtlinienanweisung ermöglicht es einem Service, eine Funktion aufzurufen. Der folgende Befehl gewährt die Amazon-SNS-Berechtigung zum Aufrufen einer Funktion namens `my-function`:

```
aws lambda add-permission --function-name my-function --action lambda:InvokeFunction --
statement-id sns \
    --principal sns.amazonaws.com --output text
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{"Sid":"sns","Effect":"Allow","Principal":
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:us-
east-2:123456789012:function:my-function"}
```

Auf diese Weise kann Amazon SNS die API `lambda:Invoke` für die Funktion aufrufen, ohne das Amazon-SNS-Thema einzuschränken, durch das der Aufruf ausgelöst wird. Um sicherzustellen, dass Ihre Funktion nur von einer bestimmten Ressource aufgerufen wird, geben Sie den Amazon-Ressourcennamen (ARN) der Ressource mit der Option `source-arn` an. Der folgende Befehl erlaubt Amazon SNS nur das Aufrufen der Funktion für Abonnements für ein Thema namens `my-topic`.

```
aws lambda add-permission --function-name my-function --action lambda:InvokeFunction --
statement-id sns-my-topic \
```

```
    --principal sns.amazonaws.com --source-arn arn:aws:sns:us-east-2:123456789012:my-
topic
```

Einige Services können Funktionen in anderen Konten aufrufen. Wenn Sie einen Quell-ARN angeben, der Ihre Konto-ID enthält, ist das kein Problem. Für Amazon S3 ist die Quelle jedoch ein Bucket, dessen ARN nicht über eine Konto-ID verfügt. Es ist möglich, dass Sie den Bucket löschen und ein anderes Konto einen Bucket mit demselben Namen erstellt. Verwenden Sie die Option `source-account` mit Ihrer Konto-ID, um sicherzustellen, dass nur Ressourcen in Ihrem Konto die Funktion aufrufen können.

```
aws lambda add-permission --function-name my-function --action lambda:InvokeFunction --
statement-id s3-account \
    --principal s3.amazonaws.com --source-arn arn:aws:s3:::DOC-EXAMPLE-BUCKET --source-
account 123456789012
```

Gewähren des Funktionszugriffs auf eine Organisation

Um einer Organisation Berechtigungen zu erteilen AWS Organizations, geben Sie die Organisations-ID als. `principal-org-id` Der folgende AddPermission AWS CLI Befehl gewährt allen Benutzern in der Organisation `o-a1b2c3d4e5f` Aufrufzugriff.

```
aws lambda add-permission --function-name example \
    --statement-id PrincipalOrgIDExample --action lambda:InvokeFunction \
    --principal * --principal-org-id o-a1b2c3d4e5f
```

> **Note**
>
> In diesem Befehl ist `Principal *`. Dies bedeutet, dass alle Benutzer in der Organisation `o-a1b2c3d4e5f` Berechtigungen für den Funktionsaufruf erhalten. Wenn Sie ein AWS Konto oder eine Rolle als angeben`Principal`, erhält nur dieser Prinzipal die Berechtigungen zum Aufrufen von Funktionen, aber nur, wenn er auch Teil der `o-a1b2c3d4e5f` Organisation ist.

Dieser Befehl erstellt eine ressourcenbasierte Richtlinie, die wie folgt aussieht:

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

```
            "Sid": "PrincipalOrgIDExample",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:example",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-a1b2c3d4e5f"
                }
            }
        }
    ]
}
```

Weitere Informationen finden Sie unter aws: PrincipalOrg ID im AWS Identity and Access Management Benutzerhandbuch.

Gewähren des Funktionszugriffs für andere Konten

Um einem anderen AWS Konto Berechtigungen zu gewähren, geben Sie die Konto-ID als`principal`. Im folgenden Beispiel wird dem Konto `111122223333` die Berechtigung zum Aufrufen von `my-function` mit dem Alias `prod` erteilt.

```
aws lambda add-permission --function-name my-function:prod --statement-id xaccount --
action lambda:InvokeFunction \
    --principal 111122223333 --output text
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:l
east-2:123456789012:function:my-function"}
```

Die ressourcenbasierte Richtlinie erteilt dem anderen Konto die Berechtigung für den Zugriff auf die Funktion, erlaubt den Benutzern in diesem Konto jedoch nicht, ihre Berechtigungen zu überschreiten. Benutzer in dem anderen Konto müssen über die entsprechenden Benutzerberechtigungen verfügen, um die Lambda-API verwenden zu können.

Um den Zugriff auf einen Benutzer oder eine Rolle in einem anderen Konto einzuschränken, geben Sie den vollständigen ARN der Identität als Prinzipal an. Beispiel, `arn:aws:iam::123456789012:user/developer`.

Der Alias schränkt ein, welche Version das andere Konto aufrufen kann. Dies erfordert, dass das andere Konto den Alias in den ARN der Funktion einschließt.

```
aws lambda invoke --function-name arn:aws:lambda:us-west-2:123456789012:function:my-function:prod out
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "1"
}
```

Der Funktionsbesitzer kann dann den Alias so aktualisieren, dass er auf eine neue Version verweist, ohne dass der Aufrufer die Methode ändern muss, mit der er Ihre Funktion aufruft. Dadurch wird sichergestellt, dass das andere Konto seinen Code nicht ändern muss, um die neue Version zu verwenden, und nur zum Aufruf der Version der Funktion berechtigt ist, die dem Alias zugeordnet ist.

Sie können kontoübergreifenden Zugriff für die meisten API-Aktionen erteilen, die für eine vorhandene Funktion ausgeführt werden. Beispielsweise könnten Sie Zugriff auf `lambda:ListAliases` gewähren, damit ein Konto eine Liste der Aliasse abrufen kann, oder `lambda:GetFunction`, damit es Ihren Funktionscode herunterladen kann. Fügen Sie jede Berechtigung separat hinzu oder verwenden Sie `lambda:*`, um Zugriff auf alle Aktionen der angegebenen Funktion zu gewähren.

Um anderen Konten Berechtigungen für mehrere Funktionen oder für Aktionen zu erteilen, die nicht für eine Funktion ausgeführt werden, empfehlen wir die Verwendung von IAM-Rollen.

Gewähren des Ebenenzugriffs für andere Konten

Um einem anderen Konto Nutzungsberechtigungen für Ebenen zu erteilen, fügen Sie der Berechtigungsrichtlinie der Ebenenversion mithilfe des Befehls add-layer-version-permission eine Anweisung hinzu. In jeder Anweisung können Sie einem einzelnen Konto, allen Konten oder einer Organisation eine Berechtigung erteilen.

Im folgenden Beispiel wird dem Konto 111122223333 Zugriff auf Version 2 der `bash-runtime`-Ebene gewährt.

```
aws lambda add-layer-version-permission --layer-name bash-runtime --statement-id
 xaccount \
```

```
--action lambda:GetLayerVersion --principal 111122223333 --version-number 2 --output
 text
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
e210ffdc-e901-43b0-824b-5fcd0dd26d16    {"Sid":"xaccount","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"lambda:GetLayerVersion","Resource":"arn:aws:
east-1:123456789012:layer:bash-runtime:2"}
```

Berechtigungen gelten nur für eine Version mit einer Ebene. Wiederholen Sie den Vorgang bei jeder Erstellung einer neuen Ebenenversion.

Um Berechtigungen für alle Konten in einer Organisation zu erteilen, verwenden Sie die Option `organization-id`. Im folgenden Beispiel wird allen Konten in einer Organisation die Berechtigung für die Verwendung von Version 3 einer Ebene erteilt.

```
aws lambda add-layer-version-permission --layer-name my-layer \
    --statement-id engineering-org --version-number 3 --principal '*' \
    --action lambda:GetLayerVersion --organization-id o-t194hfs8cz --output text
```

Die Ausgabe sollte folgendermaßen aussehen:

```
b0cd9796-d4eb-4564-939f-de7fe0b42236    {"Sid":"engineering-
org","Effect":"Allow","Principal":"*","Action":"lambda:GetLayerVersion","Resource":"arn:aws:lam
east-2:123456789012:layer:my-layer:3","Condition":{"StringEquals":
{"aws:PrincipalOrgID":"o-t194hfs8cz"}}}"
```

Um allen AWS Konten Berechtigungen zu erteilen, verwenden Sie * für den Prinzipal und lassen Sie die Organisations-ID weg. Für mehrere Konten oder Organisationen müssen Sie mehrere Anweisungen hinzufügen.

Bereinigen von ressourcenbasierten Richtlinien

Um die ressourcenbasierte Richtlinie einer Funktion anzuzeigen, verwenden Sie den Befehl `get-policy`.

```
aws lambda get-policy --function-name my-function --output text
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{"Version":"2012-10-17","Id":"default","Statement":
[{"Sid":"sns","Effect":"Allow","Principal":
{"Service":"s3.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lambda:us-
east-2:123456789012:function:my-function","Condition":{"ArnLike":
{"AWS:SourceArn":"arn:aws:sns:us-east-2:123456789012:lambda*"}}}]}      7c681fc9-
b791-4e91-acdf-eb847fdaa0f0
```

Fügen Sie bei Versionen und Aliassen die Versionsnummer oder den Alias an den Funktionsnamen an.

```
aws lambda get-policy --function-name my-function:PROD
```

Um Berechtigungen von Ihrer Funktion zu entfernen, verwenden Sie `remove-permission`.

```
aws lambda remove-permission --function-name example --statement-id sns
```

Verwenden Sie den Befehl `get-layer-version-policy`, um die Berechtigungen für einen Layer anzuzeigen.

```
aws lambda get-layer-version-policy --layer-name my-layer --version-number 3 --output
 text
```

Die Ausgabe sollte folgendermaßen aussehen:

```
b0cd9796-d4eb-4564-939f-de7fe0b42236    {"Sid":"engineering-
org","Effect":"Allow","Principal":"*","Action":"lambda:GetLayerVersion","Resource":"arn:aws:lam
west-2:123456789012:layer:my-layer:3","Condition":{"StringEquals":
{"aws:PrincipalOrgID":"o-t194hfs8cz"}}}"
```

Verwenden Sie `remove-layer-version-permission`, um Anweisungen aus der Richtlinie zu entfernen.

```
aws lambda remove-layer-version-permission --layer-name my-layer --version-number 3 --
statement-id engineering-org
```

Verwendung der attributbasierten Zugriffskontrolle in Lambda

Mit attributbasierter Zugriffskontrolle (ABAC) können Sie Tags verwenden, um den Zugriff auf Ihre Lambda-Funktionen zu steuern. Sie können Tags an eine Lambda-Funktion anhängen, sie in

bestimmten API-Anfragen übergeben oder sie an den AWS Identity and Access Management (IAM-) Principal anhängen, der die Anfrage stellt. Weitere Informationen darüber, wie attributebasierten Zugriff AWS gewährt wird, finden Sie im IAM-Benutzerhandbuch unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags.

Sie können ABAC verwenden, um die geringsten Berechtigungen zu gewähren, ohne einen Amazon-Ressourcennamen (ARN) oder ein ARN-Muster in der IAM-Richtlinie anzugeben. Stattdessen können Sie ein Tag im Bedingungselement einer IAM-Richtlinie angeben, um den Zugriff zu steuern. Die Skalierung ist mit ABAC einfacher, da Sie Ihre IAM-Richtlinien nicht aktualisieren müssen, wenn Sie neue Funktionen erstellen. Fügen Sie stattdessen Tags zu den neuen Funktionen hinzu, um den Zugriff zu steuern.

In Lambda funktionieren Tags auf Funktionsebene. Tags werden für Ebenen, Codesignaturkonfigurationen oder Ereignisquellenzuordnungen nicht unterstützt. Wenn Sie eine Funktion kennzeichnen, gelten diese Tags für alle Versionen und Aliase, die mit der Funktion verknüpft sind. Weitere Informationen zum Erstellen von Tag-Funktionen finden Sie unter Verwenden von Tags für Lambda-Funktionen.

Sie können die folgenden Bedingungsschlüsseln verwenden, um Funktionsaktionen zu steuern:

- aws: ResourceTag /tag-key: Steuert den Zugriff auf der Grundlage der Tags, die an Lambda-Funktionen angehängt sind.
- aws: RequestTag /tag-key: Erfordert, dass Tags in einer Anfrage vorhanden sind, z. B. beim Erstellen einer neuen Funktion.
- aws: PrincipalTag /tag-key : Steuert anhand der Tags, die ihrem IAM-Benutzer oder ihrer IAM-Rolle zugewiesen sind, was der IAM-Prinzipal (die Person, die die Anfrage stellt) tun darf.
- aws:TagKeys: Steuert, ob bestimmte Tag-Schlüssel in einer Anfrage verwendet werden können.

Eine vollständige Liste der Lambda-Aktionen, die ABAC unterstützen, finden Sie unter Unterstützte Funktionsaktionen und überprüfen Sie die Spalte Condition (Bedingung) in der Tabelle.

Die folgenden Schritte zeigen eine Möglichkeit, Berechtigungen mithilfe von ABAC einzurichten. In diesem Beispielszenario erstellen Sie vier IAM-Berechtigungsrichtlinien. Anschließend fügen Sie diese Richtlinien einer neuen IAM-Rolle hinzu. Schließlich erstellen Sie einen IAM-Benutzer und erteilen diesem Benutzer die Berechtigung, die neue Rolle zu übernehmen.

Themen

- Voraussetzungen

- Schritt 1: Tags für neue Funktionen anfordern
- Schritt 2: Aktionen basierend auf Tags zulassen, die einer Lambda-Funktion und einem IAM-Prinzipal zugeordnet sind
- Schritt 3: Erteilen von Listenberechtigungen
- Schritt 4: Erteilen von IAM-Berechtigungen
- Schritt 5: Erstellen der IAM-Rolle
- Schritt 6: Erstellen eines IAM-Benutzers
- Schritt 7: Testen der Berechtigungen
- Schritt 8: Bereinigen Sie Ihre Ressourcen

Voraussetzungen

Stellen Sie sicher, dass Sie über eine Lambda-Ausführungsrolle verfügen. Sie verwenden diese Rolle, wenn Sie IAM-Berechtigungen erteilen und eine Lambda-Funktion erstellen.

Schritt 1: Tags für neue Funktionen anfordern

Wenn Sie ABAC mit Lambda verwenden, empfiehlt es sich, dass alle Funktionen über Tags verfügen. Auf diese Weise können Sie sicherstellen, dass Ihre ABAC-Berechtigungsrichtlinien wie erwartet funktionieren.

Erstellen Sie eine IAM-Richtlinie ähnlich dem folgenden Beispiel. Diese Richtlinie verwendet die TagKeys Bedingungsschlüssel aws: RequestTag /tag-key, aws: ResourceTag /tag-key und aws:, um zu verlangen, dass neue Funktionen und der IAM-Prinzipal, der die Funktionen erstellt, beide das Tag haben. `project` Der `ForAllValues`-Modifikator stellt sicher, dass `project` das einzige zulässige Tag ist. Wenn Sie den `ForAllValues`-Modifikator nicht angeben, können die Benutzer der Funktion andere Tags hinzufügen, solange diese auch `project` übergeben.

Example – Tags für neue Funktionen anfordern

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction",
      "lambda:TagResource"
```

```
    ],
    "Resource": "arn:aws:lambda:*:*:function:*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/project": "${aws:PrincipalTag/project}",
        "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": "project"
      }
    }
  }
}
```

Schritt 2: Aktionen basierend auf Tags zulassen, die einer Lambda-Funktion und einem IAM-Prinzipal zugeordnet sind

Erstellen Sie eine zweite IAM-Richtlinie mithilfe des ResourceTagBedingungsschlüssels aws: / tag-key, um zu verlangen, dass das Tag des Prinzipals mit dem Tag übereinstimmt, das an die Funktion angehängt ist. Die folgende Beispielrichtlinie erlaubt es Prinzipalen mit dem `project`-Tag, Funktionen mit dem `project`-Tag aufzurufen. Wenn eine Funktion andere Tags hat, wird die Aktion verweigert.

Example – Erfordert übereinstimmende Tags für Funktion und IAM-Prinzipal

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:*:function:*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
```

```
}
```

Schritt 3: Erteilen von Listenberechtigungen

Erstellen Sie eine Richtlinie, die es dem Prinzipal ermöglicht, Lambda-Funktionen und IAM-Rollen aufzulisten. Dadurch kann der Prinzipal alle Lambda-Funktionen und IAM-Rollen auf der Konsole und beim Aufrufen der API-Aktionen sehen.

Example – Erteilen von Lambda- und IAM-Listenberechtigungen

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllResourcesLambdaNoTags",
      "Effect": "Allow",
      "Action": [
        "lambda:GetAccountSettings",
        "lambda:ListFunctions",
        "iam:ListRoles"
      ],
      "Resource": "*"
    }
  ]
}
```

Schritt 4: Erteilen von IAM-Berechtigungen

Erstellen Sie eine Richtlinie, die iam: zulässt. PassRole Diese Berechtigung ist erforderlich, wenn Sie einer Funktion eine Ausführungsrolle zuweisen. Ersetzen Sie in der folgenden Beispielrichtlinie den Beispiel-ARN durch den ARN Ihrer Lambda-Ausführungsrolle.

> **Note**
>
> Verwenden Sie den `ResourceTag`-Bedingungsschlüssel nicht in einer Richtlinie mit der `iam:PassRole`-Aktion. Sie können das Tag nicht für eine IAM-Rolle verwenden, um zu steuern, wer Zugriff zur Weiterleitung diese Rolle haben soll. Weitere Informationen zu den Berechtigungen, die für die Übergabe einer Rolle an einen Dienst erforderlich sind, finden Sie unter Einem Benutzer Berechtigungen zur Übergabe einer Rolle an einen AWS Dienst gewähren.

Example – Erteilt die Berechtigung zum Übergeben der Ausführungsrolle

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/lambda-ex"
    }
  ]
}
```

Schritt 5: Erstellen der IAM-Rolle

Es hat sich bewährt, Rollen zum Delegieren von Berechtigungen zu verwenden. Erstellen Sie eine IAM-Rolle mit dem Namen `abac-project-role`:

- In Schritt 1: Vertrauenswürdige Entität auswählen: Wählen Sie wählen AWS -Konto und wählen Sie dann Dieses Konto.
- In Schritt 2: Hinzufügen von Berechtigungen: Fügen Sie die vier IAM-Richtlinien hinzu, die Sie in den vorherigen Schritten erstellt haben.
- In Schritt 3: Benennen, Überprüfen und Erstellen: Wählen Sie Tag hinzufügen. Geben Sie für Key (Schlüssel) `project` ein. Geben Sie keinen Value (Wert) ein.

Schritt 6: Erstellen eines IAM-Benutzers

Erstellen Sie einen IAM-Benutzer mit dem Namen `abac-test-user`. Wählen Sie im Abschnitt Set permissions (Berechtigungen festlegen) die Option Attach existing policies directly (Vorhandene Richtlinien direkt anhängen) und dann Create policy (Richtlinie erstellen) aus. Geben Sie die folgende Richtliniendefinition ein. Ersetzen Sie *111122223333* durch Ihre AWS -Konto-ID. Diese Richtlinie erlaubt es `abac-test-user`, `abac-project-role` anzunehmen.

Example – IAM-Benutzer die Übernahme der ABAC-Rolle erlauben

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::111122223333:role/abac-project-role"
  }
}
```

Schritt 7: Testen der Berechtigungen

1. Melden Sie sich an der AWS Konsole an als`abac-test-user`. Weitere Informationen finden Sie unter Anmeldung als IAM-Benutzer.
2. Wechseln Sie zur `abac-project-role`-Rolle. Weitere Informationen finden Sie unter Wechseln zu einer Rolle (Konsole).
3. Erstellen einer Lambda-Funktion:
   - Wählen Sie unter Permissions (Berechtigungen) die Option Change default execution role (Standardausführungsrolle ändern) und dann unter Execution role (Ausführungsrolle) die Option Use an existing role (Vorhandene Rolle verwenden). Wählen Sie dieselbe Ausführungsrolle aus, die Sie in Schritt 4: Erteilen von IAM-Berechtigungen verwendet haben.
   - Wählen Sie unter Advanced settings (Erweiterte Einstellungen) die Option Enable tags (Tags ermöglichen) und wählen Sie dann Add new tag (Neues Tag hinzufügen). Geben Sie für Key (Schlüssel) `project` ein. Geben Sie keinen Value (Wert) ein.
4. Testen der Funktion.
5. Erstellen Sie eine zweite Lambda-Funktion und fügen Sie ein anderes Tag hinzu, z. B. `environment`. Dieser Vorgang sollte fehlschlagen, da die ABAC-Richtlinie, die Sie in Schritt 1: Tags für neue Funktionen anfordern erstellt haben, dem Prinzipal nur erlaubt, Funktionen mit dem `project`-Tag zu erstellen.
6. Erstellen Sie eine dritte Funktion ohne Tags. Dieser Vorgang sollte fehlschlagen, weil die ABAC-Richtlinie, die Sie in Schritt 1: Tags für neue Funktionen anfordern erstellt haben, dem Prinzipal nicht erlaubt, Funktionen ohne Tags zu erstellen.

Mit dieser Autorisierungsstrategie können Sie den Zugriff steuern, ohne für jeden neuen Benutzer neue Richtlinien erstellen zu müssen. Um neuen Benutzern Zugriff zu gewähren, erteilen Sie ihnen einfach die Berechtigung, die Rolle zu übernehmen, die ihrem zugewiesenen Projekt entspricht.

Schritt 8: Bereinigen Sie Ihre Ressourcen

Löschen Sie die IAM-Rolle wie folgt:

1. Öffnen Sie die Seite Roles (Rollen) in der IAM-Konsole.
2. Wählen Sie die Rolle aus, die Sie in Schritt 5 erstellt haben.
3. Wählen Sie Löschen aus.
4. Um das Löschen zu bestätigen, geben Sie den Rollennamen in das Texteingabefeld ein.
5. Wählen Sie Löschen aus.

Um den IAM-Benutzer zu löschen

1. Öffnen Sie die Seite Benutzer der IAM-Konsole.
2. Wählen Sie den IAM-Benutzer aus, den Sie in Schritt 6 erstellt haben.
3. Wählen Sie Löschen aus.
4. Um das Löschen zu bestätigen, geben Sie den Benutzernamen in das Texteingabefeld ein.
5. Wählen Sie Benutzer löschen.

So löschen Sie die Lambda-Funktion:

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die Funktion aus, die Sie erstellt haben.
3. Wählen Sie Aktionen, Löschen aus.
4. Geben Sie **`delete`** in das Texteingabefeld ein und wählen Sie Delete (Löschen) aus.

Feinabstimmung der Abschnitte „Ressourcen“ und „Bedingungen“ der Richtlinien

Sie können den Umfang der Berechtigungen eines Benutzers einschränken, indem Sie Ressourcen und Bedingungen in einer AWS Identity and Access Management (IAM)-Richtlinie angeben. Jede Aktion in einer Richtlinie unterstützt eine Kombination aus Ressourcen- und Bedingungstypen, die je nach Verhalten der Aktion variiert.

Jede IAM-Richtlinienanweisung erteilt die Berechtigung für eine Aktion, die auf eine Ressource ausgeführt wird. Wenn die Aktion nicht auf eine benannte Ressource reagiert oder Sie die

Berechtigung zum Ausführen der Aktion für alle Ressourcen erteilen, wird der Wert der Ressource in der Richtlinie als Platzhalter () dargeste (*). Für viele Aktionen können Sie die Ressourcen einschränken, die ein Benutzer ändern kann, indem Sie den Amazon-Ressourcennamen (ARN) einer Ressource oder ein ARN-Muster angeben, das mehreren Ressourcen entspricht.

Zum Einschränken von Berechtigungen nach Ressource bestimmen Sie die Ressource unter Angabe des ARN.

Format des Lambda-Ressourcen-ARN

- Funktion – `arn:aws:lambda:us-west-2:123456789012:function:my-function`
- Funktionsversion – `arn:aws:lambda:us-west-2:123456789012:function:my-function:1`
- Funktionsalias – `arn:aws:lambda:us-west-2:123456789012:function:my-function:TEST`
- Mapping von Ereignisquellen – `arn:aws:lambda:us-west-2:123456789012:event-source-mapping:fa123456-14a1-4fd2-9fec-83de64ad683de6d47`
- Ebene – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer`
- Ebenenversion – `arn:aws:lambda:us-west-2:123456789012:layer:my-layer:1`

Die folgende Richtlinie ermöglicht es einem Benutzer beispielsweise, eine Funktion AWS-Konto `123456789012` aufzurufen, die `my-function` in der Region USA West (Oregon) AWS benannt ist.

Example Aufrufen der Funktionsrichtlinie

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Invoke",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:my-function"
        }
    ]
}
```

Dies ist ein Sonderfall, da sich die Aktionskennung (`lambda:InvokeFunction`) von der API-Operation (Invoke) unterscheidet. Bei anderen Aktionen ist die Aktionskennung der Operationsname mit dem Präfix `lambda:`.

Sections

Grundlegendes zum Abschnitt „Bedingung“ in Richtlinien

Bedingungen sind ein optionales Richtlinienelement, das zusätzliche Logik anwendet, um zu bestimmen, ob eine Aktion zulässig ist. Zusätzlich zu gemeinsamen Bedingungen, die alle Aktionen unterstützen, definiert Lambda Bedingungstypen, die Sie verwenden können, um die Werte zusätzlicher Parameter für einige Aktionen einzuschränken.

Mit der Bedingung `lambda:Principal` können Sie beispielsweise den Service oder das Konto beschränken, für das ein Benutzer in der ressourcenbasierten Richtlinie einer Funktion Aufrufzugriff gewähren kann. Mit der folgenden Richtlinie kann ein Benutzer Amazon Simple Notification Service (Amazon SNS)-Themen die Berechtigung erteilen, eine Funktion mit dem Namen `test` aufzurufen.

Example Verwalten von Berechtigungen für Funktionsrichtlinien

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageFunctionPolicy",
            "Effect": "Allow",
            "Action": [
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:test:*",
            "Condition": {
                "StringEquals": {
                    "lambda:Principal": "sns.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

Die Bedingung erfordert, dass der Prinzipal Amazon SNS und kein anderer Service bzw. kein anderes Konto ist. Das Ressourcenmuster erfordert, dass der Funktionsname `test` lautet und eine Versionsnummer oder einen Alias enthält. Beispiel, `test:v1`.

Weitere Informationen zu Ressourcen und Bedingungen für Lambda und andere AWS Dienste finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Dienste in der Service Authorization Reference.

Referenzierung von Funktionen im Abschnitt „Ressourcen“ der Richtlinien

Sie referenzieren eine Lambda-Funktion in einer Richtlinienanweisung mithilfe eines Amazon-Ressourcennamens (ARN). Das Format des ARN für eine Funktion hängt davon ab, ob Sie die gesamte Funktion, eine Funktionsversion (unqualifiziert), eine Funktionsversion oder einen Alias referenzieren.

Bei Lambda-API-Aufrufen können Benutzer eine Version oder einen Alias angeben, indem sie einen Versions-ARN oder Alias-ARN im GetFunction`FunctionName`Parameter übergeben oder einen Wert im GetFunction`Qualifier`Parameter festlegen. Lambda trifft Autorisierungsentscheidungen, indem es das Ressourcenelement in der IAM-Richtlinie sowohl mit dem in API-Aufrufen übergebenen `FunctionName`n als auch dem `Qualifier` vergleicht. Wenn es keine Übereinstimmung gibt, lehnt Lambda die Anforderung ab.

Unabhängig davon, ob Sie eine Aktion für Ihre Funktion zulassen oder verweigern, müssen Sie die richtigen ARN-Typen für Funktionen in Ihrer Richtlinienanweisung verwenden, um die erwarteten Ergebnisse zu erzielen. Wenn Ihre Richtlinie beispielsweise auf den unqualifizierten ARN verweist, akzeptiert Lambda Anfragen, die auf den unqualifizierten ARN verweisen, lehnt jedoch Anfragen ab, die auf einen qualifizierten ARN verweisen.

> **Note**
>
> Sie können kein Platzhalterzeichen (*) verwenden, um die Konto-ID abzugleichen. Weitere Informationen zur zulässigen Syntax finden Sie unter IAM JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Example Zulassen des Aufrufs eines nicht qualifizierten ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction"
        }
    ]
}
```

Wenn Ihre Richtlinie auf einen bestimmten qualifizierten ARN verweist, akzeptiert Lambda Anfragen, die auf diesen ARN verweisen, lehnt aber Anfragen ab, die auf den nicht qualifizierten ARN oder einen anderen qualifizierten ARN verweisen, z. B. `myFunction:2`.

Example Zulassen des Aufrufs eines bestimmten qualifizierten ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction:1"
        }
    ]
}
```

Wenn Ihre Richtlinie mit `:*` einen qualifizierten ARN referenziert, akzeptiert Lambda alle qualifizierten ARN, lehnt jedoch Anfragen ab, die den unqualifizierten ARN referenzieren.

Example Zulassen des Aufrufs eines beliebigen qualifizierten ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction:*"
```

```
        }
    ]
}
```

Wenn Ihre Richtlinie mit * einen ARN referenziert, akzeptiert Lambda alle qualifizierten oder unqualifizierten ARNs.

Example Zulassen des Aufrufs eines beliebigen qualifizierten oder nicht qualifizierten ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-west-2:123456789012:function:myFunction*"
        }
    ]
}
```

Unterstützte Funktionsaktionen

Aktionen, die für eine Funktion verwender werden, können – wie in der folgenden Tabelle beschrieben – nach Funktion, Version oder Alias-ARN auf eine spezifische Funktion eingeschränkt werden. Aktionen, die keine Ressourcenbeschränkungen unterstützen, werden für alle Ressourcen gewährt (*).

Funktionsaktionen

Aktion	Ressource	Bedingung
AddPermission	Funktion	`lambda:Principal`
RemovePermission	Funktionsversion	`aws:ResourceTag/${TagKey}`
	Funktionsalias	`lambda:FunctionUrlAuthType`
Aufrufen	Funktion	`aws:ResourceTag/${TagKey}`
Berechtigung: `lambda:InvokeFunction`	Funktionsversion	`lambda:EventSourceToken`

Aktion	Ressource	Bedingung
	Funktionsalias	

CreateFunction	Funktion	`lambda:CodeSigningConfigArn`
		`lambda:Layer`
		`lambda:VpcIds`
		`lambda:SubnetIds`
		`lambda:SecurityGroupIds`
		`aws:ResourceTag/${TagKey}`
		`aws:RequestTag/${TagKey}`
		`aws:TagKeys`

UpdateFunctionKonfiguration	Funktion	`lambda:CodeSigningConfigArn`
		`lambda:Layer`
		`lambda:VpcIds`
		`lambda:SubnetIds`
		`lambda:SecurityGroupIds`
		`aws:ResourceTag/${TagKey}`

Aktion	Ressource	Bedingung
CreateAlias	Funktion	`aws:ResourceTag/${TagKey}`
DeleteAlias		
DeleteFunction		
DeleteFunctionCodeSigningConfig		
DeleteFunctionParallelität		
GetAlias		
GetFunction		
GetFunctionCodeSigningConfig		
GetFunctionParallelität		
GetFunctionKonfiguration		
GetPolicy		
ListProvisionedConcurrencyConfigs		
ListAliases		
ListTags		
ListVersionsByFunction		
PublishVersion		
PutFunctionCodeSigningConfig		
PutFunctionParallelität		
UpdateAlias		
UpdateFunctionKode		

Aktion	Ressource	Bedingung
CreateFunctionUrlConfig DeleteFunctionUrlConfig GetFunctionUrlConfig UpdateFunctionUrlConfig	Funktion Funktionsalias	lambda:FunctionUrlAuthType lambda:FunctionArn aws:ResourceTag/${TagKey}
ListFunctionUrlConfigs	Funktion	lambda:FunctionUrlAuthType
DeleteFunctionEventInvokeConfig GetFunctionEventInvokeConfig ListFunctionEventInvokeKonfigurationen PutFunctionEventInvokeConfig UpdateFunctionEventInvokeConfig	Funktion	aws:ResourceTag/${TagKey}
DeleteProvisionedConcurrencyConfig GetProvisionedConcurrencyConfig PutProvisionedConcurrencyConfig	Funktionsalias Funktionsversion	aws:ResourceTag/${TagKey}
GetAccountEinstellungen ListFunctions	*	None
TagResource	Funktion	aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys

Aktion	Ressource	Bedingung
UntagResource	Funktion	`aws:ResourceTag/${TagKey}` `aws:TagKeys`

Unterstützte Aktionen zur Zuordnung von Ereignisquellen

Für Ereignisquellenzuordnungen können Sie Lösch- und Aktualisierungsberechtigungen auf eine bestimmte Ereignisquelle beschränken. Mit der Bedingung `lambda:FunctionArn` können Sie Benutzer konfigurieren lassen, welche Funktionen von einer Ereignisquelle aufgerufen werden.

Für diese Aktionen ist die Ressource die Ereignisquellen-Zuweisung. Daher bietet Lambda eine Bedingung, mit der Sie Berechtigungen basierend auf der Funktion, die die Ereignisquellen-Zuweisung aufruft, einschränken können.

Aktionen für die Ereignisquellen-Zuweisung

Aktion	Ressource	Bedingung
DeleteEventSourceMapping UpdateEventSourceMapping	Ereignisquellen-Zuweisung	`lambda:FunctionArn`
CreateEventSourceMapping GetEventSourceMapping	*	`lambda:FunctionArn`
ListEventSourceMappings	*	None

Unterstützte Layer-Aktionen

Mit Ebenenaktionen können Sie die Ebenen einschränken, die ein Benutzer verwalten oder mit einer Funktion verwenden kann. Aktionen im Zusammenhang mit der Ebenenverwendung und Ebenenberechtigung reagieren auf die Version einer Ebene, während `PublishLayerVersion` auf den Namen einer Ebene reagiert. Beide können mit Platzhaltern verwendet werden, um die Ebenen, mit denen ein Benutzer arbeiten kann, nach Name einzuschränken.

> **Note**
>
> Die Aktion „GetLayerVersion“ gilt auch für GetLayerVersionByArn. Lambda unterstützt `GetLayerVersionByArn` nicht als IAM-Aktion.

Ebenenaktionen

Aktion	Ressource	Bedingung
AddLayerVersionPermission RemoveLayerVersionPermission GetLayerVersion GetLayerVersionPolicy DeleteLayerVersión	Ebenenversion	None
ListLayerVersionen PublishLayerVersion	Ebene	Keine
ListLayers	*	None

Sicherheit in AWS Lambda

Die Sicherheit in der Cloud hat für AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud: AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen für AWS Lambda finden Sie unter Durch das Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud: Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. 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 erläutert, wie das Modell der geteilten Verantwortung bei der Verwendung von Lambda zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Lambda zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre Lambda-Ressourcen zu überwachen und zu schützen.

Weitere Informationen zur Anwendung von Sicherheitsprinzipien auf Lambda-Anwendungen finden Sie bei Serverless Land unter Sicherheit.

Themen

Datenschutz in AWS Lambda

Das AWS Modell der geteilten VerantwortungModell gilt für den Datenschutz in AWS Lambda. Wie in diesem Modell beschrieben, AWS ist für den Schutz der globalen Infrastruktur verantwortlich, die alle ausführt AWS Cloud. 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 Ihnen, -Anmeldeinformationen zu schützen AWS-Konto und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit - AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API- und Benutzeraktivitätsprotokollierung mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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-140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Lambda oder anderen AWS-Services über die Konsole, API AWS CLI oder AWS SDKs arbeiten. 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.

Abschnitte

Verschlüsselung während der Übertragung

Lambda-API-Endpunkte unterstützen ausschließlich sichere Verbindungen über HTTPS. Wenn Sie Lambda-Ressourcen mit der AWS Management Console,AWS dem SDK oder der Lambda-API verwalten, wird die gesamte Kommunikation mit Transport Layer Security (TLS) verschlüsselt. Eine vollständige Liste der API-Endpunkte finden Sie unter AWS Regionen und Endpunkte in Allgemeine AWS-Referenz.

Wenn Sie Ihre Funktion mit einem Dateisystem verbinden, verwendet Lambda Verschlüsselung während der Übertragung für alle Verbindungen. Weitere Informationen finden Sie unter Datenverschlüsselung in Amazon EFS im Benutzerhandbuch zu Amazon Elastic File System.

Wenn Sie Umgebungsvariablen verwenden, können Sie Konsolenverschlüsselungshelfer aktivieren, um die clientseitige Verschlüsselung zu verwenden, um die Umgebungsvariablen während der Übertragung zu schützen. Weitere Informationen finden Sie unter Sicherung von Lambda-Umgebungsvariablen.

Verschlüsselung im Ruhezustand

Lambda verschlüsselt immer Umgebungsvariablen im Ruhezustand. Standardmäßig verwendet Lambda einen , AWS KMS key den Lambda in Ihrem Konto erstellt, um Ihre Umgebungsvariablen zu verschlüsseln. Dies Von AWS verwalteter Schlüssel heißt `aws/lambda`.

Auf Funktionsbasis können Sie Lambda optional so konfigurieren, dass ein vom Kunden verwalteter Schlüssel anstelle des standardmäßigen Von AWS verwalteter Schlüssel verwendet wird, um Ihre Umgebungsvariablen zu verschlüsseln. Weitere Informationen finden Sie unter Sicherung von Lambda-Umgebungsvariablen.

Lambda verschlüsselt stets Dateien, die Sie zu Lambda hochladen, einschließlich Bereitstellungspaketen und Ebenenarchiven.

Amazon CloudWatch Logs und verschlüsseln Daten AWS X-Ray standardmäßig und können für die Verwendung eines vom Kunden verwalteten Schlüssels konfiguriert werden. Weitere Informationen

finden Sie unter Verschlüsseln von Protokolldaten in - CloudWatch Protokollen und Datenschutz in AWS X-Ray.

Identitäts- und Zugriffsverwaltung für AWS Lambda

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, um Lambda-Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Lambda.

Service-Benutzer – Wenn Sie den Lambda-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere Lambda-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle verstehen, kann Ihnen dies helfen, die richtigen Berechtigungen von Ihrem Administrator anzufordern. Unter Fehlerbehebung für AWS Lambda-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in Lambda haben.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für -Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Lambda. Ihre Aufgabe besteht darin, zu bestimmen,

auf welche Lambda-Funktionen und -Ressourcen Ihre Service-Nutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM zu verstehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Lambda verwenden kann, finden Sie unter Featuresweise von AWS Lambda mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Lambda verfassen können. Beispiele für identitätsbasierte Lambda-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Lambda.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

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

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

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

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

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, 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 im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und 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 in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen

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

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

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

IAM-Rollen

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

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

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

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff: Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. 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.
  - Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil,

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

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

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in 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 festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Identitätsbasierte Richtlinien

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

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

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

Ressourcenbasierte Richtlinien

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

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

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

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Featuresweise von AWS Lambda mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Lambda zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit Lambda verwenden können.

IAM-Features, die Sie mit AWS Lambda verwenden können

IAM-Feature	Lambda-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Ja
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Teilweise
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Nein
Servicerollen	Ja
Service-verknüpfte Rollen	Teilweise

Einen Überblick über das Zusammenwirken von Lambda und anderen -AWSServices mit den meisten IAM-Funktionen finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien für Lambda

Unterstützt Richtlinien auf Identitätsbasis.	Ja

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

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

Beispiele für identitätsbasierte Richtlinien für Lambda

Beispiele für identitätsbasierte Lambda-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Lambda.

Ressourcenbasierte Richtlinien in Lambda

Unterstützt ressourcenbasierte Richtlinien	Ja

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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

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 in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto

auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Sie können eine ressourcenbasierte Richtlinie an eine Lambda-Funktion oder -Ebene anfügen. Diese Richtlinie definiert, welche Prinzipale Aktionen auf der Funktion oder Ebene ausführen können.

Informationen zum Anfügen einer ressourcenbasierten Richtlinie an eine Funktion oder Ebene finden Sie unter Arbeiten mit ressourcenbasierten Richtlinien in Lambda.

Richtlinienaktionen für Lambda

Unterstützt Richtlinienaktionen	Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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 Lambda-Aktionen finden Sie unter Von definierte Aktionen AWS Lambda in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in Lambda verwenden das folgende Präfix vor der Aktion:

```
lambda
```

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

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

Beispiele für identitätsbasierte Lambda-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Lambda.

Richtlinienressourcen für Lambda

Unterstützt Richtlinienressourcen	Ja

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

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

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

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

Eine Liste der Lambda-Ressourcentypen und ihrer ARNs finden Sie unter Von definierte Ressourcentypen AWS Lambda in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Lambda definierte Aktionen.

Beispiele für identitätsbasierte Lambda-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Lambda.

Richtlinienbedingungsschlüssel für Lambda

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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, wertet AWS die Bedingung mittels 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 servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Lambda-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Lambda in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Lambda definierte Aktionen.

Beispiele für identitätsbasierte Lambda-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Lambda.

ACLs in Lambda

Unterstützt ACLs	Nein

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

ABAC mit Lambda

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 mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

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

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

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

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

Weitere Informationen zum Markieren von Lambda-Ressourcen finden Sie unter Verwendung der attributbasierten Zugriffskontrolle in Lambda.

Verwenden temporärer Anmeldeinformationen mit Lambda

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, unter anderem darüber, welche AWS-Services mit temporären Anmeldeinformationen arbeiten, finden Sie unter AWS-Services, die mit IAM arbeiten im IAM-Benutzerhandbuch.

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

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Weiterleiten von Zugriffssitzungen für Lambda

Unterstützt Forward Access Sessions (FAS)	Nein

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. 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 Lambda

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.

In Lambda wird eine Servicerolle als Ausführungsrolle bezeichnet.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Ausführungsrolle könnte die Lambda-Funktionalität beeinträchtigen.

Serviceverknüpfte Rollen für Lambda

Unterstützt serviceverknüpfte Rollen	Teilweise

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

Lambda verfügt im Gegensatz zu Lambda@Edge nicht über serviceverknüpfte Rollen. Weitere Informationen finden Sie unter Serviceverknüpfte Rollen für Lambda@Edge im Amazon- CloudFront Entwicklerhandbuch.

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.

Beispiele für identitätsbasierte Richtlinien für AWS Lambda

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

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

Einzelheiten zu Aktionen und Ressourcentypen, die von Lambda definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Lambda in der Service-Autorisierungs-Referenz.

Themen

Bewährte Methoden für Richtlinien

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

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen 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 Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Verwenden von Lambda-Konsole

Um auf die AWS Lambda-Konsole zuzugreifen, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Lambda-Ressourcen in Ihrem aufzulisten und anzuzeigenAWS-Konto. Wenn Sie

eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Eine Beispielrichtlinie, die minimalen Zugriff für die Funktionsentwicklung gewährt, finden Sie unter Schreiben einer Beispielrichtlinie, die Benutzerberechtigungen für eine Funktion gewährt. Zusätzlich zu den Lambda-APIs verwendet die Lambda-Konsole weitere Services, um Auslöserkonfigurationen anzuzeigen und neue Auslöser hinzuzufügen. Wenn Ihre Benutzer Lambda mit anderen Services nutzen, benötigen sie auch Zugriff auf diese Services. Details zum Konfigurieren weiterer Services mit Lambda finden Sie unter Lambda mit Ereignissen aus anderen Diensten aufrufen AWS.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Von verwaltete Richtlinien für AWS Lambda

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle AWS-Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Themen

- AWS Von verwaltete Richtlinie: AWSLambda_FullAccess
- AWS Von verwaltete Richtlinie: AWSLambda_ReadOnlyAccess

- AWS Von verwaltete Richtlinie: AWSLambdaBasicExecutionRole
- AWS Von verwaltete Richtlinie: AWSLambdaDynamoDBExecutionRole
- AWS Von verwaltete Richtlinie: AWSLambdaENIManagementAccess
- AWS Von verwaltete Richtlinie: AWSLambdaExecute
- AWS Von verwaltete Richtlinie: AWSLambdaInvocation-DynamoDB
- AWS Von verwaltete Richtlinie: AWSLambdaKinesisExecutionRole
- AWS Von verwaltete Richtlinie: AWSLambdaMSKExecutionRole
- AWS Von verwaltete Richtlinie: AWSLambdaRole
- AWS Von verwaltete Richtlinie: AWSLambdaSQSQueueExecutionRole
- AWS Von verwaltete Richtlinie: AWSLambdaVPCAccessExecutionRole
- Lambda-Aktualisierungen für AWS-verwaltete Richtlinien

AWS Von verwaltete Richtlinie: AWSLambda_FullAccess

Diese Richtlinie ermöglicht Vollzugriff auf alle Lambda-Aktionen. Außerdem erteilt sie Berechtigungen für andere AWS-Services, die zur Entwicklung und Verwaltung von Lambda-Ressourcen verwendet werden.

Die Richtlinie `AWSLambda_FullAccess` kann an Benutzer, Gruppen und Rollen angefügt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `lambda`: Ermöglicht Prinzipalen Vollzugriff auf Lambda.
- `cloudformation`: Ermöglicht es Prinzipalen, AWS CloudFormation-Stacks zu beschreiben und die Ressourcen in diesen Stacks aufzulisten.
- `cloudwatch` – Ermöglicht es Prinzipalen, Amazon- CloudWatch Metriken aufzulisten und Metrikdaten abzurufen.
- `ec2`: Ermöglicht es Prinzipalen, Sicherheitsgruppen, Subnetze und VPCs zu beschreiben.
- `iam`: Ermöglicht es Prinzipalen, Richtlinien, Richtlinienversionen, Rollen, Rollenrichtlinien, angefügte Rollenrichtlinien und die Liste der Rollen abzurufen. Diese Richtlinie ermöglicht es Prinzipalen außerdem, Rollen an Lambda zu übergeben. Die Berechtigung `PassRole` wird verwendet, wenn Sie einer Funktion eine Ausführungsrolle zuweisen.
- `kms`: Ermöglicht Prinzipalen das Auflisten von Aliasen.

- `logs` – Ermöglicht es Prinzipalen, Amazon- CloudWatch Protokollgruppen zu beschreiben. Bei Protokollgruppen, die mit einer Lambda-Funktion verknüpft sind, ermöglicht diese Richtlinie dem Prinzipal, Protokollstreams zu beschreiben, Protokollereignisse abzurufen und Protokollereignisse zu filtern.
- `states`: Ermöglicht es Prinzipalen, AWS Step Functions-Zustandsautomaten zu beschreiben und aufzulisten.
- `tag`: Ermöglicht es Prinzipalen, Ressourcen auf der Grundlage ihrer Tags abzurufen.
- `xray`: Ermöglicht es Prinzipalen, AWS X-Ray-Ablaufverfolgungsübersichten zu erhalten und eine Liste mit Ablaufverfolgungen (angegeben nach ID) abzurufen.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambda_FullAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambda_ReadOnlyAccess

Diese Richtlinie ermöglicht schreibgeschützten Zugriff auf Lambda-Ressourcen und andere AWS-Services, die zur Entwicklung und Verwaltung von Lambda-Ressourcen verwendet werden.

Die Richtlinie `AWSLambda_ReadOnlyAccess` kann an Benutzer, Gruppen und Rollen angefügt werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `lambda`: Ermöglicht es Prinzipalen, alle Ressourcen abzurufen und aufzulisten.
- `cloudformation`: Ermöglicht es Prinzipalen, AWS CloudFormation-Stacks zu beschreiben und aufzulisten sowie die Ressourcen in diesen Stacks aufzulisten.
- `cloudwatch` – Ermöglicht es Prinzipalen, Amazon- CloudWatch Metriken aufzulisten und Metrikdaten abzurufen.
- `ec2`: Ermöglicht es Prinzipalen, Sicherheitsgruppen, Subnetze und VPCs zu beschreiben.
- `iam`: Ermöglicht es Prinzipalen, Richtlinien, Richtlinienversionen, Rollen, Rollenrichtlinien, angefügte Rollenrichtlinien und die Liste der Rollen abzurufen.
- `kms`: Ermöglicht Prinzipalen das Auflisten von Aliasen.
- `logs` – Ermöglicht es Prinzipalen, Amazon- CloudWatch Protokollgruppen zu beschreiben. Bei Protokollgruppen, die mit einer Lambda-Funktion verknüpft sind, ermöglicht diese Richtlinie dem

Prinzipal, Protokollstreams zu beschreiben, Protokollereignisse abzurufen und Protokollereignisse zu filtern.

- `states`: Ermöglicht es Prinzipalen, AWS Step Functions-Zustandsautomaten zu beschreiben und aufzulisten.
- `tag`: Ermöglicht es Prinzipalen, Ressourcen auf der Grundlage ihrer Tags abzurufen.
- `xray`: Ermöglicht es Prinzipalen, AWS X-Ray-Ablaufverfolgungsübersichten zu erhalten und eine Liste mit Ablaufverfolgungen (angegeben nach ID) abzurufen.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambda_ReadOnlyAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaBasicExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Hochladen von Protokollen in CloudWatch -Protokolle.

Die Richtlinie `AWSLambdaBasicExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaBasicExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaDynamoDBExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Lesen von Datensätzen aus einem Amazon-DynamoDB-Stream und zum Schreiben in CloudWatch Protokolle.

Die Richtlinie `AWSLambdaDynamoDBExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaDynamoDBExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaENIManagementAccess

Diese Richtlinie erteilt Berechtigungen zum Erstellen, Beschreiben und Löschen von Elastic Network-Schnittstellen, die von einer VPC-fähigen Lambda-Funktion verwendet werden.

Die Richtlinie `AWSLambdaENIManagementAccess` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaENIManagementAccess im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaExecute

Diese Richtlinie gewährt - `PUT` und -`GET`Zugriff auf Amazon Simple Storage Service und vollen Zugriff auf - CloudWatch Protokolle.

Die Richtlinie `AWSLambdaExecute` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaExecute im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaInvocation-DynamoDB

Diese Richtlinie gewährt Lesezugriff auf Amazon DynamoDB Streams.

Die Richtlinie `AWSLambdaInvocation-DynamoDB` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaInvocation-DynamoDB im AWS Referenzhandbuch zur -verwalteten Richtlinie .

AWS Von verwaltete Richtlinie: AWSLambdaKinesisExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Lesen von Ereignissen aus einem Amazon Kinesis Data Stream und zum Schreiben in CloudWatch Logs.

Die Richtlinie `AWSLambdaKinesisExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaKinesisExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaMSKExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Lesen und Zugreifen auf Datensätze aus einem Amazon Managed Streaming for Apache Kafka-Cluster, zum Verwalten von Elastic Network-Schnittstellen und zum Schreiben in - CloudWatch Protokolle.

Die Richtlinie `AWSLambdaMSKExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaMSKExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaRole

Diese Richtlinie erteilt Berechtigungen zum Aufrufen von Lambda-Funktionen.

Die Richtlinie `AWSLambdaRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaSQSQueueExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Lesen und Löschen von Nachrichten aus einer Amazon Simple Queue Service-Warteschlange und gewährt Schreibberechtigungen für - CloudWatch Protokolle.

Die Richtlinie `AWSLambdaSQSQueueExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaSQSQueueExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AWSLambdaVPCAccessExecutionRole

Diese Richtlinie gewährt Berechtigungen zum Verwalten von Elastic Network-Schnittstellen innerhalb einer Amazon Virtual Private Cloud und zum Schreiben in CloudWatch Protokolle.

Die Richtlinie `AWSLambdaVPCAccessExecutionRole` kann an Benutzer, Gruppen und Rollen angefügt werden.

Weitere Informationen zu dieser Richtlinie, einschließlich des JSON-Richtliniendokuments und der Richtlinienversionen, finden Sie unter AWSLambdaVPCAccessExecutionRole im AWS Referenzhandbuch zu -verwalteten Richtlinien.

Lambda-Aktualisierungen für AWS-verwaltete Richtlinien

Änderung	Beschreibung	Datum
AWSLambdaVPCAccessExecutionRole – Änderung	Lambda hat die `AWSLambdaVPCAccessExecutionRole` Richtlinie aktualisiert, um die Aktion zuzulassen `ec2:DescribeSubnets` .	5. Januar 2024
AWSLambda_ReadOnlyAccess – Änderung	Lambda hat die `AWSLambda_ReadOnlyAccess` - Richtlinie aktualisiert, um Prinzipalen das Auflisten von AWS CloudFormation-Stacks zu ermöglichen.	27. Juli 2023
AWS Lambda hat die Änderungsverfolgung gestartet	AWS Lambda hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.	27. Juli 2023

Fehlerbehebung für AWS Lambda-Identität und -Zugriff

Diagnostizieren und beheben Sie mithilfe der folgenden Informationen gängige Probleme, die bei der Verwendung von Lambda und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Lambda auszuführen.
- Ich bin nicht autorisiert, iam durchzuführen:PassRole

- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Lambda-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in Lambda auszuführen.

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 IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `lambda:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `lambda:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der Aktion „`iam:PassRole`“ autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Lambda übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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 in Lambda 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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Lambda-Ressourcen gewähren

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

Weitere Informationen finden Sie hier:

- Informationen dazu, ob Lambda diese Funktionen unterstützt, finden Sie unter Featuresweise von AWS Lambda mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- 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 So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Erstellen Sie eine Governance-Strategie für Lambda-Funktionen und -Layer

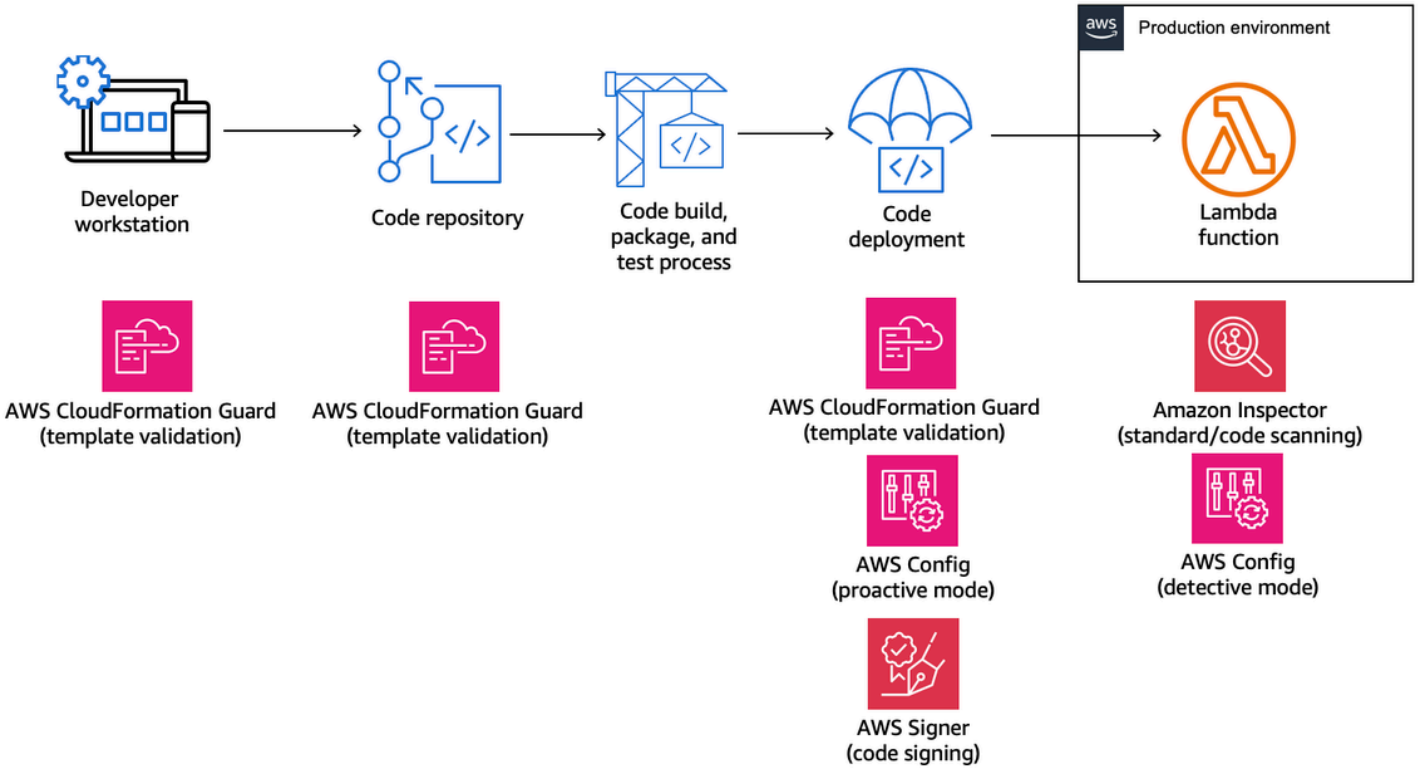
Bei der Entwicklung und Bereitstellung cloudnativer Serverless-Anwendungen müssen Sie durch angemessene Governance- und Schutzmaßnahmen für Agilität und eine schnelle Markteinführung

sorgen. Dazu legen Sie auf Unternehmensebene Prioritäten fest, wobei Sie entweder die Agilität oder durch geeignete Governance, Schutzmaßnahmen und Kontrollen die Risikovermeidung an erste Stelle setzen. Normalerweise werden Sie keine so klare Grenze ziehen, sondern beide Aspekte – Agilität und Sicherheit – in Ihrem Softwareentwicklungszyklus abbilden möchten. Ganz gleich, wo im Lebenszyklus Ihres Unternehmens diese Anforderungen stehen, Sie werden mit hoher Wahrscheinlichkeit Governance-Funktionen in Ihre Prozesse und Toolchains implementieren müssen.

Hier sind einige Beispiele für Governance-Kontrollen, die ein Unternehmen für Lambda implementieren könnte:

- Lambda-Funktionen dürfen nicht öffentlich zugänglich sein.
- Lambda-Funktionen müssen mit einer VPC verbunden sein.
- Lambda-Funktionen sollten keine veralteten Laufzeiten verwenden.
- Lambda-Funktionen müssen mit einer Reihe erforderlicher Tags markiert werden.
- Lambda-Layer dürfen außerhalb der Organisation nicht zugänglich sein.
- Wenn Lambda-Funktionen mit einer Sicherheitsgruppe verbunden sind, müssen beide übereinstimmende Tags haben.
- Lambda-Funktionen mit einem verbundenen Layer müssen eine genehmigte Version verwenden
- Lambda-Umgebungsvariablen müssen im Ruhezustand mit einem vom Kunden verwalteten Schlüssel verschlüsselt sein.

Das folgende Diagramm ist ein Beispiel für eine umfassende Governance-Strategie, bei der Kontrollen und Richtlinien während des gesamten Softwareentwicklungs- und Bereitstellungsprozesses implementiert werden:



In den folgenden Themen wird erklärt, wie Sie Kontrollen für die Entwicklung und Bereitstellung von Lambda-Funktionen in Ihrem Unternehmen implementieren. Die Ausführungen gelten für Startups und große Unternehmen gleichermaßen. Möglicherweise verfügt Ihr Unternehmen bereits über geeignete Tools. In den folgenden Themen wird ein modularer Ansatz für diese Kontrollen verfolgt, damit Sie die Komponenten auswählen können, die Sie tatsächlich benötigen.

Themen

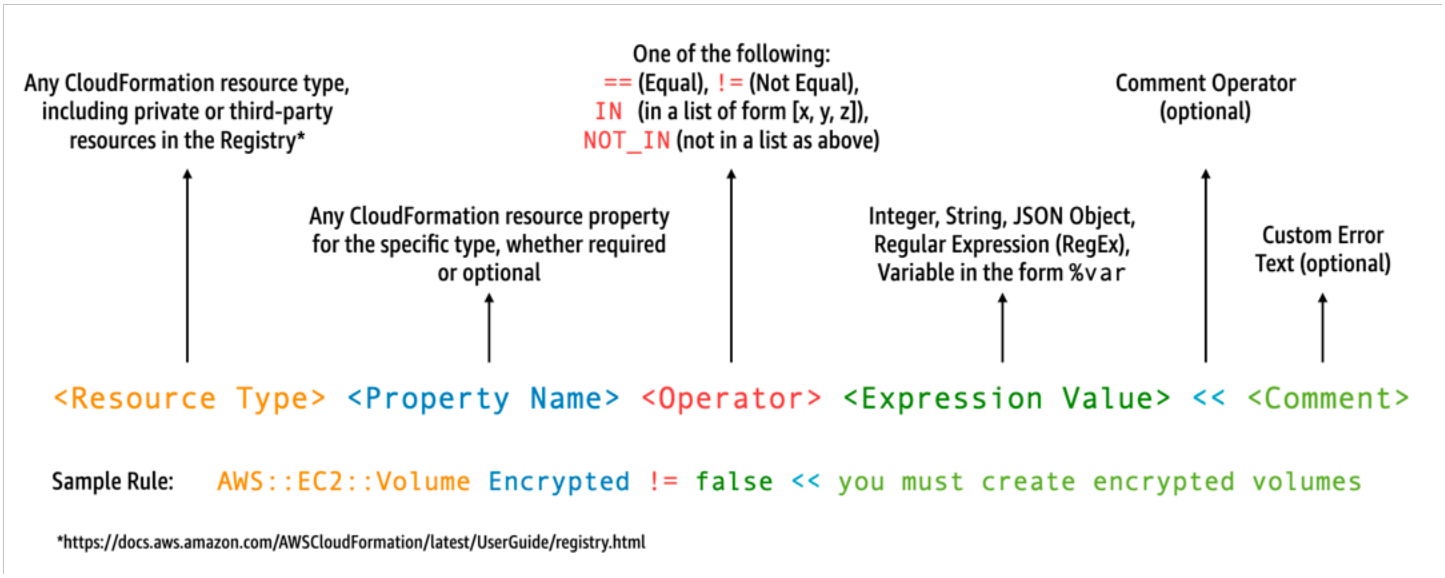
- Proaktive Kontrollen für Lambda mit AWS CloudFormation Guard
- Implementieren Sie präventive Kontrollen für Lambda mit AWS Config
- Erkennen Sie nicht konforme Lambda-Bereitstellungen und -Konfigurationen mit AWS Config
- Lambda-Codesignatur mit AWS Signer
- Automatisieren Sie Sicherheitsbewertungen für Lambda mit Amazon Inspector
- Implementieren von Beobachtbarkeit für Lambda-Sicherheit und -Compliance

Proaktive Kontrollen für Lambda mit AWS CloudFormation Guard

AWS CloudFormation Guard ist ein universelles Open-Source- policy-as-code Bewertungstool. Es kann für präventive Governance und Compliance verwendet werden, indem Infrastructure as Code (IaC)-Vorlagen und Servicezusammenstellungen anhand von Richtlinienregeln validiert werden. Diese Regeln können an die Anforderungen Ihres Teams oder Ihrer Organisation angepasst werden. Für Lambda-Funktionen können die Guard-Regeln verwendet werden, um die Ressourcenerstellung und Konfigurationsupdates zu steuern. Dazu werden die erforderlichen Eigenschaftseinstellungen definiert, die beim Erstellen oder Aktualisieren einer Lambda-Funktion erforderlich sind.

Compliance-Administratoren definieren die Liste der Kontrollen und Governance-Richtlinien, die für die Bereitstellung und Aktualisierung von Lambda-Funktionen erforderlich sind. Plattformadministratoren implementieren die Kontrollen in CI/CD-Pipelines als Pre-Commit-Validierungs-Webhooks mit Code-Repositorys und stellen Entwicklern Befehlszeilentools zur Validierung von Vorlagen und Code auf lokalen Workstations zur Verfügung. Entwickler schreiben Code, validieren Vorlagen mit Befehlszeilentools und übertragen dann den Code in Repositorys, die vor der Bereitstellung in einer AWS-Umgebung automatisch über die CI/CD-Pipelines validiert werden.

Guard ermöglicht es Ihnen wie folgt, Regeln zu schreiben und Kontrollen in einer domainspezifischen Sprache zu implementieren.



Angenommen, Sie möchten, dass Entwickler nur die neuesten Laufzeiten verwenden. Sie könnten zwei verschiedene Richtlinien erstellen. Eine, um Laufzeiten zu bestimmen, die bereits veraltet sind,

und eine andere, um Laufzeiten zu bestimmen, die demnächst veraltet sein werden. Dazu könnten Sie die folgende `etc/rules.guard`-Datei schreiben:

```
let lambda_functions = Resources.*[
    Type == "AWS::Lambda::Function"
]

rule lambda_already_deprecated_runtime when %lambda_functions !empty {
    %lambda_functions {
        Properties {
            when Runtime exists {
                Runtime !in ["dotnetcore3.1", "nodejs12.x", "python3.6", "python2.7",
 "dotnet5.0", "dotnetcore2.1", "ruby2.5", "nodejs10.x", "nodejs8.10", "nodejs4.3",
 "nodejs6.10", "dotnetcore1.0", "dotnetcore2.0", "nodejs4.3-edge", "nodejs"] <<Lambda
 function is using a deprecated runtime.>>
            }
        }
    }
}

rule lambda_soon_to_be_deprecated_runtime when %lambda_functions !empty {
    %lambda_functions {
        Properties {
            when Runtime exists {
                Runtime !in ["nodejs16.x", "nodejs14.x", "python3.7", "java8",
 "dotnet7", "go1.x", "ruby2.7", "provided"] <<Lambda function is using a runtime that
 is targeted for deprecation.>>
            }
        }
    }
}
```

Angenommen, Sie schreiben die folgende `iac/lambda.yaml` CloudFormation Vorlage, die eine Lambda-Funktion definiert:

```
  Fn:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.7
      CodeUri: src
      Handler: fn.handler
      Role: !GetAtt FnRole.Arn
      Layers:
```

```
        - arn:aws:lambda:us-east-1:111122223333:layer:LambdaInsightsExtension:35
```

Nach der Installation des Guard-Dienstprogramms überprüfen Sie die Vorlage:

```
cfn-guard validate --rules etc/rules.guard --data iac/lambda.yaml
```

Das Ergebnis sieht folgendermaßen aus:

```
lambda.yaml Status = FAIL
FAILED rules
rules.guard/lambda_soon_to_be_deprecated_runtime
---
Evaluating data lambda.yaml against rules rules.guard
Number of non-compliant resources 1
Resource = Fn {
  Type      = AWS::Lambda::Function
  Rule = lambda_soon_to_be_deprecated_runtime {
    ALL {
      Check =  Runtime not IN
 ["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"]
 {
       ComparisonError {
         Message          = Lambda function is using a runtime that is targeted for
 deprecation.
         Error            = Check was not compliant as property [/Resources/
Fn/Properties/Runtime[L:88,C:15]] was not present in [(resolved, Path=[L:0,C:0]
 Value=["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"])]
       }
         PropertyPath    = /Resources/Fn/Properties/Runtime[L:88,C:15]
         Operator        = NOT IN
         Value           = "python3.7"
         ComparedWith    =
 [["nodejs16.x","nodejs14.x","python3.7","java8","dotnet7","go1.x","ruby2.7","provided"]]
         Code:
              86.  Fn:
              87.    Type: AWS::Lambda::Function
              88.    Properties:
              89.      Runtime: python3.7
              90.      CodeUri: src
              91.      Handler: fn.handler

      }
    }
```

```
  }
}
```

Guard zeigt Entwicklern auf ihren lokalen Workstations, dass sie die Vorlage aktualisieren müssen, um eine Laufzeit zu verwenden, die von der Organisation zugelassen ist. Dies geschieht, bevor ein Commit in ein Code-Repository übernommen wird und anschließend Prüfungen innerhalb einer CI/CD-Pipeline fehlschlagen. Ihre Entwickler erhalten direktes Feedback, wie sie konforme Vorlagen entwickeln und können ihre Zeit darauf verwenden, Code zu schreiben, der geschäftlichen Nutzen bietet. Diese Kontrolle kann vor der Bereitstellung auf der lokalen Entwickler-Workstation, in einem Pre-Commit-Validierungs-Webhook und/oder in der CI/CD-Pipeline angewendet werden.

Einschränkungen

Wenn Sie AWS Serverless Application Model-(AWS SAM)-Vorlagen verwenden, um Lambda-Funktionen zu definieren, beachten Sie, dass Sie die Guard-Regel aktualisieren müssen, um nach dem Ressourcentyp `AWS::Serverless::Function` wie folgt zu suchen.

```
let lambda_functions = Resources.*[
    Type == "AWS::Serverless::Function"
]
```

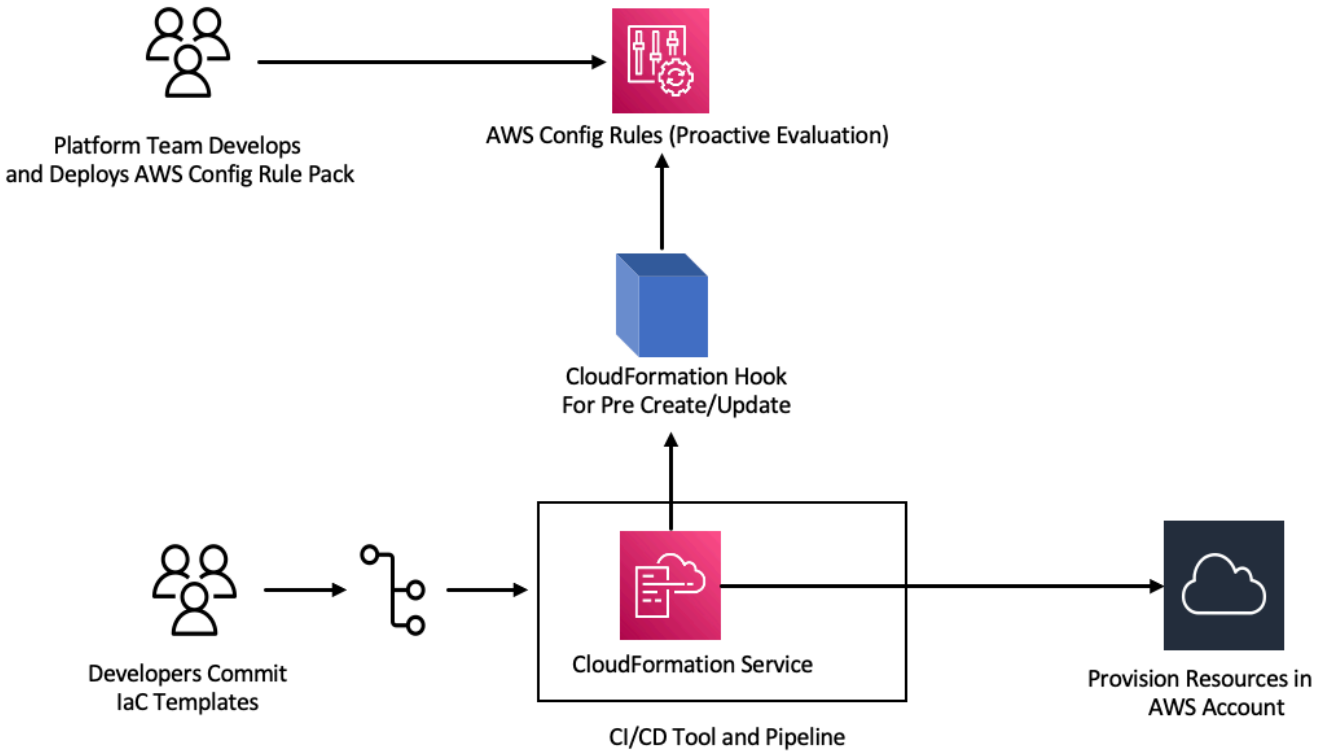
Guard erwartet außerdem, dass die Eigenschaften in der Ressourcendefinition enthalten sind. AWS SAM-Vorlagen ermöglichen die Angabe von Eigenschaften in einem separaten Globals-Abschnitt. Eigenschaften, die im Globals-Abschnitt definiert sind, werden nicht mit Ihren Guard-Regeln validiert.

Beachten Sie, dass Guard, wie in der Dokumentation zur Fehlerbehebung bei Guard beschrieben, keine intrinsischen Kurzformen wie `!GetAtt` oder `!Sub` unterstützt, sondern stattdessen die Verwendung der erweiterten Formen erfordert: `Fn::GetAtt` und `Fn::Sub`. (Im vorherigen Beispiel wird die Role-Eigenschaft nicht ausgewertet, daher wurde der Einfachheit halber die intrinsische Kurzform verwendet.)

Implementieren Sie präventive Kontrollen für Lambda mit AWS Config

Es ist wichtig, so früh wie möglich im Entwicklungsprozess die Konformität Ihrer Serverless-Anwendungen sicherzustellen. In diesem Thema behandeln wir die Implementierung präventiver Kontrollen mithilfe von AWS Config. Ziel ist es, Konformitätsprüfungen frühzeitig im Entwicklungsprozess zu implementieren und dieselben Kontrollen in den CI/CD-Pipelines zu verwenden. Dadurch werden auch Ihre Kontrollen in einem zentral verwalteten Regelspeicher standardisiert, sodass Sie Ihre Kontrollen konsistent auf alle Konten anwenden können. AWS

Nehmen wir zum Beispiel an, Ihre Compliance-Administratoren haben eine Anforderung definiert, um sicherzustellen, dass alle Lambda-Funktionen die AWS X-Ray Ablaufverfolgung beinhalten. Mit dem AWS Config proaktiven Modus können Sie vor der Bereitstellung Konformitätsprüfungen Ihrer Lambda-Funktionsressourcen durchführen, wodurch das Risiko der Bereitstellung falsch konfigurierter Lambda-Funktionen verringert und Entwicklern Zeit gespart wird, indem sie ihnen schnelleres Feedback zur Infrastruktur als Codevorlagen geben. Im Folgenden wird der Ablauf präventiver Kontrollen visualisiert mit: AWS Config



Nehmen wir an, es wird festgelegt, dass für alle Lambda-Funktionen die Ablaufverfolgung aktiviert sein muss. Als Reaktion darauf stellt das Plattformteam fest, dass eine bestimmte AWS Config Regel proaktiv für alle Konten ausgeführt werden muss. Diese Regel kennzeichnet jede Lambda-Funktion, für die keine X-Ray-Ablaufverfolgung konfiguriert ist, als nicht konforme Ressource. Das Team entwickelt eine Regel, verpackt sie in ein Konformitätspaket und stellt das Konformitätspaket für alle Konten bereit, um sicherzustellen, dass alle AWS Konten in der Organisation diese Kontrollen einheitlich anwenden. Sie können die Regel in der AWS CloudFormation Guard 2.x.x-Syntax schreiben, die folgende Form hat:

```
rule name when condition { assertion }
```

Im Folgenden finden Sie ein Beispiel für eine Guard-Regel, die überprüft, ob für Lambda-Funktionen die Ablaufverfolgung aktiviert ist:

```
rule lambda_tracing_check {
  when configuration.tracingConfig exists {
      configuration.tracingConfig.mode == "Active"
  }
}
```

Das Plattformteam ergreift weitere Maßnahmen und schreibt vor, dass bei jeder AWS CloudFormation Bereitstellung ein Pre-Create/Update-Hook aufgerufen wird. Das Team übernimmt die volle Verantwortung für die Entwicklung dieses Hooks und die Konfiguration der Pipeline, mit dem Ziel, die zentrale Kontrolle der Compliance-Regeln zu stärken und ihre konsistente Anwendung in allen Implementierungen sicherzustellen. Informationen zur Entwicklung, Paketierung und Registrierung eines AWS CloudFormation Hooks finden Sie in der Dokumentation zur CloudFormation Befehlszeilenschnittstelle (CFN-CLI) unter Developing Hooks. Sie können die CloudFormation CLI verwenden, um das Hook-Projekt zu erstellen:

```
cfn init
```

Der Befehl fragt Sie nach einigen grundlegenden Informationen zu Ihrem Hook-Projekt und erstellt ein Projekt mit den folgenden Dateien:

```
README.md
<hook-name>.json
rpdk.log
src/handler.py
template.yml
```

```
hook-role.yaml
```

Der Hook-Entwickler fügt der Konfigurationsdatei `<hook-name>.json` den gewünschten Zielressourcentyp hinzu. In der folgenden Konfiguration ist ein Hook so konfiguriert, dass er ausgeführt wird, bevor eine Lambda-Funktion mit CloudFormation erstellt wird. Sie können ähnliche Handler auch für die Aktionen `preUpdate` und `preDelete` hinzufügen.

```
    "handlers": {
        "preCreate": {
            "targetNames": [
                "AWS::Lambda::Function"
            ],
            "permissions": []
        }
    }
```

Sie müssen außerdem sicherstellen, dass der CloudFormation Hook über die entsprechenden Berechtigungen zum Aufrufen der AWS Config APIs verfügt. Aktualisieren Sie dazu die Rollendefinitionsdatei `hook-role.yaml`. Die Rollendefinitionsdatei hat standardmäßig die folgende Vertrauensrichtlinie, die es ermöglicht, die Rolle CloudFormation zu übernehmen.

```
      AssumeRolePolicyDocument:
        Version: '2012-10-17'
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - hooks.cloudformation.amazonaws.com
                - resources.cloudformation.amazonaws.com
```

Damit der Hook Konfigurations-APIs aufrufen kann, müssen Sie der Policy-Anweisung die folgenden Berechtigungen hinzufügen. Anschließend reichen Sie das Hook-Projekt mit dem `cfn submit` Befehl ein, der eine Rolle mit den erforderlichen Berechtigungen für Sie CloudFormation erstellt.

```
      Policies:
        - PolicyName: HookTypePolicy
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
```

```
                Action:
                  - "config:Describe*"
                  - "config:Get*"
                  - "config:List*"
                  - "config:SelectResourceConfig"
                Resource: "*
```

Als Nächstes müssen Sie eine Lambda-Funktion in eine `src/handler.py`-Datei schreiben. In dieser Datei finden Sie Methoden mit dem Namen und `preCreate`, `preUpdate` und `preDelete`, die bereits bei der Initiierung des Projekts erstellt wurden. Ihr Ziel ist es, eine allgemeine, wiederverwendbare Funktion zu schreiben, die die AWS Config `StartResourceEvaluation` API im proaktiven Modus aufruft, und zwar mithilfe von AWS SDK for Python (Boto3). Dieser API-Aufruf verwendet Ressourceneigenschaften als Eingabe und vergleicht die Ressource mit der Regeldefinition.

```
def validate_lambda_tracing_config(resource_type, function_properties:
 MutableMapping[str, Any]) -> ProgressEvent:
  LOG.info("Fetching proactive data")
  config_client = boto3.client('config')
  resource_specs = {
      'ResourceId': 'MyFunction',
      'ResourceType': resource_type,
      'ResourceConfiguration': json.dumps(function_properties),
      'ResourceConfigurationSchemaType': 'CFN_RESOURCE_SCHEMA'
  }
  LOG.info("Resource Specifications:", resource_specs)
  eval_response = config_client.start_resource_evaluation(EvaluationMode='PROACTIVE',
 ResourceDetails=resource_specs, EvaluationTimeout=60)
  ResourceEvaluationId = eval_response.ResourceEvaluationId
  compliance_response =
 config_client.get_compliance_details_by_resource(ResourceEvaluationId=ResourceEvaluationId)
  LOG.info("Compliance Verification:",
 compliance_response.EvaluationResults[0].ComplianceType)
  if "NON_COMPLIANT" == compliance_response.EvaluationResults[0].ComplianceType:
      return ProgressEvent(status=OperationStatus.FAILED, message="Lambda function
 found with no tracing enabled : FAILED", errorCode=HandlerErrorCode.NonCompliant)
  else:
      return ProgressEvent(status=OperationStatus.SUCCESS, message="Lambda function
 found with tracing enabled : PASS.")
```

Jetzt können Sie die allgemeine Funktion vom Handler für den Pre-Create-Hook aus aufrufen. Ein Beispiel für den Handler:

```
@hook.handler(HookInvocationPoint.CREATE_PRE_PROVISION)
def pre_create_handler(
        session: Optional[SessionProxy],
        request: HookHandlerRequest,
        callback_context: MutableMapping[str, Any],
        type_configuration: TypeConfigurationModel
) -> ProgressEvent:
    LOG.info("Starting execution of the hook")
    target_name = request.hookContext.targetName
    LOG.info("Target Name:", target_name)
    if "AWS::Lambda::Function" == target_name:
        return validate_lambda_tracing_config(target_name,
            request.hookContext.targetModel.get("resourceProperties")
        )
    else:
        raise exceptions.InvalidRequest(f"Unknown target type: {target_name}")
```

Nach diesem Schritt können Sie den Hook registrieren und ihn so konfigurieren, dass er alle Ereignisse bei der AWS Lambda Funktionserstellung abhört.

Ein Entwickler bereitet die IaC-Vorlage (Infrastructure as Code) für einen Serverless-Microservice mithilfe von Lambda vor. Diese Vorbereitung umfasst die Einhaltung interner Standards, gefolgt von lokalen Tests und dem Commit der Vorlage in das Repository. Hier ist ein Beispiel für eine IaC-Vorlage:

```
  MyLambdaFunction:
  Type: 'AWS::Lambda::Function'
  Properties:
    Handler: index.handler
    Role: !GetAtt LambdaExecutionRole.Arn
    FunctionName: MyLambdaFunction
    Code:
      ZipFile: |
        import json

        def handler(event, context):
            return {
                'statusCode': 200,
                'body': json.dumps('Hello World!')
            }
    Runtime: python3.8
    TracingConfig:
```

```
        Mode: PassThrough
    MemorySize: 256
    Timeout: 10
```

Als Teil des CI/CD-Prozesses ruft der CloudFormation Dienst bei der Bereitstellung der CloudFormation Vorlage den Pre-Create/Update-Hook unmittelbar vor der Bereitstellung des Ressourcentyps auf. `AWS::Lambda::Function` Der Hook verwendet AWS Config Regeln, die im proaktiven Modus ausgeführt werden, um zu überprüfen, ob die Lambda-Funktionskonfiguration die vorgeschriebene Ablaufverfolgungskonfiguration enthält. Die Antwort des Hooks bestimmt den nächsten Schritt. Wenn die Vorschriften eingehalten werden, signalisiert der Hook den Erfolg und CloudFormation fährt mit der Bereitstellung der Ressourcen fort. Wenn nicht, schlägt die CloudFormation Stack-Bereitstellung fehl, die Pipeline wird sofort gestoppt und das System zeichnet die Details zur späteren Überprüfung auf. An die relevanten Stakeholder werden Compliance-Benachrichtigungen gesendet.

Sie finden die Informationen zum Erfolg/Fehlschlagen des Hooks in der CloudFormation Konsole:

Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Events (19)

Search events

Timestamp	Logical ID	Status	Status reason	Hook invocations
2023-08-29 23:50:23 UTC-0500	HookTestStack	ROLLBACK_COMPLETE	-	-
2023-08-29 23:50:22 UTC-0500	LambdaExecutionRole	DELETE_COMPLETE	-	-
2023-08-29 23:50:21 UTC-0500	MyApi	DELETE_COMPLETE	-	-
2023-08-29 23:50:20 UTC-0500	LambdaExecutionRole	DELETE_IN_PROGRESS	-	-
2023-08-29 23:50:20 UTC-0500	MyLambdaFunction	DELETE_COMPLETE	-	-
2023-08-29 23:50:20 UTC-0500	MyApi	DELETE_IN_PROGRESS	-	-
2023-08-29 23:50:18 UTC-0500	HookTestStack	ROLLBACK_IN_PROGRESS	The following resource(s) failed to create: [MyLambdaFunction]. Rollback requested by user.	-
2023-08-29 23:50:17 UTC-0500	MyLambdaFunction	CREATE_FAILED	The following hook(s) failed: [AWSSamples::LambdaTracingCheck::Hook]	-
2023-08-29 23:50:17 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	AWSSamples::LambdaTracingCheck::Hook
2023-08-29 23:50:16 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	AWSSamples::LambdaTracingCheck::Hook
2023-08-29 23:50:15 UTC-0500	MyLambdaFunction	CREATE_IN_PROGRESS	-	-
2023-08-29 23:50:14 UTC-0500	LambdaExecutionRole	CREATE_COMPLETE	-	-
2023-08-29 23:49:59 UTC-0500	MyApi	CREATE_COMPLETE	-	-
2023-08-29 23:49:59 UTC-0500	MyApi	CREATE_IN_PROGRESS	Resource creation Initiated	-
2023-08-29 23:49:58 UTC-0500	LambdaExecutionRole	CREATE_IN_PROGRESS	Resource creation Initiated	-
2023-08-29 23:49:58 UTC-0500	LambdaExecutionRole	CREATE_IN_PROGRESS	-	-
2023-08-29 23:49:58 UTC-0500	MyApi	CREATE_IN_PROGRESS	-	-
2023-08-29 23:49:55 UTC-0500	HookTestStack	CREATE_IN_PROGRESS	User Initiated	-
2023-08-29 23:49:50 UTC-0500	HookTestStack	REVIEW_IN_PROGRESS	User Initiated	-

Wenn Sie Logs für Ihren CloudFormation Hook aktiviert haben, können Sie das Ergebnis der Hook-Auswertung erfassen. Hier ist ein Beispielprotokoll für einen Hook mit dem Status „Fehlgeschlagen“, was darauf hinweist, dass für die Lambda-Funktion X-Ray nicht aktiviert ist:

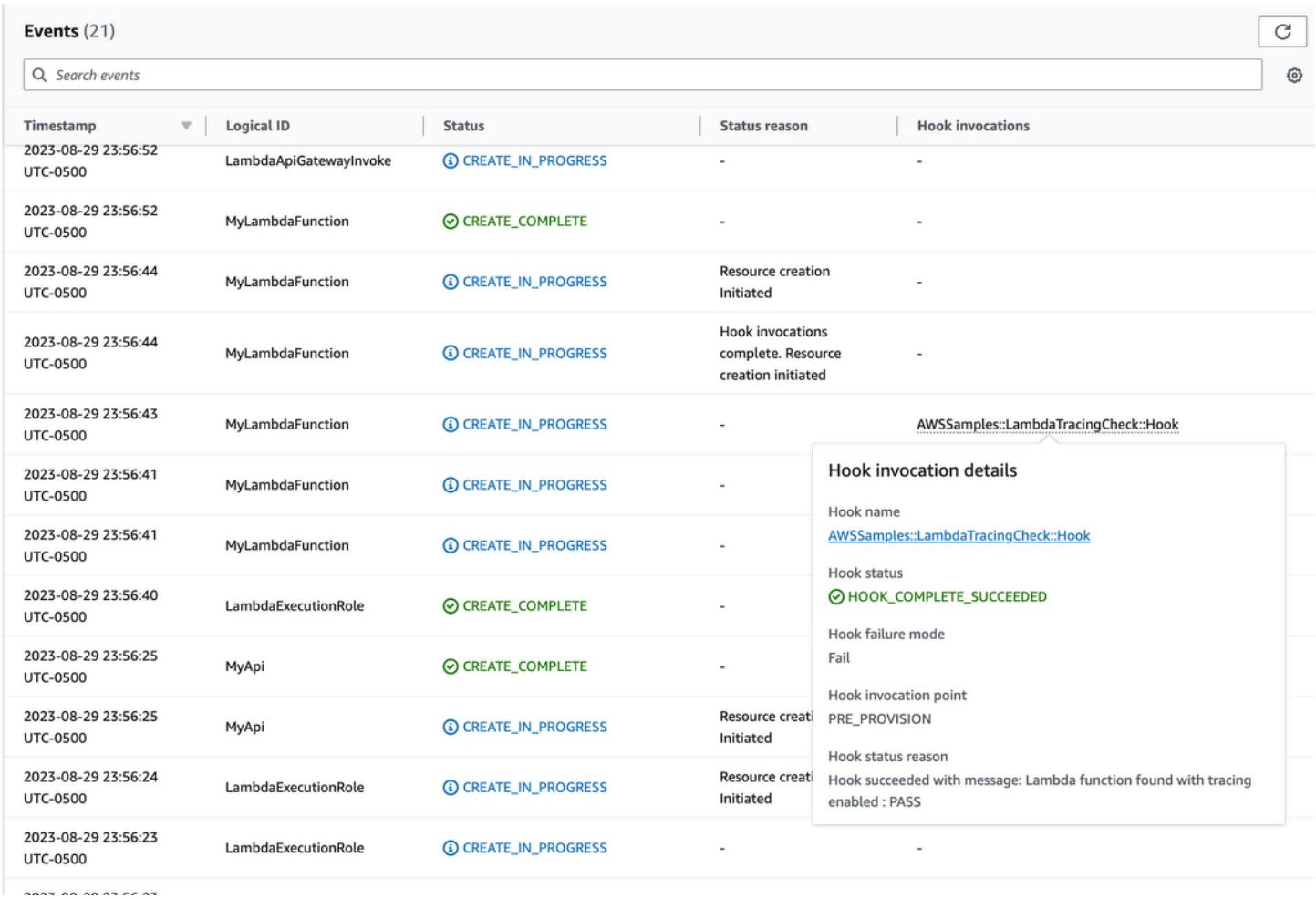
2023-08-29T23:50:17.574-05:00 ProgressEvent(status=<OperationStatus.FAILED: 'FAILED'>, errorCode=<HandlerErrorCode.NonCompliant: 'NonCompliant'…

```
ProgressEvent(status=<OperationStatus.FAILED: 'FAILED'>, errorCode=<HandlerErrorCode.NonCompliant: 'NonCompliant'>, message='Lambda
function found with no tracing enabled : FAILED', result=None, callbackContext=None, callbackDelaySeconds=0, resourceModel=None,
resourceModels=None, nextToken=None)
```

Copy

No newer events at this moment. *Auto retry paused.* Resume

Hat der Entwickler entschieden, die IaC so zu ändern, dass der Wert `TracingConfig Mode` in `Active` aktualisiert wird und die Bereitstellung erneut erfolgt, wird der Hook erfolgreich ausgeführt und der Stack fährt mit der Erstellung der Lambda-Ressource fort.



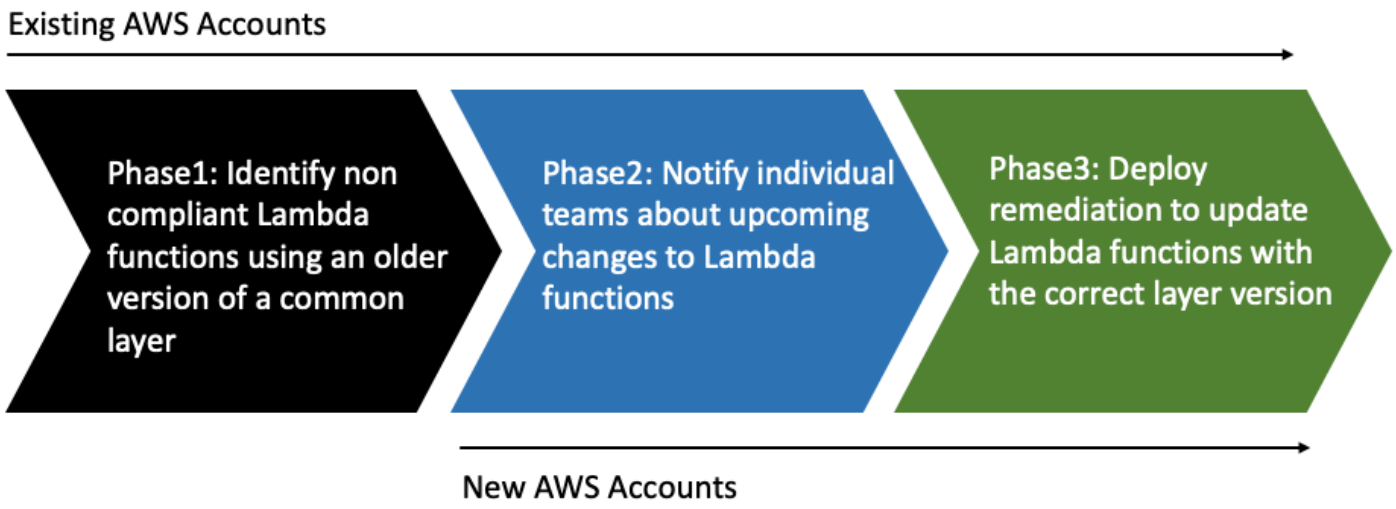
Auf diese Weise können Sie präventive Kontrollen AWS Config im proaktiven Modus implementieren, wenn Sie serverlose Ressourcen in Ihren AWS Konten entwickeln und bereitstellen. Durch die Integration von AWS Config -Regeln in die CI/CD-Pipeline können Sie nicht konforme Ressourcenbereitstellungen identifizieren und optional blockieren, z. B. Lambda-Funktionen, denen eine aktive Ablaufverfolgungskonfiguration fehlt. Dadurch wird sichergestellt, dass nur Ressourcen in Ihren AWS Umgebungen eingesetzt werden, die den neuesten Governance-Richtlinien entsprechen.

Erkennen Sie nicht konforme Lambda-Bereitstellungen und -Konfigurationen mit AWS Config

Neben der proaktiven Bewertung AWS Config kann auch reaktiv Ressourcenbereitstellungen und -konfigurationen erkannt werden, die nicht Ihren Governance-Richtlinien entsprechen. Das ist wichtig, weil sich Governance-Richtlinien ändern können, wenn Ihr Unternehmen sich weiterentwickelt und neue Best-Practices eingeführt werden.

Angenommen, Sie legen bei der Bereitstellung oder Aktualisierung von Lambda-Funktionen eine brandneue Richtlinie fest: Alle Lambda-Funktionen müssen immer eine bestimmte, genehmigte Lambda-Layer-Version verwenden. Sie können AWS Config konfigurieren, um neue oder aktualisierte Funktionen für Layer-Konfigurationen zu überwachen. Wenn eine Funktion AWS Config erkannt wird, die keine genehmigte Layer-Version verwendet, wird die Funktion als nicht konforme Ressource gekennzeichnet. Sie können optional so konfigurieren AWS Config , dass die Ressource automatisch repariert wird, indem Sie mithilfe eines Automatisierungsdokuments eine Behebungsaktion angeben. AWS Systems Manager Sie könnten beispielsweise ein Automatisierungsdokument in Python mit dem schreiben AWS SDK for Python (Boto3), wodurch die nicht konforme Funktion aktualisiert wird, sodass sie auf die genehmigte Layer-Version verweist. Es AWS Config dient somit sowohl als detektive als auch als korrektive Kontrolle und automatisiert das Compliance-Management.

Wir brechen diesen Prozess in drei zentrale Implementierungsphasen auf:



Phase 1: Identifizieren der Zugriffsressourcen

Aktivieren Sie zunächst AWS Config alle Ihre Konten und konfigurieren Sie es so, dass AWS Lambda-Funktionen aufgezeichnet werden. Auf diese Weise kann AWS Config beobachtet

werden, wann Lambda-Funktionen erstellt oder aktualisiert werden. Anschließend können Sie benutzerdefinierte Richtlinienregeln konfigurieren, um nach bestimmten Richtlinienverstößen zu suchen, die AWS CloudFormation Guard -Syntax verwenden. Guard-Regeln haben die folgende allgemeine Form:

```
rule name when condition { assertion }
```

Im Folgenden finden Sie eine Beispielregel, mit der überprüft wird, ob ein Layer auf eine alte Layer-Version eingestellt ist:

```
rule desiredlayer when configuration.layers !empty {
    some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn
}
```

Sehen wir uns die Syntax und den Regelaufbau etwas genauer an:

- Regelname: Der Name der Regel im Beispiel lautet `desiredlayer`.
- Bedingung: Diese Klausel gibt die Bedingung an, unter der die Regel überprüft werden soll. Im angegebenen Beispiel lautet die Bedingung `configuration.layers !empty`. Das bedeutet, dass die Ressource nur ausgewertet werden sollte, wenn die `layers`-Eigenschaft in der Konfiguration nicht leer ist.
- Assertion: Nach der `when`-Klausel bestimmt die Assertion, was die Regel überprüft. Die Assertion (Behauptung) `some configuration.layers[*].arn != CONFIG_RULE_PARAMETERS.OldLayerArn` prüft, ob einer der ARNs des Lambda-Layers nicht mit dem Wert `OldLayerArn` übereinstimmt. Wenn es keine Übereinstimmung gibt, ist die Assertion wahr und die Regel gilt als bestanden. Andernfalls schlägt sie fehl.

`CONFIG_RULE_PARAMETERS`ist ein spezieller Satz von Parametern, der mit der AWS Config Regel konfiguriert wird. In diesem Fall ist `OldLayerArn` ein Parameter in `CONFIG_RULE_PARAMETERS`. Benutzer können so einen bestimmten ARN-Wert als veraltet oder abgelaufen festlegen. Anschließend überprüft die Regel, ob Lambda-Funktionen diesen alten ARN verwenden.

Phase 2: Visualisierung und Entwicklung

AWS Config sammelt Konfigurationsdaten und speichert diese Daten in Amazon Simple Storage Service (Amazon S3) -Buckets. Sie können Amazon Athena verwenden, um diese Daten direkt aus Ihren S3-Buckets abzufragen. Mit Athena können Sie diese Daten

auf Organisationsebene aggregieren und sich einen ganzheitlichen Überblick über die Ressourcenkonfigurationen in all Ihren Konten verschaffen. Informationen zum Einrichten der Aggregation von Ressourcenkonfigurationsdaten finden Sie unter Visualisieren von AWS Config Daten mit Athena und QuickSight Amazon im AWS Cloud Operations and Management-Blog.

Im Folgenden finden Sie ein Beispiel für eine Athena-Abfrage zur Identifizierung aller Lambda-Funktionen, die einen bestimmten Layer-ARN verwenden:

```
WITH unnested AS (
    SELECT
      item.awsaccountid AS account_id,
      item.awsregion AS region,
      item.configuration AS lambda_configuration,
      item.resourceid AS resourceid,
      item.resourcename AS resourcename,
      item.configuration AS configuration,
      json_parse(item.configuration) AS lambda_json
    FROM
      default.aws_config_configuration_snapshot,
      UNNEST(configurationitems) as t(item)
    WHERE
      "dt" = 'latest'
      AND item.resourcetype = 'AWS::Lambda::Function'
  )

  SELECT DISTINCT
    region as Region,
    resourcename as FunctionName,
    json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,
    json_extract_scalar(lambda_json, '$.timeout') AS timeout,
    json_extract_scalar(lambda_json, '$.version') AS version
  FROM
    unnested
  WHERE
    lambda_configuration LIKE '%arn:aws:lambda:us-
east-1:111122223333:layer:AnyGovernanceLayer:24%'
```

Hier sind die Ergebnisse der Abfrage:

Query results | Query stats

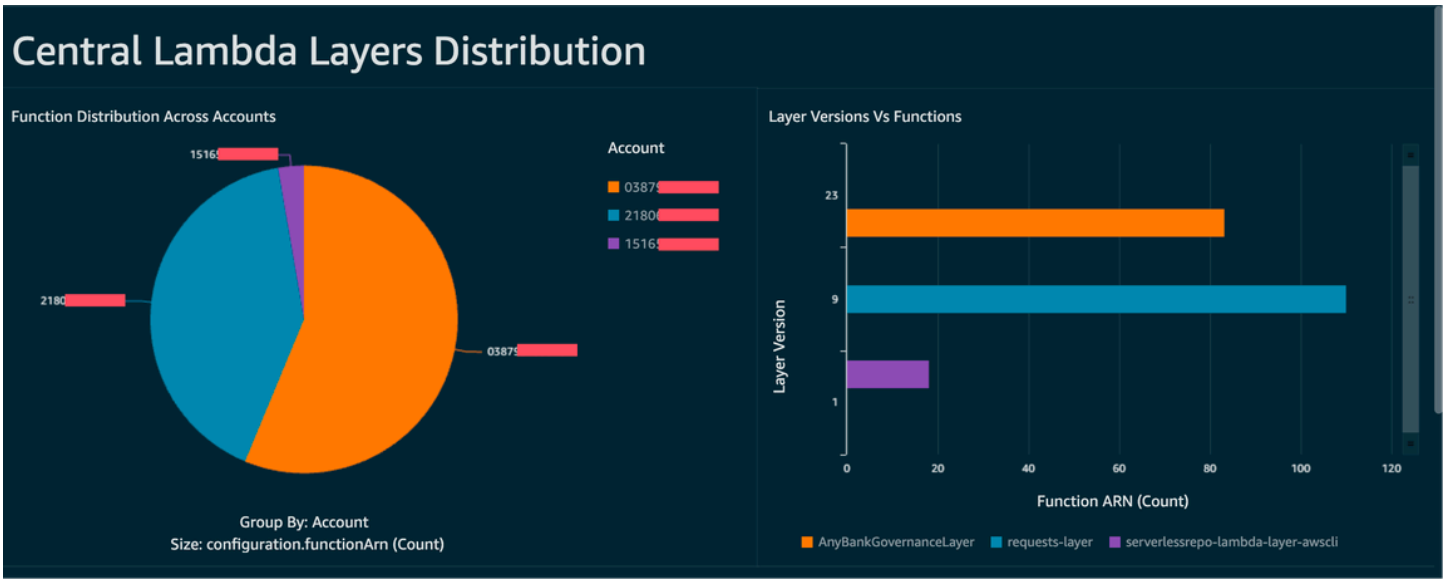
Completed — Time in queue: 127 ms — Run time: 1.803 sec — Data scanned: 239.40 KB

Results (27) — Copy — Download results

Search rows — 1

#	Region	FunctionName	memory_size	timeout	version
1	us-east-1	UpdateUIForPublishEvents	128	18	$LATEST
2	us-east-1	SchedulerCLI-InstanceSchedulerMain	128	300	$LATEST
3	us-east-1	my_functions_function10	128	3	$LATEST
4	us-east-1	lex-web-ui-CognitoIdentityP-CleanStackNameFunction-1TSORSH6L6YXQ	128	300	$LATEST
5	us-east-1	GetLatestArn	128	3	$LATEST
6	us-east-1	aws-python-http-api-project-dev-hello	1024	6	$LATEST
7	us-east-1	cloud9-MyTest-MyTest-688JGPVYP37L	128	15	$LATEST
8	us-east-1	my_functions_function1	128	3	$LATEST
9	us-east-1	my_functions_function25	128	3	$LATEST

Wenn die AWS Config Daten unternehmensweit aggregiert sind, können Sie dann mit Amazon QuickSight ein Dashboard erstellen. Durch den Import Ihrer Athena-Ergebnisse in Amazon können Sie visualisieren QuickSight, wie gut Ihre Lambda-Funktionen der Layer-Versionsregel entsprechen. Im Dashboard können Sie konforme und nicht konforme Ressourcen hervorheben und dementsprechend Durchsetzungsrichtlinien festlegen, wie im nächsten Abschnitt beschrieben. Die folgende Abbildung zeigt ein Beispiel-Dashboard, in dem die Verteilung der Layer-Versionen auf Funktionen innerhalb der Organisation aufgeschlüsselt ist.



Phase 3: Implementierung und Durchsetzung

Sie können Ihre Layer-Versionsregel, die Sie in Phase 1 erstellt haben, jetzt optional über ein Systems-Manager-Automatisierungsdokument, das Sie als Python-Skript mit AWS SDK for Python (Boto3) erstellt haben, mit einer Behebungsaktion verknüpfen. Das Skript ruft die

UpdateFunctionKonfigurations-API-Aktion für jede Lambda-Funktion auf und aktualisiert die Funktionskonfiguration mit dem neuen Layer-ARN. Alternativ können Sie das Skript so schreiben, dass eine Pull-Anfrage an das Code-Repository gesendet wird, um den Layer-ARN zu aktualisieren. Auf diese Weise werden künftige Codebereitstellungen ebenfalls mit dem richtigen Layer-ARN aktualisiert.

Lambda-Codesignatur mit AWS Signer

AWS Signer ist ein vollständig verwalteter Codesignaturdienst, mit dem Sie Ihren Code anhand einer digitalen Signatur validieren können, um sicherzustellen, dass er unverändert ist und von einem vertrauenswürdigen Publisher stammt. AWS Signer kann in Verbindung mit AWS Lambda verwendet werden, um vor der Implementierung in Ihren AWS-Umgebungen zu prüfen, ob Funktionen und Layer unverändert sind. Ihr Unternehmen bleibt so vor böswilligen Akteuren geschützt, die sich möglicherweise Zugangsdaten verschafft haben, um neue Funktionen zu entwickeln oder bestehende Funktionen zu verändern.

Um die Codesignatur für Ihre Lambda-Funktionen einzurichten, erstellen Sie zunächst einen S3-Bucket mit aktivierter Versionierung. Erstellen Sie anschließend ein Signaturprofil mit AWS Signer, geben Sie Lambda als Plattform und die Gültigkeitsdauer des Signaturprofils in Tagen an. Beispiel:

```
Signer:
  Type: AWS::Signer::SigningProfile
  Properties:
    PlatformId: AWSLambda-SHA384-ECDSA
    SignatureValidityPeriod:
      Type: DAYS
      Value: !Ref pValidDays
```

Verwenden Sie dann das Signaturprofil und erstellen Sie eine Signaturkonfiguration mit Lambda. Legen Sie fest, was geschehen soll, wenn in der Signaturkonfiguration ein Artefakt erkannt wird, das nicht mit der erwarteten digitalen Signatur übereinstimmt: warnen (aber die Bereitstellung zulassen) oder erzwingen (und die Bereitstellung blockieren). Das folgende Beispiel ist für Erzwingen und Bereitstellungen blockieren konfiguriert.

```
SigningConfig:
  Type: AWS::Lambda::CodeSigningConfig
  Properties:
    AllowedPublishers:
      SigningProfileVersionArns:
        - !GetAtt Signer.ProfileVersionArn
    CodeSigningPolicies:
      UntrustedArtifactOnDeployment: Enforce
```

Sie haben AWS Signer mit Lambda jetzt so konfiguriert, dass nicht vertrauenswürdige Bereitstellungen blockiert werden. Nehmen wir an, Sie haben eine Funktionsanfrage fertig programmiert und sind nun bereit, die Funktion bereitzustellen. Der erste Schritt besteht darin, den

Code mit den entsprechenden Abhängigkeiten zu komprimieren und dann das Artefakt mit dem von Ihnen erstellten Signaturprofil zu signieren. Sie können dies tun, indem Sie das ZIP-Artefakt in den S3-Bucket hochladen und dann einen Signaturauftrag starten.

```
aws signer start-signing-job \
--source 's3={bucketName=your-versioned-bucket,key=your-prefix/your-zip-
artifact.zip,version=QyaJ3c4qa50LXV.9VaZgXHlsGbvCXxpT}' \
--destination 's3={bucketName=your-versioned-bucket,prefix=your-prefix/}' \
--profile-name your-signer-id
```

Das Ergebnis ist eine Ausgabe wie die folgende, wobei `jobId` das Objekt ist, das im Ziel-Bucket und Präfix erstellt wurde, und `jobOwner` die 12-stellige AWS-Konto-ID, unter der der Auftrag ausgeführt wurde.

```
{
    "jobId": "87a3522b-5c0b-4d7d-b4e0-4255a8e05388",
    "jobOwner": "111122223333"
  }
```

Jetzt können Sie Ihre Funktion mithilfe des signierten S3-Objekts und der von Ihnen erstellten Codesignatur-Konfiguration bereitstellen.

```
  Fn:
    Type: AWS::Serverless::Function
    Properties:
      CodeUri: s3://your-versioned-bucket/your-prefix/87a3522b-5c0b-4d7d-
b4e0-4255a8e05388.zip
      Handler: fn.handler
      Role: !GetAtt FnRole.Arn
      CodeSigningConfigArn: !Ref pSigningConfigArn
```

Sie können eine Funktionsbereitstellung alternativ mit dem ursprünglichen unsignierten Quell-ZIP-Artefakt testen. Die Bereitstellung sollte mit der folgenden Fehlermeldung fehlschlagen:

```
Lambda cannot deploy the function. The function or layer might be signed using a
 signature that the client is not configured to accept. Check the provided signature
 for unsigned.
```

Wenn Sie Ihre Funktionen mithilfe von AWS Serverless Application Model (AWS SAM) erstellen und bereitstellen, übernimmt der Paketbefehl das Hochladen des ZIP-Artefakts auf S3 und startet auch

den Signaturauftrag und ruft das signierte Artefakt ab. Verwenden Sie dazu den folgenden Befehl mit diesen Parametern:

```
sam package -t your-template.yaml \
--output-template-file your-output.yaml \
--s3-bucket your-versioned-bucket \
--s3-prefix your-prefix \
--signing-profiles your-signer-id
```

Mit AWS Signer können Sie überprüfen, ob ZIP-Artefakte, die in Ihren Konten bereitgestellt werden, vertrauenswürdig sind. Sie können den oben genannten Prozess in Ihre CI/CD-Pipelines aufnehmen und verlangen, dass allen Funktionen eine Codesignatur-Konfiguration zugewiesen ist. Verwenden Sie dabei die in den vorherigen Themen beschriebenen Techniken. Durch die Verwendung einer Codesignatur bei der Bereitstellung von Lambda-Funktionen verhindern Sie, dass böswillige Akteure, die möglicherweise Anmeldeinformationen für die Erstellung oder Änderung von Funktionen erhalten haben, bösartigen Code in Ihre Funktionen einschleusen.

Automatisieren Sie Sicherheitsbewertungen für Lambda mit Amazon Inspector

Amazon Inspector ist ein automatisierter Schwachstellen-Management-Service, der Workloads kontinuierlich auf bekannte Softwareschwachstellen und unbeabsichtigte Netzwerkfreigabe durchsucht. Amazon Inspector erstellt einen Bericht, der die Schwachstelle beschreibt, die betroffene Ressource identifiziert, den Schweregrad der Schwachstelle bewertet und Hilfestellung zur Behebung gibt.

Amazon Inspector bietet eine kontinuierliche, automatisierte Schwachstellenanalyse für Lambda-Funktionen und -Layer. Amazon Inspector stellt zwei Scantypen für Lambda bereit:

- Lambda-Standardscan (Standard): Scannt Anwendungsabhängigkeiten innerhalb einer Lambda-Funktion und ihrer Layer auf Paketschwachstellen.
- Lambda-Codescan: Scannt den benutzerdefinierten Anwendungscode in Funktionen und Layern auf Code-Schwachstellen. Sie können entweder den Lambda-Standardscan einzeln oder zusammen mit dem Lambda-Codescan aktivieren.

Um Amazon Inspector zu aktivieren, navigieren Sie zur Amazon-Inspector-Konsole, erweitern Sie den Bereich Einstellungen und wählen Sie Kontoverwaltung. Wählen Sie auf der Registerkarte Konten die Option Aktivieren und wählen Sie dann eine der Scanoptionen aus.

Sie können Amazon Inspector für mehrere Konten aktivieren und bei der Einrichtung von Amazon Inspector die Berechtigungen zur Verwaltung von Amazon Inspector für die Organisation an bestimmte Konten delegieren. Während der Aktivierung müssen Sie Amazon Inspector Berechtigungen erteilen, indem Sie die folgende Rolle erstellen: `AWSServiceRoleForAmazonInspector2`. In der Amazon-Inspector-Konsole können Sie diese Rolle mit einem Klick erstellen.

Beim Lambda-Standardscan initiiert Amazon Inspector Schwachstellenscans von Lambda-Funktionen in den folgenden Situationen:

- Sobald Amazon Inspector eine bestehende Lambda-Funktion entdeckt.
- Wenn Sie eine neue Lambda-Funktion bereitstellen.
- Wenn Sie ein Update für den Anwendungscode oder die Abhängigkeiten einer vorhandenen Lambda-Funktion oder ihrer Layer bereitstellen.

- Immer wenn Amazon Inspector seiner Datenbank ein neues CVE-Element (Common Vulnerabilities and Exposures) hinzufügt und dieses CVE für Ihre Funktion relevant ist.

Beim Lambda-Codescan wertet Amazon Inspector Ihren Lambda-Funktionscode mithilfe von Automated Reasoning und Machine Learning aus. Dabei wird der Anwendungscode auf die allgemeine Einhaltung der Sicherheitsregeln hin analysiert. Wenn Amazon Inspector eine Sicherheitslücke in Ihrem Anwendungscode für Lambda-Funktionen entdeckt, erstellt Amazon Inspector einen detaillierten Schwachstellenbericht für den Code. Eine Liste möglicher Erkennungen finden Sie in der Amazon CodeGuru Detector Library.

Rufen Sie die Amazon-Inspector-Konsole auf, um die Berichte einzusehen. Wählen Sie im Menü Funde die Option Nach Lambda-Funktion, um die Ergebnisse der Sicherheitsscans anzuzeigen, die für Lambda-Funktionen durchgeführt wurden.

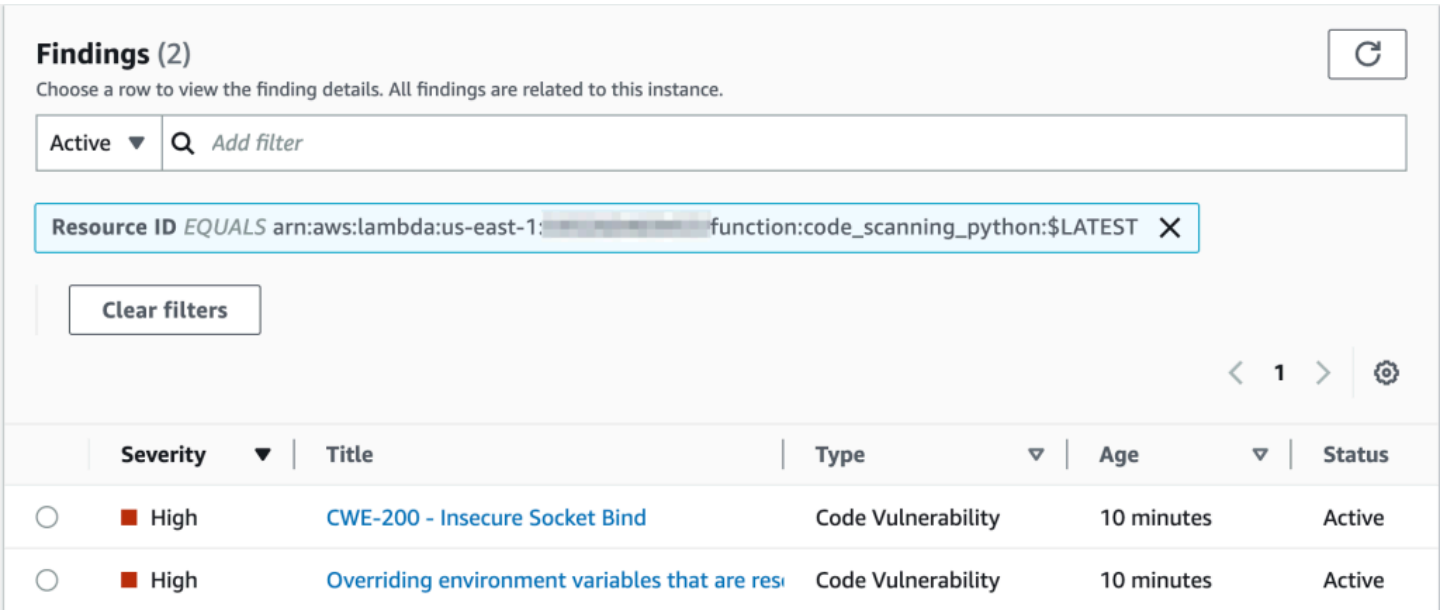
Um eine Lambda-Funktion vom Standardscan auszuschließen, kennzeichnen Sie die Funktion mit dem folgenden Schlüssel-Wert-Paar:

- `Key:InspectorExclusion`
- `Value:LambdaStandardScanning`

Um eine Lambda-Funktion von Codescans auszuschließen, kennzeichnen Sie die Funktion mit dem folgenden Schlüssel-Wert-Paar:

- `Key:InspectorCodeExclusion`
- `Value:LambdaCodeScanning`

Wie in der folgenden Abbildung dargestellt, erkennt Amazon Inspector Schwachstellen automatisch und kategorisiert die Funde beispielsweise als Codeschwachstelle. Das deutet darauf hin, dass sich die Schwachstelle im Funktionscode befindet und nicht in einer der codeabhängigen Bibliotheken. Sie können diese Details für eine bestimmte Funktion oder mehrere Funktionen gleichzeitig einsehen.



Sie können jeden Befund eingehend untersuchen und erfahren, wie Sie das Problem beheben können.

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior.

Finding ID: arn:aws:inspector2:us-east-1:[redacted]:finding/[redacted]

Overriding environment variables that are reserved by AWS Lambda might lead to unexpected behavior or failure of the Lambda function.

Finding overview	
AWS account ID	[redacted]
Severity	High
Type	Code Vulnerability
Detector name	Override of reserved variable names in a Lambda function
Relevant CWE	--
Rule ID	Rule-434311
Detector tags	#availability, #aws-python-sdk, #aws-lambda, #data-integrity, #maintainability, #security, #security-context, #python
Fix available	Yes
Created at	March 29, 2023 10:08 AM (UTC-04:00)

Vulnerability details	
File path	lambda_function.py

Vulnerability location

```
3  import socket
4
5  def lambda_handler(event, context):
6
7      # print("Scenario 1");
8      os.environ['_HANDLER'] = 'hello'
9      # print("Scenario 1 ends")
10
11     # print("Scenario 2");
12     s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
13     s.bind(('',0))
```

Suggested remediation

Your code attempts to override an environment variable that is reserved by the Lambda runtime environment. This can lead to unexpected behavior and might break the execution of your Lambda function.

Achten Sie bei der Verwendung von Lambda-Funktionen darauf, dass Sie die Namenskonventionen einhalten. Weitere Informationen finden Sie unter Verwenden Sie Lambda-Umgebungsvariablen, um Werte im Code zu konfigurieren.

Sie sind für die Lösungsvorschläge verantwortlich, die Sie akzeptieren. Lesen Sie sich die Lösungsvorschläge immer durch, bevor Sie sie annehmen. Möglicherweise müssen Sie Anpassungen an den Lösungsvorschlägen vornehmen, damit Ihr Code am Ende auch das tut, was Sie beabsichtigt haben.

Implementieren von Beobachtbarkeit für Lambda-Sicherheit und -Compliance

AWS Config ist ein hilfreiches Tool, um nicht konforme AWS-Serverless-Ressourcen zu finden und zu beheben. Jede Änderung, die Sie an Ihren Serverless-Ressourcen vornehmen, wird in AWS Config aufgezeichnet. AWS Config ermöglicht es Ihnen außerdem, Konfigurations-Snapshot-Daten auf S3 zu speichern. Sie können Amazon Athena und Amazon verwenden QuickSight , um Dashboards zu erstellen und AWS Config Daten anzuzeigen. In Erkennen Sie nicht konforme Lambda-Bereitstellungen und -Konfigurationen mit AWS Config haben wir besprochen, wie sich bestimmte Konfigurationen wie Lambda-Layer visualisieren lassen. Dieses Thema erweitert diese Konzepte.

Abrufen von Informationen zu Lambda-Konfigurationen

Sie können Abfragen verwenden, um wichtige Konfigurationen wie AWS-Konto-ID, Region, AWS X-Ray-Ablaufverfolgungskonfiguration, VPC-Konfiguration, Speichergröße, Laufzeit und Tags abzurufen. Hier ist eine Beispielabfrage, mit der Sie diese Informationen von Athena abrufen können:

```
WITH unnested AS (
    SELECT
      item.awsaccountid AS account_id,
      item.awsregion AS region,
      item.configuration AS lambda_configuration,
      item.resourceid AS resourceid,
      item.resourcename AS resourcename,
      item.configuration AS configuration,
      json_parse(item.configuration) AS lambda_json
    FROM
      default.aws_config_configuration_snapshot,
      UNNEST(configurationitems) as t(item)
    WHERE
      "dt" = 'latest'
      AND item.resourcetype = 'AWS::Lambda::Function'
  )

  SELECT DISTINCT
    account_id,
    tags,
    region as Region,
    resourcename as FunctionName,
    json_extract_scalar(lambda_json, '$.memorySize') AS memory_size,
```

```
    json_extract_scalar(lambda_json, '$.timeout') AS timeout,
    json_extract_scalar(lambda_json, '$.runtime') AS version
    json_extract_scalar(lambda_json, '$.vpcConfig.SubnetIds') AS vpcConfig
    json_extract_scalar(lambda_json, '$.tracingConfig.mode') AS tracingConfig
  FROM
    unnested
```

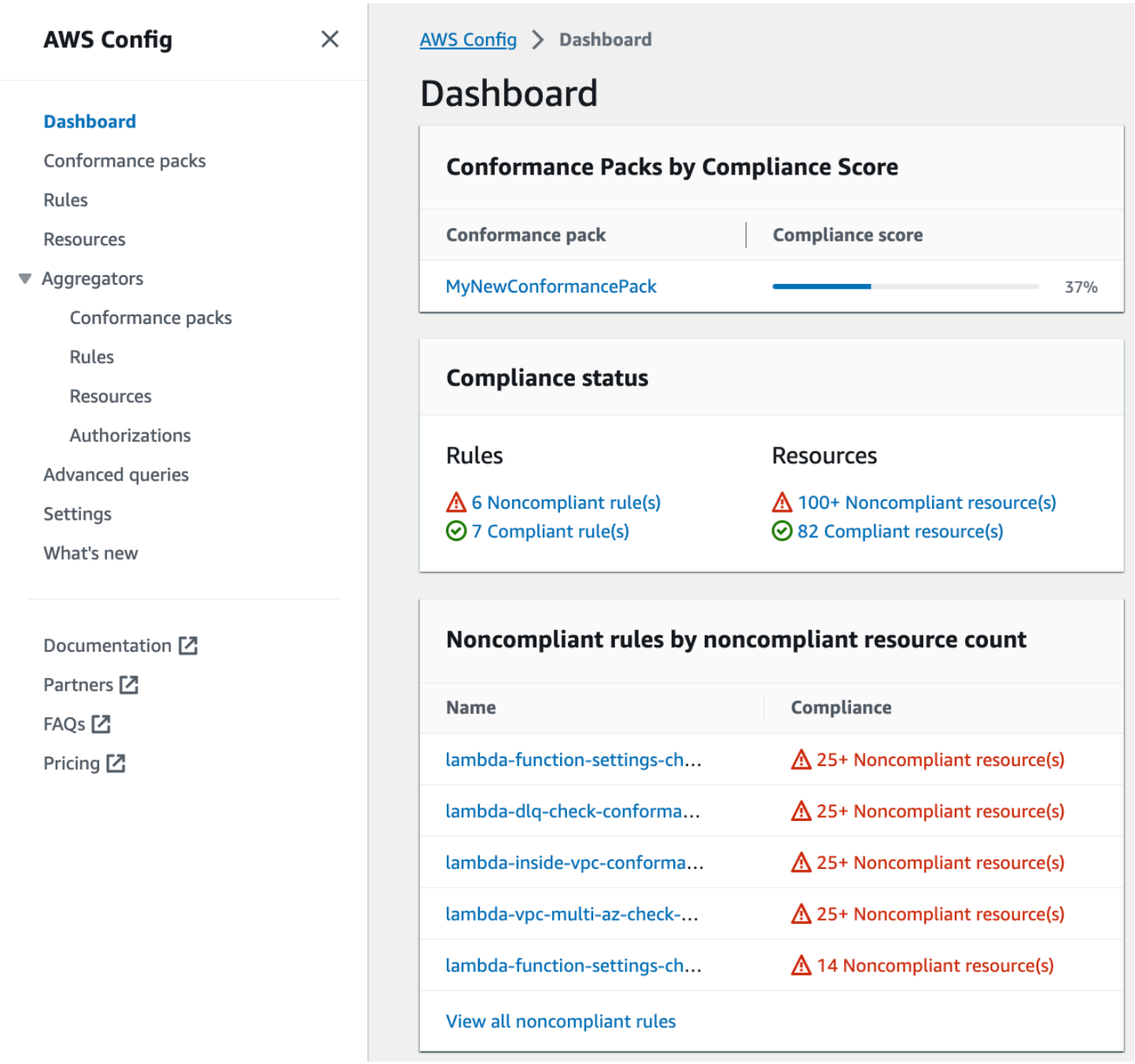
Sie können die Abfrage verwenden, um ein Amazon QuickSight -Dashboard zu erstellen und die Daten zu visualisieren. Informationen zum Aggregieren von AWS Ressourcenkonfigurationsdaten, Erstellen von Tabellen in Athena und Erstellen von Amazon- QuickSight Dashboards auf den Daten von Athena finden Sie unter Visualisieren von AWS Config Daten mit Athena und Amazon QuickSight im AWS Cloud Operations and Management-Blog. Diese Abfrage ruft auch Tag-Informationen für die Funktionen ab. Dies ermöglicht eine genauere Untersuchung Ihrer Workloads und Umgebungen, insbesondere wenn Sie benutzerdefinierte Tags verwenden.

Weitere Informationen über die Aktionen, die Sie ergreifen können, finden Sie im Abschnitt Behandlung von Beobachtbarkeitsbefunden weiter unten in diesem Thema.

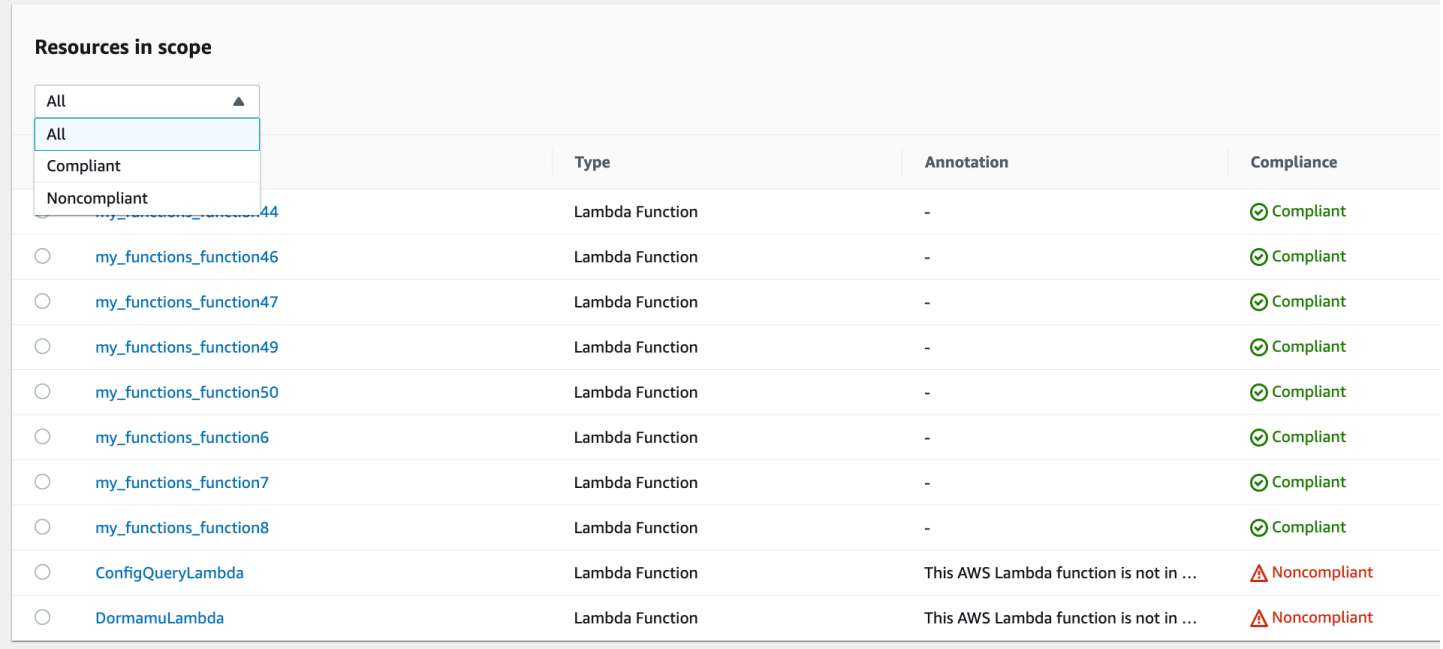
Abrufen von Informationen zur Lambda-Konformität

Mit den AWS Config von generierten Daten können Sie Dashboards auf Organisationsebene erstellen, um die Einhaltung von Vorschriften zu überwachen. Dies ermöglicht eine konsistente Nachverfolgung und Überwachung von:

- Compliance-Paketen nach Konformitätsbewertung
- Regeln von nicht konformen Ressourcen
- Compliance status (Compliance-Status)

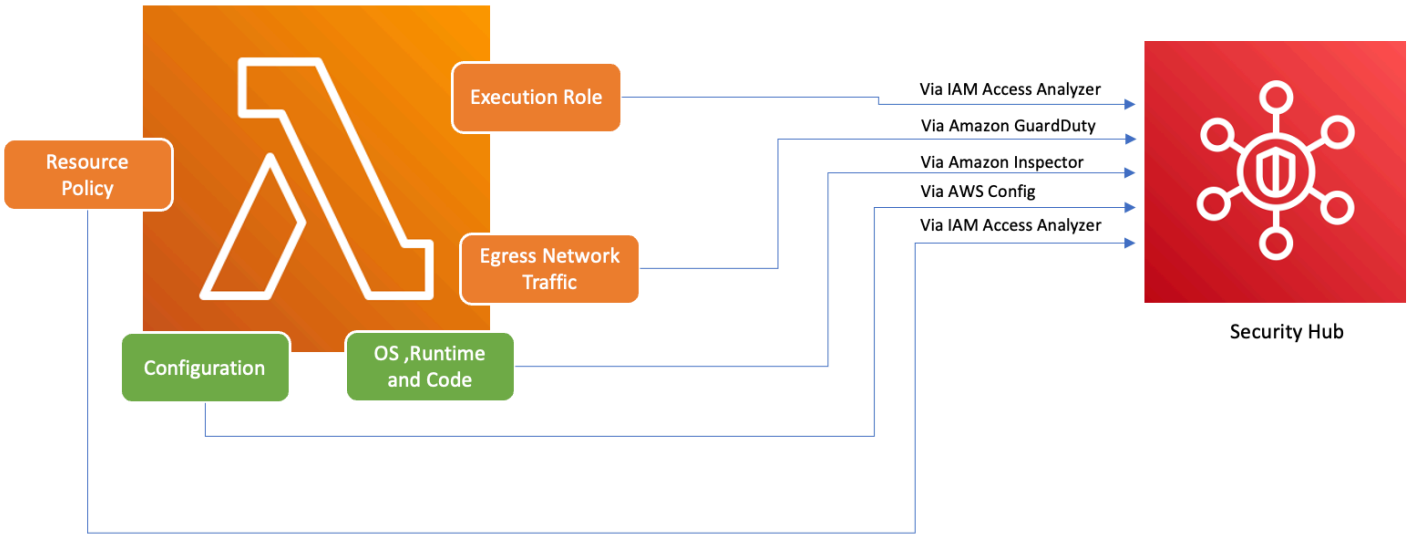


Überprüfen Sie jede Regel, um Ressourcen zu identifizieren, die für diese Regel nicht konform sind. Wenn Ihre Organisation beispielsweise vorschreibt, dass alle Lambda-Funktionen einer VPC zugeordnet werden müssen, und Sie eine AWS Config-Regel zur Konformitätserkennung bereitgestellt haben, können Sie die `lambda-inside-vpc`-Regel in der obigen Liste auswählen.



Weitere Informationen über die Aktionen, die Sie ergreifen können, finden Sie im Abschnitt [Behandlung von Beobachtbarkeitsbefunden] weiter unten.

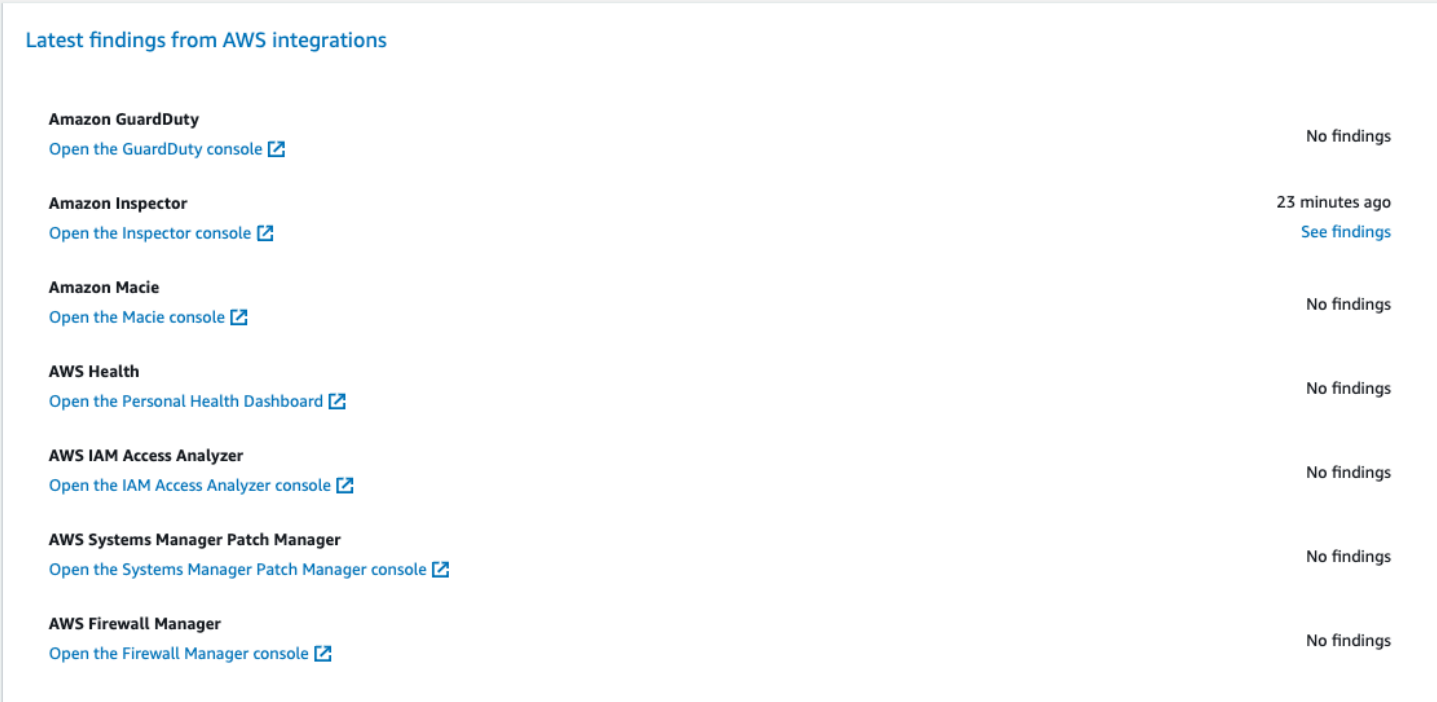
Abrufen von Informationen zu den Lambda-Funktionsgrenzen über Security Hub



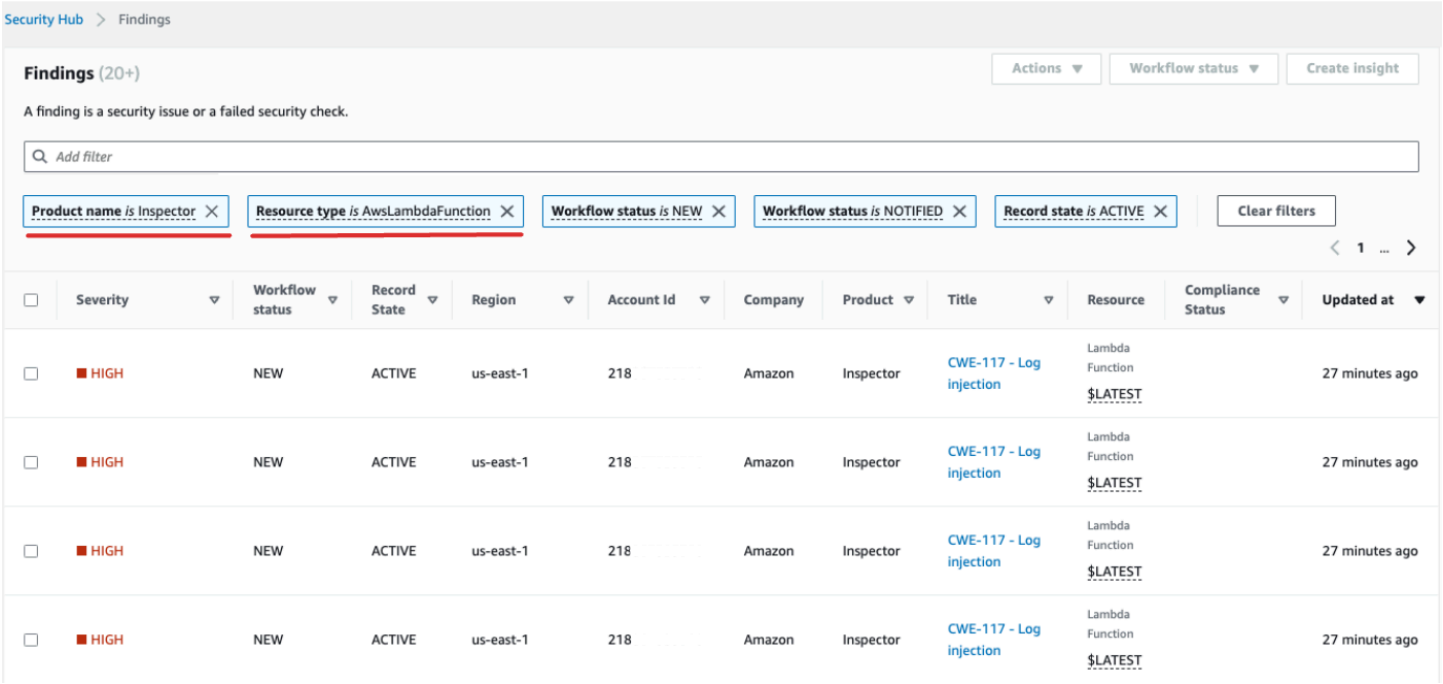
Um sicherzustellen, dass AWS-Dienste, einschließlich Lambda, sicher verwendet werden können, hat AWS die Foundational Security Best Practices v1.0.0 eingeführt. Diese Sammlung von bewährten Methoden enthält klare Richtlinien für den Schutz von Ressourcen und Daten in der AWS-Umgebung und unterstreicht, wie wichtig Sicherheitsmaßnahmen sind. AWS Security Hub ergänzt dieses Angebot um ein zentrales Sicherheits- und Compliance-Center. Es aggregiert, organisiert und

priorisiert Sicherheitserkenntnisse aus mehreren Services AWS wie Amazon Inspector AWS Identity and Access Management Access Analyzer, und Amazon GuardDuty. Amazon Inspector

Wenn Sie Security Hub, Amazon Inspector, IAM Access Analyzer und innerhalb Ihrer AWS Organisation GuardDuty aktiviert haben, aggregiert Security Hub automatisch die Ergebnisse dieser Services. Betrachten wir zum Beispiel Amazon Inspector. Mit Security Hub können Sie Code- und Paketschwachstellen in Lambda-Funktionen effizient identifizieren. Navigieren Sie in der Security-Hub-Konsole zum unteren Abschnitt Aktuelle Befunde aus AWS-Integrationen. Hier können Sie Ergebnisse aus verschiedenen integrierten AWS-Diensten einsehen und untersuchen.



Für Details klicken Sie in der zweiten Spalte auf den Link Befunde anzeigen. Daraufhin wird eine nach Produkten gefilterte Liste mit Ergebnissen angezeigt, z. B. Amazon Inspector. Um Ihre Suche auf Lambda-Funktionen zu beschränken, setzen Sie `ResourceType` auf `AwsLambdaFunction`. Nun werden Ergebnisse von Amazon Inspector zu Lambda-Funktionen angezeigt.



Für können GuardDutySie verdächtige Netzwerkverkehrsmuster identifizieren. Solche Anomalien könnten auf die Existenz von potenziell bösartigem Code in Ihrer Lambda-Funktion hindeuten.

Mit IAM Access Analyzer können Sie Richtlinien überprüfen, insbesondere solche mit Bedingungsanweisungen, die externen Entitäten Funktionszugriff gewähren. Darüber hinaus wertet IAM Access Analyzer Berechtigungen aus, die bei der Verwendung der -AddPermissionOperation in der Lambda-API zusammen mit einem festgelegt wurden`EventSourceToken`.

Behandlung von Beobachtbarkeitsbefunden

Angesichts der vielfältigen Konfigurationen, die für Lambda-Funktionen möglich sind, und ihrer unterschiedlichen Anforderungen ist eine standardisierte Automatisierungslösung für die Problembehebung möglicherweise nicht für jede Situation geeignet. Darüber hinaus werden Änderungen in den verschiedenen Umgebungen unterschiedlich implementiert. Wenn Sie auf eine Konfiguration stoßen, die nicht konform zu sein scheint, beachten Sie die folgenden Richtlinien:

1. Strategie zur Kennzeichnung

   Wir empfehlen die Implementierung einer umfassenden Kennzeichnungsstrategie. Jede Lambda-Funktion sollte mit folgenden Schlüsselinformationen gekennzeichnet sein:

   - Eigentümer: Die Person oder das Team, die für die Funktion verantwortlich ist.
   - Umgebung: Produktion, Staging, Entwicklung oder Sandbox.

- Anwendung: Der breitere Kontext, zu dem diese Funktion gehört, falls zutreffend.

2. Kontakt zum Eigentümer

   Anstatt notwendige Änderungen zu automatisieren (wie die Anpassung der VPC-Konfiguration), sollten Sie sich an die Eigentümer nicht konformer Funktionen (siehe Eigentümer-Tag) wenden und ihnen genügend Zeit geben, um entweder:

   - nicht konforme Konfigurationen für Lambda-Funktionen anzupassen
   - eine Erklärung bereitzustellen und eine Ausnahme anzufordern oder die Compliance-Standards anzupassen

3. Fühen Sie eine Configuration Management Database (CMDB)

   Tags können zwar unmittelbar Kontext liefern, eine zentralisierte CMDB kann jedoch genauere Informationen liefern. Die Datenbank kann detaillierte Informationen über jede Lambda-Funktion, ihre Abhängigkeiten und andere wichtige Metadaten enthalten. Eine CMDB ist eine unschätzbare Ressource für Audits, Konformitätsprüfungen und die Identifizierung der Eigentümer einer Funktion.

Da sich Serverless-Infrastrukturen kontinuierlich weiterentwickeln, ist es wichtig, Überwachungsmaßnahmen proaktiv zu organisieren. Mit Tools wie AWS Config, Security Hub und Amazon Inspector können potenzielle Anomalien oder nicht konforme Konfigurationen schnell identifiziert werden. Tools allein können jedoch keine vollständige Konformität oder optimale Konfigurationen gewährleisten. Es ist wichtig, diese Tools mit gut dokumentierten Prozessen und bewährten Verfahren zu kombinieren.

- Feedback-Schleife: Sobald Korrekturmaßnahmen ergriffen werden, sollten Sie sicherstellen, dass es eine Feedback-Schleife gibt. Dabei werden nicht konforme Ressourcen regelmäßig überprüft, um zu ermitteln, ob sie aktualisiert wurden oder immer noch dieselben Probleme haben.
- Dokumentation: Beobachtungen, Maßnahmen und alle gewährten Ausnahmen sollten immer dokumentiert werden. Eine ordnungsgemäße Dokumentation hilft nicht nur bei Audits, sondern trägt auch dazu bei, den Prozess zu verbessern, um die Compliance und Sicherheit dauerhaft zu stärken.
- Schulung und Sensibilisierung: Alle Beteiligten, insbesondere die Eigentümer der Lambda-Funktionen, sollten regelmäßig geschult und über bewährte Verfahren, Unternehmensrichtlinien und Compliance-Vorschriften informiert werden. Regelmäßige Workshops, Webinare oder

Schulungen können einen großen Beitrag dazu leisten, dass alle Beteiligten bezüglich Sicherheit und Compliance auf dem gleichen Stand sind.

Zusammenfassend lässt sich sagen, dass Tools und Technologien zwar die Erkennung und Meldung von potenziellen Problemen unterstützen, der Faktor Mensch –Verständnis, Kommunikation, Schulung und Dokumentation – aber weiterhin von zentraler Bedeutung ist. Beides zusammen ergibt eine leistungsstarke Kombination, um sicherzustellen, dass Ihre Lambda-Funktionen und die größere Infrastruktur konform, sicher und für Ihre Geschäftsanforderungen optimiert sind.

Compliance-Validierung für AWS Lambda

Die Auditoren Dritter bewerten die Sicherheit und die Compliance von AWS Lambda im Rahmen mehrerer AWS-Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Eine Liste der AWS-Services, die in den Geltungsbereich bestimmter Compliance-Programme fallen, finden Sie auf der Seite AWS-Services in Scope nach Compliance-Programm. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Die Auditberichte von Drittanbietern lassen sich mit AWS Artifact herunterladen. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS-Artifact.

Ihre Compliance-Verantwortung bei Verwendung von Lambda hängt von der Vertraulichkeit der Daten, den Compliance-Zielen des Unternehmens und den geltenden Gesetzen und Vorschriften ab. Sie können Governance-Kontrollen implementieren, um sicherzustellen, dass die Lambda-Funktionen Ihres Unternehmens Ihren Compliance-Anforderungen entsprechen. Weitere Informationen finden Sie unter Erstellen Sie eine Governance-Strategie für Lambda-Funktionen und -Layer.

Ausfallsicherheit in AWS Lambda

Im Zentrum der globalen AWS-Infrastruktur stehen die AWS-Regionen und Availability Zones. AWS Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die mit Netzwerken mit geringer Latenz, hohem Durchsatz und hochredundanten Vernetzungen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

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

Zusätzlich zur globalen AWS-Infrastruktur stellt Lambda verschiedene Funktionen bereit, um Ihren Anforderungen in Bezug auf Ausfallsicherheit und Datensicherung zu erfüllen.

- Versioning – Sie können in Lambda Versioning verwenden, um Code und Konfiguration Ihrer Funktion während ihrer Entwicklung zu speichern. In Verbindung mit Aliasnamen können Sie Versioning verwenden, um blaue/grüne und fortlaufende Bereitstellungen ausfzuführen. Details hierzu finden Sie unter Versionen der Lambda-Funktion.

- Skalierung – Wenn Ihre Funktion während der Verarbeitung einer früheren Anforderung eine weitere Anforderung empfängt, startet Lambda eine weitere Instance Ihrer Funktion, um die höhere Last zu verarbeiten. Lambda wird automatisch skaliert, um 1.000 gleichzeitige Ausführungen pro Region zu verarbeiten, ein Kontingent, das bei Bedarf erhöht werden kann. Details hierzu finden Sie unter Die Lambda-Funktionsskalierung verstehen.
- Hohe Verfügbarkeit – Lambda führt Ihre Funktion in mehreren Availability Zones aus, um sicherzustellen, dass sie für die Verarbeitung von Ereignissen verfügbar ist, wenn der Service in einer Zone unterbrochen wird. Wenn Sie Ihre Funktion für die Herstellung von Verbindungen mit einer Virtual Private Cloud (VPC) in Ihrem Konto konfigurieren, geben Sie Subnetze in mehreren Availability Zones an, um eine hohe Verfügbarkeit sicherzustellen. Details hierzu finden Sie unter Lambda-Funktionen Zugriff auf Ressourcen in einer Amazon VPC gewähren.
- Reservierte Gleichzeitigkeit – Um sicherzustellen, dass Ihre Funktion stets skaliert werden kann, um zusätzliche Anforderungen zu verarbeiten, können Sie für sie Gleichzeitigkeit reservieren. Die Reservierung von Gleichzeitigkeit für eine Funktion stellt sicher, dass sie bis zu einer angegebenen Anzahl gleichzeitiger Aufrufe skaliert werden kann, diese Anzahl jedoch nicht überschreitet. Auf diese Weise wird sichergestellt, dass keine Anforderungen verloren gehen, da andere Funktionen der gesamte verfügbare Gleichzeitigkeit verbrauchen. Details hierzu finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.
- Wiederholversuche – Im Fall asynchroner Aufrufe und bestimmter, von anderen Diensten ausgelöster Aufrufe führt Lambda bei Fehlern automatisch Wiederholversuche mit Verzögerungen zwischen den einzelnen Wiederholversuchen aus. Für die Ausführung der Wiederholversuche sind andere Clients und AWS-Services, die Funktionen synchron aufrufen, verantwortlich. Details hierzu finden Sie unter Grundlegendes zum Wiederholungsverhalten in Lambda.
- Warteschlange für unzustellbare Nachrichten – Im Fall asynchroner Aufrufe können Sie Lambda für das Senden von Anforderungen an eine Warteschlange für unzustellbare Nachrichten konfigurieren, wenn Wiederholversuche fehlschlagen. Eine Warteschlange für unzustellbare Nachrichten ist ein Amazon-SNS-Thema oder eine Amazon-SQS-Warteschlange, die Ereignisse zur Fehlerbehebung oder erneuten Verarbeitung empfängt. Details hierzu finden Sie unter Warteschlangen für unzustellbare Nachrichten.

Sicherheit der Infrastruktur in AWS Lambda

Als verwalteter Service ist AWS Lambda durch die globalen Verfahren zur Gewährleistung der Netzwerksicherheit von AWS geschützt. Informationen zu AWS-Sicherheitsservices und wie AWS die Infrastruktur schützt, finden Sie unter AWS-Cloud-Sicherheit. Informationen zum Entwerfen Ihrer

AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Lambda 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 Fehlerbehebung bei Lambda-Funktionen

AWS Lambda lässt sich in andere AWS Dienste integrieren, um Sie bei der Überwachung und Fehlerbehebung Ihrer Lambda-Funktionen zu unterstützen. Lambda überwacht Lambda-Funktionen automatisch in Ihrem Namen und meldet Metriken über Amazon. CloudWatch Damit Sie Ihren Code während der Ausführung überwachen können, verfolgt Lambda automatisch die Anzahl der Anfragen, die Dauer des Aufrufs pro Anfrage und die Anzahl der Anfragen, die zu einem Fehler führen.

Sie können andere AWS Dienste verwenden, um Probleme mit Ihren Lambda-Funktionen zu beheben. In diesem Abschnitt wird beschrieben, wie Sie diese AWS -Services verwenden, um Ihre Lambda-Funktionen und -Anwendungen zu überwachen, zu verfolgen, zu debuggen und zu beheben. Einzelheiten zur Funktionsprotokollierung und zu Fehlern in jeder Laufzeit finden Sie in den einzelnen Laufzeitabschnitten.

Weitere Informationen zur Überwachung von Lambda-Anwendungen finden Sie bei Serverless Land unter Monitoring and observability.

Sections

Überwachungsfunktionen in der Lambda-Konsole

Der Lambda-Service überwacht Funktionen in Ihrem Namen und sendet Metriken an Amazon CloudWatch. Die Lambda-Konsole erstellt Überwachungsdiagramme für diese Metriken und zeigt sie auf der Seite Überwachung für jede Lambda-Funktion an.

Die Lambda-Konsole stellt Metriken, Protokolle und Ablaufverfolgungen in einem einzigen Fenster bereit. Die Konsole umfasst Filter für Zeitbereich, Zeitzone und Aktualisierungsoptionen, die für alle Bereiche allgemein gelten. Sie können Metriken, Protokolle und Ablaufverfolgungen (Traces) einfach korrelieren und so die mittlere Wiederherstellungszeit (Mean Time To Recovery, MTTR) bei der Behebung von Fehlern in Ihren Lambda-Funktionen reduzieren.

Preisgestaltung

CloudWatch verfügt über ein unbegrenztes kostenloses Kontingent. Über den Schwellenwert des kostenlosen Kontingents hinaus CloudWatch werden Gebühren für Metriken, Dashboards, Alarme, Protokolle und Erkenntnisse berechnet. Weitere Informationen finden Sie unter Amazon- CloudWatch Preise.

Verwenden von Lambda-Konsole

Ihre Lambda-Funktionen und -Anwendungen können Sie in der Lambda-Konsole überwachen.

So überwachen Sie eine Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie den Tab Überwachung.

Arten von Überwachungsdiagrammen

Der folgende Abschnitt beschreibt die Überwachungsdiagramme in der Lambda-Konsole.

Lambda-Überwachungsdiagramme

- Aufrufe – Gibt die Häufigkeit an, mit der die Funktion jeweils aufgerufen wurde.
- Duration (Dauer) – Die durchschnittliche, minimale und maximale Zeitspanne, die Ihr Funktionscode zur Verarbeitung eines Ereignisses aufwendet.

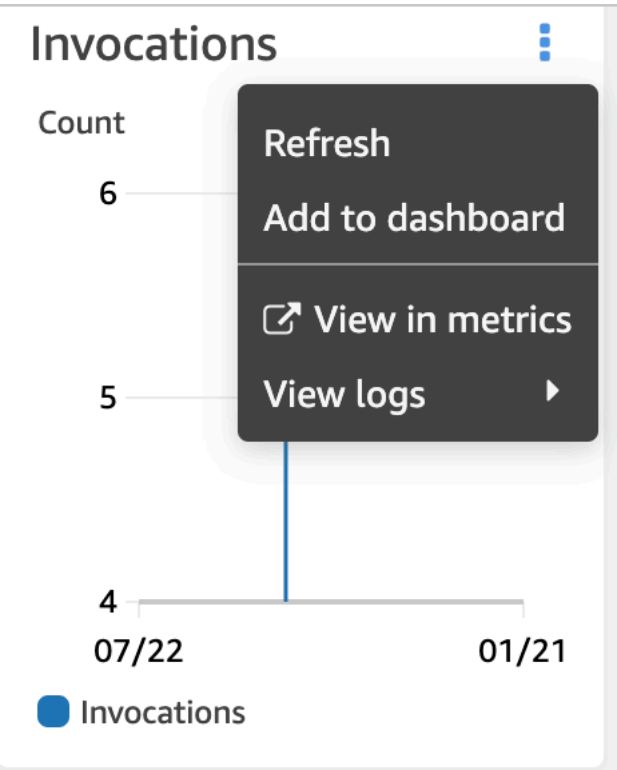
- Error count and success rate (%) (Fehleranzahl und Erfolgsrate (%)) – Die Anzahl der Fehler und der Prozentsatz der Aufrufe, die ohne Fehler abgeschlossen wurden.
- Throttles (Drosselungen) – Die Häufigkeit, mit der ein Aufruf aufgrund von Nebenläufigkeitslimits fehlgeschlagen ist.
- IteratorAge – Bei Stream-Ereignisquellen das Alter des letzten Elements im Batch, als Lambda es empfangen und die Funktion aufgerufen hat.
- Asynchrone Zustellungsfehler – Die Anzahl der Fehler, die bei dem Versuch von Lambda, in eine Ziel- oder Warteschlange zu schreiben, aufgetreten sind.
- Gleichzeitige Ausführungen – Die Anzahl der Funktions-Instances, die Ereignisse verarbeiten.

Anzeigen von Diagrammen in der Lambda-Konsole

Im folgenden Abschnitt wird beschrieben, wie Sie CloudWatch Überwachungsdiagramme in der Lambda-Konsole anzeigen und das CloudWatch Metrik-Dashboard öffnen.

So zeigen Sie Überwachungsdiagramme für eine Funktion an

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie den Tab Überwachung.
4. Wählen Sie aus den vordefinierten Zeitbereichen oder wählen Sie einen benutzerdefinierten Zeitbereich aus.
5. Um die Definition eines Diagramms in anzuzeigen CloudWatch, wählen Sie die drei vertikalen Punkte (Widget-Aktionen) und dann In Metriken anzeigen, um das Metrik-Dashboard in der CloudWatch Konsole zu öffnen.

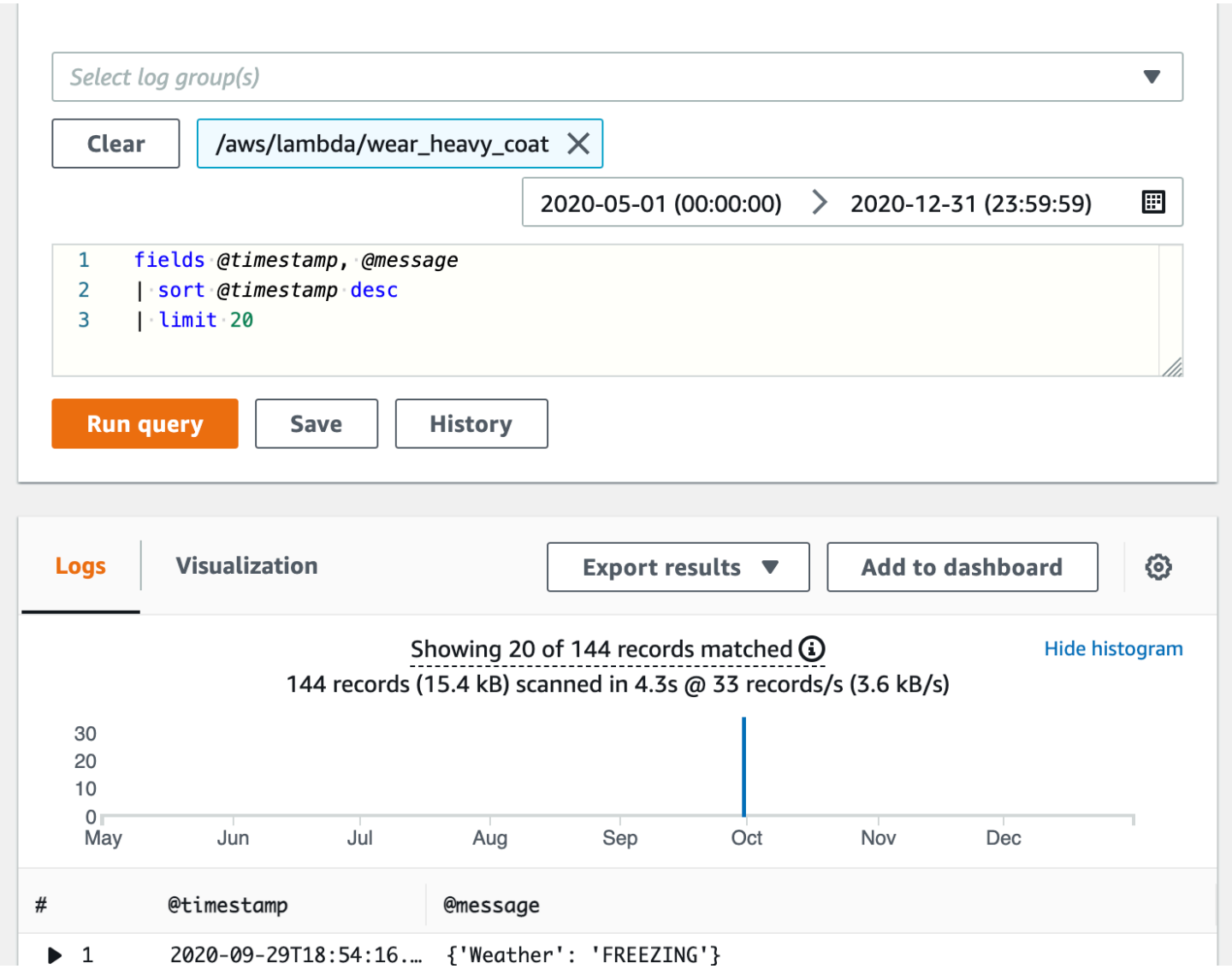


Anzeigen von Abfragen in der CloudWatch Logs-Konsole

Im folgenden Abschnitt wird beschrieben, wie Sie Berichte aus CloudWatch Logs Insights anzeigen und zu einem benutzerdefinierten Dashboard in der CloudWatch Logs-Konsole hinzufügen.

So zeigen Sie Berichte für eine Funktion an

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie den Tab Überwachung.
4. Wählen Sie Protokolle anzeigen in CloudWatch.
5. Wählen Sie In Logs Insights anzeigen aus.
6. Wählen Sie aus den vordefinierten Zeitbereichen oder wählen Sie einen benutzerdefinierten Zeitbereich aus.
7. Klicken Sie auf Abfrage ausführen.
8. (Optional) Wählen Sie Save (Speichern) aus.



Als nächstes

- Erfahren Sie mehr über die Metriken, die Lambda aufzeichnet und an sendet, CloudWatch in Arbeiten mit Lambda-Funktionsmetriken.
- Erfahren Sie, wie Sie CloudWatch Lambda Insights verwenden, um Leistungsmetriken und Protokolle der Lambda-Funktionslaufzeit in zu erfassen und zu aggregierenÜberwachen Sie die Funktionsleistung mit Amazon CloudWatch Lambda Insights.

Arbeiten mit Lambda-Funktionsmetriken

Wenn Ihre AWS Lambda Funktion die Verarbeitung eines Ereignisses abgeschlossen hat, sendet Lambda Metriken über den Aufruf an Amazon. CloudWatch Für diese Metriken fallen keine Gebühren an.

Auf der CloudWatch Konsole können Sie Diagramme und Dashboards mit diesen Metriken erstellen. Sie können Alarme so einstellen, dass sie auf Änderungen bei Auslastung, Leistung oder Fehlerraten reagieren. Lambda sendet metrische Daten CloudWatch in 1-Minuten-Intervallen an. Wenn Sie einen direkteren Einblick in Ihre Lambda-Funktion wünschen, können Sie hochauflösende benutzerdefinierte Metriken erstellen, wie bei Serverless Land beschrieben. Für benutzerdefinierte Metriken und CloudWatch Alarme fallen Gebühren an. Weitere Informationen finden Sie unter Amazon CloudWatch – Preise.

Auf dieser Seite werden die Metriken für den Aufruf, die Leistung und die Parallelität von Lambda-Funktionen beschrieben, die auf der Konsole verfügbar sind. CloudWatch

Sections

Metriken auf der Konsole anzeigen CloudWatch

Sie können die CloudWatch Konsole verwenden, um Funktionsmetriken nach Funktionsname, Alias oder Version zu filtern und zu sortieren.

Um Metriken auf der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die Seite „Metriken“ (`AWS/Lambda`Namespace) der CloudWatch Konsole.
2. Wählen Sie auf der Registerkarte Durchsuchen unter Metriken eine der folgenden Dimensionen aus:

   - Nach Funktionsname (`FunctionName`) – Zeigen Sie Aggregatmetriken für alle Versionen und Aliase einer Funktion anzeigen.
   - Nach Ressource (`Resource`) – Zeigen Sie Metriken für eine Version oder den Alias einer Funktion an.

- Nach ausgeführter Version (`ExecutedVersion`) – Zeigen Sie Metriken für eine Kombination aus Alias und Version an. Verwenden Sie die Dimension `ExecutedVersion`, um Fehlerraten für zwei Versionen einer Funktion zu vergleichen, die beide Ziele eines gewichteten Alias sind.
- Funktionsübergreifend (keine) — Zeigt aggregierte Metriken für alle Funktionen in der aktuellen AWS-Region Version an.

3. Wählen Sie eine Metrik und dann Ad to graph (Zu Grafik hinzufügen) oder eine andere grafische Option aus.

Standardmäßig verwenden Diagramme die `Sum`-Statistik für alle Metriken. Um eine andere Statistik auszuwählen und das Diagramm anzupassen, verwenden Sie die Optionen auf der Registerkarte Graphed metrics (Graphierte Metriken).

> **Note**
>
> Der Zeitstempel einer Metrik gibt an, wann die Funktion aufgerufen wurde. Abhängig von der Dauer des Aufrufs kann es einige Minuten dauern, bis die Metrik ausgegeben wird. Wenn Ihre Funktion beispielsweise ein Timeout von 10 Minuten aufweist, suchen Sie dann über 10 Minuten in der Vergangenheit hinaus nach genauen Metriken.

Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Arten von Metriken

Im folgenden Abschnitt werden die Typen von Lambda-Metriken beschrieben, die auf der CloudWatch Konsole verfügbar sind.

Aufrufmetriken

Aufrufmetriken sind binäre Indikatoren für das Ergebnis eines Lambda-Funktionsaufrufs. Wenn die Funktion beispielsweise einen Fehler zurückgibt, sendet Lambda die `Errors`-Metrik mit dem Wert 1. Um die Anzahl der Funktionsfehler zu erhalten, die jede Minute aufgetreten sind, lassen Sie sich die `Sum` der `Errors`-Metrik mit einem Zeitraum von 1 Minute anzeigen.

> **Note**
>
> Zeigen Sie die folgenden Aufrufmetriken mit der `Sum`-Statistik an.

- `Invocations` – Die Häufigkeit, mit der Ihr Funktionscode aufgerufen wird, einschließlich erfolgreicher Aufrufe und Aufrufe, die zu einem Funktionsfehler führen. Aufrufe werden nicht aufgezeichnet, wenn die Aufrufanforderung gedrosselt wird oder anderweitig zu einem Aufruffehler führt. Der Wert von `Invocations` entspricht der Anzahl der fakturierten Anforderungen.
- `Errors` – Die Anzahl der Aufrufe, die zu einem Funktionsfehler führen. Funktionsfehler schließen Ausnahmen ein, die Ihr Code ausgibt, und Ausnahmen, die die Lambda-Laufzeit ausgibt. Die Laufzeit gibt Fehler für Probleme wie Timeouts und Konfigurationsfehler zurück. Um die Fehlerquote zu berechnen, teilen Sie den Wert von `Errors` durch den Wert von `Invocations`. Beachten Sie, dass der Zeitstempel für eine Fehlermetrik widerspiegelt, wann die Funktion aufgerufen wurde, und nicht, wann der Fehler aufgetreten ist.
- `DeadLetterErrors` – Bei asynchronen Aufrufen die Häufigkeit, mit der Lambda versucht, ein Ereignis an eine Warteschlange für unzustellbare Nachrichten zu senden, was jedoch fehlschlägt. Zustellungsfehler können aufgrund von falsch konfigurierten Ressourcen oder Größenbeschränkungen auftreten.
- `DestinationDeliveryFailures` – Bei asynchronen Aufrufen und unterstützten Zuordnung von Ereignisquellen die Häufigkeit, mit der Lambda versucht, ein Ereignis an ein Ziel zu senden, dies jedoch fehlschlägt. Für die Zuordnung von Ereignisquellen unterstützt Lambda Ziele für Streamquellen (DynamoDB und Kinesis). Zustellungsfehler können aufgrund von Berechtigungsfehlern, falsch konfigurierten Ressourcen oder Größenbeschränkungen auftreten. Fehler können auch dann passieren, wenn Ihre Konfiguration einen nicht unterstützten Zieltyp enthält, z. B. eine Amazon-SQS-FIFO-Warteschlange oder ein Amazon-SNS-FIFO-Thema.
- `Throttles` – Die Anzahl der Aufruf-Anforderungen, die gedrosselt werden. Wenn alle Funktions-Instances Anforderungen verarbeiten und keine Nebenläufigkeit zum Hochskalieren verfügbar ist, lehnt Lambda zusätzliche Anforderungen mit einem `TooManyRequestsException`-Fehler ab. Gedrosselte Anforderungen und andere Aufruffehler zählen nicht als `Invocations` oder `Errors`.
- `OversizedRecordCount`: Bei Amazon-DocumentDB-Ereignisquellen die Anzahl von Ereignissen mit einer Größe von mehr als 6 MB, die Ihre Funktion aus Ihrem Change-Stream empfängt. Lambda verwirft die Nachricht und gibt diese Metrik aus.
- `ProvisionedConcurrencyInvocations` – Gibt an, wie oft Ihr Funktionscode für bereitgestellte Gleichzeitigkeit aufgerufen wird.
- `ProvisionedConcurrencySpilloverInvocations` – Gibt an, wie oft Ihr Funktionscode für Standard-Gleichzeitigkeit aufgerufen wird, wenn die gesamte bereitgestellte Gleichzeitigkeit verwendet wird.
- `RecursiveInvocationsDropped`— Die Häufigkeit, mit der Lambda den Aufruf Ihrer Funktion gestoppt hat, weil erkannt wurde, dass Ihre Funktion Teil einer unendlichen rekursiven

Schleife ist. Verwenden Sie die rekursive Lambda-Schleifenerkennung, um Endlosschleifen zu verhindernüberwacht, wie oft eine Funktion als Teil einer Kette von Anfragen aufgerufen wird, indem Metadaten nachverfolgt werden, die von unterstützten SDKs hinzugefügt wurden. AWS Wenn Ihre Funktion mehr als 16 Mal als Teil einer Kette von Anfragen aufgerufen wird, verwirft Lambda den nächsten Aufruf.

Leistungsmetriken

Performance-Metriken stellen Performance-Details zu einem einzelnen Funktionsaufruf bereit. Die Metrik `Duration` gibt beispielsweise die Zeit in Millisekunden an, die Ihre Funktion auf die Verarbeitung eines Ereignisses aufwendet. Um einen Eindruck davon zu erhalten, wie schnell Ihre Funktion Ereignisse verarbeitet, können Sie sich diese Metriken mit der Statistik `Average` oder `Max` anzeigen lassen.

- `Duration` – Die Zeit, die Ihr Funktionscode auf die Verarbeitung eines Ereignisses aufwendet. Die fakturierte Dauer für einen Aufruf ist der Wert von `Duration`, aufgerundet auf die nächste Millisekunde. `Duration` beinhaltet nicht die Kaltstartzeit.
- `PostRuntimeExtensionsDuration` – Die kumulative Zeit, die die Laufzeit nach Abschluss des Funktionscodes mit Erweiterungen verbringt.
- `IteratorAge`: Bei DynamoDB-, Kinesis- und Amazon-DocumentDB-Ereignisquellen das Alter des letzten Datensatzes im Ereignis. Diese Matrik misst die Zeit zwischen dem Zeitpunkt, zu dem ein Stream den Datensatz empfängt, und dem Zeitpunkt, zu dem die Zuordnung von Ereignisquellen das Ereignis an die Funktion sendet.
- `OffsetLag` – Bei selbstverwalteten Apache-Kafka- und Amazon Managed Streaming für Apache Kafka (Amazon MSK)-Ereignisquellen, die Versatzdifferenz zwischen dem letzten Datensatz, der in ein Thema geschrieben wurde, und dem letzten Datensatz, den die Konsumentengruppe Ihrer Funktion verarbeitet hat. Ein Kafka-Thema kann zwar mehrere Partitionen haben, diese Metrik misst die Offset-Verzögerung jedoch auf Themenebene.

`Duration` unterstützt auch Perzentilstatistiken (p). Verwenden Sie Perzentile, um Ausreißerwerte auszuschließen, die `Averages`- und `Maximum`-Statistiken verzerren. Die p95-Statistik zeigt beispielsweise die maximale Dauer von 95 % der Aufrufe, ohne die langsamsten 5 %. Weitere Informationen finden Sie unter Perzentile im CloudWatch Amazon-Benutzerhandbuch.

Gleichzeitigkeitsmetriken

Lambda meldet Gleichzeitigkeitsmetriken als aggregierte Anzahl der Instances, die Ereignisse in einer Funktion, Version, Alias oder AWS-Region verarbeiten. Zeigen Sie diese Metriken mit der Statistik `Max` an, um zu sehen, wie nah Sie an den Grenzwerten für Gleichzeitigkeit sind.

- `ConcurrentExecutions` – Die Anzahl der Funktionsinstances, die Ereignisse verarbeiten. Wenn diese Zahl das Kontingent für gleichzeitige Ausführungen für die Region oder das Limit reservierter Gleichzeitigkeit für die Funktion erreicht, drosselt Lambda weitere Aufrufanforderungen.
- `ProvisionedConcurrentExecutions` – Die Anzahl der Funktions-Instances, die Ereignisse für bereitgestellte Gleichzeitigkeit verarbeiten. Für jeden Aufruf eines Alias oder einer Version mit Provisioned Concurrency gibt Lambda die aktuelle Anzahl aus.
- `ProvisionedConcurrencyUtilization`— Für eine Version oder einen Alias wird der Wert von `ProvisionedConcurrentExecutions` dividiert durch die Gesamtmenge der konfigurierten Parallelität angegeben. Wenn Sie beispielsweise für Ihre Funktion eine bereitgestellte Parallelität von 10 konfigurieren und Ihr Wert 7 `ProvisionedConcurrentExecutions` ist, dann ist Ihr Wert 0,7. `ProvisionedConcurrencyUtilization`
- `UnreservedConcurrentExecutions` – Für eine Region die Anzahl der Ereignisse, die Funktionen ohne reservierte Nebenläufigkeit verarbeiten.
- `ClaimedAccountConcurrency` – Mit Bezug auf eine Region die Menge an Gleichzeitigkeit, die für On-Demand-Aufrufe nicht verfügbar ist. `ClaimedAccountConcurrency` entspricht `UnreservedConcurrentExecutions` plus dem Betrag der zugewiesenen Gleichzeitigkeit (d. h. der gesamten reservierten Gleichzeitigkeit plus der gesamten bereitgestellten Gleichzeitigkeit). Weitere Informationen finden Sie unter Die Metrik `ClaimedAccountConcurrency`.

Metriken asynchroner Aufrufe

Metriken asynchroner Aufrufe liefern Details zu asynchronen Aufrufen aus Ereignisquellen und direkten Aufrufen. Sie können Schwellenwerte und Alarme festlegen, um Sie über bestimmte Änderungen zu informieren. Zum Beispiel, wenn die Anzahl der Ereignisse, die für die Verarbeitung in die Warteschlange gestellt werden, ungewollt ansteigt (`AsyncEventsReceived`). Oder wenn ein Ereignis lange auf seine Verarbeitung gewartet hat (`AsyncEventAge`).

- `AsyncEventsReceived` – Die Anzahl der Ereignisse, die Lambda erfolgreich zur Verarbeitung in die Warteschlange stellt. Diese Metrik bietet einen Einblick in die Anzahl der Ereignisse, die eine Lambda-Funktion empfängt. Überwachen Sie diese Metrik und stellen Sie Alarme für

Schwellenwerte ein, um nach Problemen zu suchen. Zum Beispiel, um eine unerwünschte Anzahl von Ereignissen zu erkennen, die an Lambda gesendet werden, und um schnell Probleme zu diagnostizieren, die auf falsche Auslöser- oder Funktionskonfigurationen zurückzuführen sind. Diskrepanzen zwischen `AsyncEventsReceived` und `Invocations` können auf eine unterschiedliche Verarbeitung, verworfene Ereignisse oder einen möglichen Rückstand in der Warteschlange hinweisen.

- `AsyncEventAge` – Die Zeit zwischen dem erfolgreichen Einstellen des Ereignisses in die Warteschlange durch Lambda und dem Aufruf der Funktion. Der Wert dieser Metrik steigt, wenn Ereignisse aufgrund von Aufruffehlern oder Drosselung erneut versucht werden. Überwachen Sie diese Metrik und legen Sie Alarme für Schwellenwerte für verschiedene Statistiken fest, wenn sich eine Warteschlange immer länger wird. Um einen Anstieg dieser Metrik zu beheben, sehen Sie sich die `Errors`-Metrik an, um Funktionsfehler zu identifizieren, und die `Throttles`-Metrik, um Gleichzeitigkeitsprobleme zu identifizieren.
- `AsyncEventsDropped` – Die Anzahl der Ereignisse, die verworfen werden, ohne die Funktion erfolgreich auszuführen. Wenn Sie eine Warteschlange für unzustellbare Nachrichten oder ein `OnFailure`-Ziel konfigurieren, werden Ereignisse dorthin gesendet, bevor sie gelöscht werden. Ereignisse werden aus verschiedenen Gründen verworfen. Beispielsweise können Ereignisse das maximale Ereignisalter überschreiten oder die maximale Anzahl von Wiederholungsversuchen ausschöpfen, oder die reservierte Gleichzeitigkeit ist möglicherweise auf 0 gesetzt. Um herauszufinden, warum Ereignisse verworfen werden, sehen Sie sich die `Errors`-Metrik an, um Funktionsfehler zu identifizieren, und die `Throttles`-Metrik, um Gleichzeitigkeitsprobleme zu identifizieren.

Verwenden von CloudWatch Amazon-Protokollen mit AWS Lambda

AWS Lambda überwacht Lambda-Funktionen automatisch in Ihrem Namen, um Sie bei der Behebung von Funktionsfehlern zu unterstützen. Solange die Ausführungsrolle Ihrer Funktion über die erforderlichen Berechtigungen verfügt, erfasst Lambda Protokolle für alle Anfragen, die von Ihrer Funktion bearbeitet werden, und sendet sie an Amazon CloudWatch Logs.

Sie können Protokollierungsanweisungen in Ihren Code einfügen, damit Sie überprüfen können, ob Ihr Code wie erwartet funktioniert. Lambda integriert sich automatisch in CloudWatch Logs und sendet alle Logs aus Ihrem Code an eine CloudWatch Loggruppe, die mit einer Lambda-Funktion verknüpft ist.

Standardmäßig sendet Lambda Protokolle an eine Protokollgruppe mit dem Namen `/aws/lambda/<function name>`. Wenn Sie möchten, dass Ihre Funktion Logs an eine andere Gruppe sendet, können Sie dies mit der Lambda-Konsole, der AWS Command Line Interface (AWS CLI) oder der Lambda-API konfigurieren. Weitere Informationen hierzu finden Sie unter the section called “Konfiguration von Protokollgruppen CloudWatch ”.

Sie können Protokolle für Lambda-Funktionen mithilfe der Lambda-Konsole, der CloudWatch Konsole, der AWS Command Line Interface (AWS CLI) oder der CloudWatch API anzeigen.

> **Note**
>
> Es kann 5 bis 10 Minuten dauern, bis Protokolle nach einem Funktionsaufruf angezeigt werden.

Abschnitt

Voraussetzungen

Ihre Ausführungsrolle benötigt die Berechtigung, Protokolle in Logs hochzuladen. CloudWatch Sie können CloudWatch Log-Berechtigungen mithilfe der von Lambda bereitgestellten `AWSLambdaBasicExecutionRole` AWS verwalteten Richtlinie hinzufügen. Führen Sie den folgenden Befehl aus, um diese Richtlinie zu Ihrer Rolle hinzuzufügen:

```
aws iam attach-role-policy --role-name your-role --policy-arn arn:aws:iam::aws:policy/
service-role/AWSLambdaBasicExecutionRole
```

Weitere Informationen finden Sie unter the section called “AWS verwaltete Richtlinien”.

Preisgestaltung

Für die Verwendung von Lambda-Protokollen fallen keine zusätzlichen Gebühren an. Es fallen jedoch die Standardgebühren für CloudWatch Logs an. Weitere Informationen finden Sie unter CloudWatch Preise.

Konfigurieren erweiterter Protokollierungsoptionen für die Lambda-Funktion

Um Ihnen mehr Kontrolle darüber zu geben, wie die Protokolle Ihrer Funktionen erfasst, verarbeitet und verwendet werden, bietet Lambda folgende Konfigurationsoptionen für die Protokollierung:

- Protokollformat – Wählen Sie zwischen Klartext und einem strukturierten JSON-Format für die Protokolle Ihrer Funktion aus.
- Protokollebene — Wählen Sie für strukturierte JSON-Logs die Detailebene der Logs, an die Lambda sendet CloudWatch, wie ERROR, DEBUG oder INFO
- Protokollgruppe — wählen Sie die CloudWatch Protokollgruppe aus, an die Ihre Funktion Logs sendet

Konfiguration der JSON- und Klartext-Protokollformate

Das Erfassen Ihrer Protokollausgaben als JSON-Schlüssel-Wert-Paare erleichtert das Suchen und Filtern beim Debuggen Ihrer Funktionen. Mit Protokollen im JSON-Format können Sie Ihren Protokollen auch Tags und Kontextinformationen hinzufügen. Das kann Ihnen bei der automatisierten Analyse großer Mengen von Protokolldaten helfen. Sofern Ihr Entwicklungsworkflow nicht auf vorhandenen Tools basiert, die Lambda-Protokolle im Klartext verarbeiten, empfehlen wir Ihnen, JSON als Protokollformat auszuwählen.

Für alle von Lambda verwalteten Laufzeiten können Sie wählen, ob die Systemprotokolle Ihrer Funktion im unstrukturierten Klartext- oder CloudWatch JSON-Format an Logs gesendet werden. Systemprotokolle sind die von Lambda generierten Protokolle und werden manchmal auch als Plattformereignisprotokolle bezeichnet.

Wenn Sie für unterstützte Laufzeiten eine der unterstützten integrierten Protokollierungsmethoden verwenden, kann Lambda auch die Anwendungsprotokolle Ihrer Funktion (die Protokolle, die Ihr Funktionscode generiert) im strukturierten JSON-Format ausgeben. Wenn Sie das Protokollformat Ihrer Funktion für diese Laufzeiten konfigurieren, gilt die von Ihnen ausgewählte Konfiguration sowohl für System- als auch für Anwendungsprotokolle.

Wenn Ihre Funktion für unterstützte Laufzeiten eine unterstützte Protokollierungsbibliothek oder -methode verwendet, müssen Sie keine Änderungen an Ihrem vorhandenen Code vornehmen, damit Lambda Protokolle in strukturiertem JSON erfasst.

> **Note**
>
> Durch die Verwendung der JSON-Protokollformatierung werden zusätzliche Metadaten hinzugefügt und Protokollmeldungen als JSON-Objekte kodiert, die eine Reihe von Schlüssel-Wert-Paaren enthalten. Aus diesem Grund kann die Größe der Protokollmeldungen Ihrer Funktion zunehmen.

Unterstützte Laufzeiten und Protokollierungsmethoden

Lambda unterstützt derzeit die Option, strukturierte JSON-Anwendungsprotokolle für folgende Laufzeiten auszugeben.

Laufzeit	Unterstützte Versionen
Java	Alle Java-Laufzeiten außer Java 8 auf Amazon Linux 1
Node.js	Node.js 16 und höher
Python	Python 3.7 oder höher

Damit Lambda die Anwendungsprotokolle Ihrer Funktion CloudWatch im strukturierten JSON-Format senden kann, muss Ihre Funktion die folgenden integrierten Protokollierungstools zur Ausgabe von Protokollen verwenden:

- Java – der `LambdaLogger`-Logger oder Log4j2.
- Node.js – die Konsolenmethoden `console.trace`, `console.debug`, `console.log`, `console.info`, `console.error` und `console.warn`
- Python – die `logging`-Standard-Python-Bibliothek

Weitere Hinweise zur Verwendung erweiterter Protokollierungsoptionen mit unterstützten Laufzeiten finden Sie unter the section called “Protokollierung”, the section called “Protokollierung” und the section called “Protokollierung”.

Für andere verwaltete Lambda-Laufzeiten unterstützt Lambda derzeit nur nativ die Erfassung von Systemprotokollen im strukturierten JSON-Format. Sie können jedoch weiterhin zu jeder Laufzeit Anwendungsprotokolle im strukturierten JSON-Format erfassen, indem Sie Protokollierungstools wie Powertools für AWS Lambda die Ausgabe von Protokollausgaben im JSON-Format verwenden.

Standardprotokollformate

Derzeit ist das Standard-Protokollformat für alle Lambda-Laufzeiten das Klartextformat.

Wenn Sie bereits Logging-Bibliotheken wie Powertools verwenden, AWS Lambda um Ihre Funktionsprotokolle im strukturierten JSON-Format zu generieren, müssen Sie Ihren Code nicht ändern, wenn Sie die JSON-Protokollformatierung auswählen. Lambda codiert Protokolle, die bereits JSON-codiert sind, nicht doppelt, sodass die Anwendungsprotokolle Ihrer Funktion weiterhin wie zuvor erfasst werden.

JSON-Format für Systemprotokolle

Wenn Sie das Protokollformat Ihrer Funktion als JSON konfigurieren, wird jedes Systemprotokollelement (Plattformereignis) als JSON-Objekt erfasst, das Schlüssel-Wert-Paare mit den folgenden Schlüsseln enthält:

- `"time"` – die Uhrzeit, zu der die Protokollmeldung generiert wurde
- `"type"` – die Art des Ereignisses, das protokolliert wird
- `"record"` – der Inhalt der Protokollausgabe

Das Format des `"record"`-Werts hängt von der Art des protokollierten Ereignisses ab. Weitere Informationen finden Sie unter the section called “Telemetrie-API `Event`-Objekttypen”. Weitere Hinweise zu den Protokollebenen, die Systemprotokollereignissen zugewiesen sind, finden Sie unter the section called “Zuordnung von Ereignissen auf Systemprotokollebene”.

Zum Vergleich zeigen die folgenden beiden Beispiele dieselbe Protokollausgabe sowohl im Klartext- als auch im strukturierten JSON-Format. Beachten Sie, dass Systemprotokollereignisse in den meisten Fällen mehr Informationen enthalten, wenn sie im JSON-Format ausgegeben werden, als wenn sie im Klartext ausgegeben werden.

Example Klartext:

```
2023-03-13 18:56:24.046000 fbe8c1   INIT_START  Runtime Version:
 python:3.9.v18  Runtime Version ARN: arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0
```

Example strukturiertes JSON:

```
{
  "time": "2023-03-13T18:56:24.046Z",
  "type": "platform.initStart",
  "record": {
    "initializationType": "on-demand",
    "phase": "init",
    "runtimeVersion": "python:3.9.v18",
    "runtimeVersionArn": "arn:aws:lambda:eu-
west-1::runtime:edb5a058bfa782cb9cedc6d534ac8b8c193bc28e9a9879d9f5ebaaf619cd0fc0"
  }
}
```

> **Note**
>
> Die the section called “Telemetrie-API” gibt immer Plattformereignisse wie `START` und `REPORT` im JSON-Format aus. Die Konfiguration des Formats der Systemprotokolle, an die Lambda sendet, CloudWatch hat keinen Einfluss auf das Verhalten der Lambda-Telemetrie-API.

JSON-Format für Anwendungsprotokolle

Wenn Sie das Protokollformat Ihrer Funktion als JSON konfigurieren, werden Anwendungsprotokollausgaben, die mit unterstützten Protokollierungsbibliotheken und -methoden geschrieben wurden, als JSON-Objekt erfasst, das Schlüssel-Wert-Paare mit folgenden Schlüsseln enthält.

- `"timestamp"` – die Uhrzeit, zu der die Protokollmeldung generiert wurde
- `"level"` – die der Meldung zugewiesene Protokollebene
- `"message"` – der Inhalt der Protokollmeldung
- `"requestId"` (Python und Node.js) oder `"AWSrequestId"` (Java) – die eindeutige Anforderungs-ID für den Funktionsaufruf

Abhängig von der Laufzeit und der Protokollierungsmethode, die Ihre Funktion verwendet, kann dieses JSON-Objekt auch zusätzliche Schlüsselpaare enthalten. Wenn Sie Node.js verwenden und Ihre Funktion beispielsweise `console`-Methoden nutzt, um Fehlerobjekte mit mehreren Argumenten zu protokollieren, enthält das JSON-Objekt zusätzliche Schlüssel-Wert-Paare mit den Schlüsseln `errorMessage`, `errorType` und `stackTrace`. Weitere Informationen zu JSON-formatierten Protokollen in verschiedenen Lambda-Laufzeiten finden Sie unter the section called “Protokollierung”, the section called “Protokollierung” und the section called “Protokollierung”.

> **Note**
>
> Der Schlüssel, den Lambda für den Zeitstempelwert verwendet, unterscheidet sich für Systemprotokolle und für Anwendungsprotokolle. Bei Systemprotokollen verwendet Lambda den Schlüssel `"time"`, um die Konsistenz mit der Telemetrie-API aufrechtzuerhalten. Bei Anwendungsprotokollen folgt Lambda den Konventionen der unterstützten Laufzeiten und verwendet `"timestamp"`.

Zum Vergleich zeigen die folgenden beiden Beispiele dieselbe Protokollausgabe sowohl im Klartext- als auch im strukturierten JSON-Format.

Example Klartext:

```
2023-10-27T19:17:45.586Z 79b4f56e-95b1-4643-9700-2807f4e68189 INFO some log message
```

Example strukturiertes JSON:

```
{
    "timestamp":"2023-10-27T19:17:45.586Z",
    "level":"INFO",
    "message":"some log message",
    "requestId":"79b4f56e-95b1-4643-9700-2807f4e68189"
}
```

Festlegen des Protokollformats Ihrer Funktion

Um das Protokollformat für Ihre Funktion zu konfigurieren, können Sie die Lambda-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Sie können das Protokollformat einer Funktion auch mithilfe der API-Befehle CreateFunctionund UpdateFunctionConfiguration Lambda, der AWS::Serverless::FunctionRessource AWS Serverless Application Model (AWS SAM) und der AWS CloudFormation AWS::Lambda::FunctionRessource konfigurieren.

Das Ändern des Protokollformats Ihrer Funktion hat keine Auswirkungen auf bestehende Protokolle, die in CloudWatch Logs gespeichert sind. Nur neue Protokolle verwenden das aktualisierte Format.

Wenn Sie das Protokollformat Ihrer Funktion in JSON ändern und keine Protokollebene festlegen, setzt Lambda die Anwendungsprotokollebene und die Systemprotokollebene Ihrer Funktion automatisch auf INFO. Das bedeutet, dass Lambda nur Protokollausgaben der Stufe INFO und niedriger an CloudWatch Logs sendet. Weitere Informationen zur Filterung auf Anwendungs- und Systemprotokollebene finden Sie unter the section called “Filterung auf Protokollebene”

> **Note**
>
> Wenn das Protokollformat Ihrer Funktion auf Klartext gesetzt ist, ist die Standardeinstellung auf Protokollebene für Python-Laufzeiten WARN. Das bedeutet, dass Lambda nur Protokollausgaben der Stufe WARN und niedriger an CloudWatch Logs sendet. Wenn Sie das Protokollformat Ihrer Funktion in JSON ändern, ändert sich dieses Standardverhalten. Weitere Informationen zur Protokollierung in Python finden Sie unter the section called “Protokollierung”.

Bei Funktionen von Node.js, die EMF-Logs (Embedded Metric Format) ausgeben, kann die Änderung des Protokollformats Ihrer Funktion in JSON dazu führen, dass Ihre Metriken nicht erkannt CloudWatch werden können.

> **Important**
>
> Wenn Ihre Funktion Powertools for AWS Lambda (TypeScript) oder die Open-Source-EMF-Clientbibliotheken zur Ausgabe von EMF-Protokollen verwendet, aktualisieren Sie Ihre Powertools - und EMF-Bibliotheken auf die neuesten Versionen, um sicherzustellen, dass Ihre Protokolle weiterhin korrekt analysiert CloudWatch werden können. Wenn Sie zum JSON-Protokollformat wechseln, empfehlen wir Ihnen zudem, Tests durchzuführen, um die Kompatibilität mit den eingebetteten Metriken Ihrer Funktion sicherzustellen. Weitere Hinweise zu den Funktionen von node.js, die EMF-Protokolle ausgeben, finden Sie unter the section called “Verwenden von Clientbibliotheken im Embedded Metric Format (EMF) mit strukturierten JSON-Protokollen”.

So konfigurieren Sie das Protokollformat einer Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Auswählen einer Funktion
3. Wählen Sie auf der Konfigurationsseite der Funktion die Option Überwachungs- und Betriebstools aus.
4. Wählen Sie im Bereich Protokollierungskonfiguration die Option Bearbeiten aus.
5. Wählen Sie unter Protokollinhalt für Protokollformat entweder Text oder JSON aus.
6. Wählen Sie Speichern.

So ändern Sie das Protokollformat einer vorhandenen Funktion (AWS CLI)

- Verwenden Sie den Befehl `update-function-configuration`, um das Protokollformat einer vorhandenen Funktion zu ändern. Legen Sie die `LogFormat`-Option in `LoggingConfig` entweder auf `JSON` oder `Text` fest.

```
aws lambda update-function-configuration \
--function-name myFunction --logging-config LogFormat=JSON
```

So legen Sie das Protokollformat fest, wenn Sie eine Funktion erstellen (AWS CLI)

- Verwenden Sie die Option `--logging-config` im Befehl `create-function`, um das Protokollformat zu konfigurieren, wenn Sie eine neue Funktion erstellen. Legen Sie `LogFormat`

auf `JSON` oder `Text` fest. Mit dem folgenden Beispielbefehl wird mithilfe der Laufzeit Node.js 18 eine Funktion erstellt, die Protokolle in strukturiertem JSON ausgibt.

Wenn Sie beim Erstellen einer Funktion kein Protokollformat angeben, verwendet Lambda das Standardprotokollformat für die von Ihnen ausgewählte Laufzeitversion. Informationen zu den Standard-Protokollierungsformaten finden Sie unter the section called “Standardprotokollformate”.

```
aws lambda create-function --function-name myFunction --runtime nodejs18.x \
--handler index.handler --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/LambdaRole --logging-config LogFormat=JSON
```

Filterung auf Protokollebene

Lambda kann die Protokolle Ihrer Funktion filtern, sodass nur Protokolle mit einer bestimmten Detailebene oder niedriger an CloudWatch Logs gesendet werden. Sie können die Filterung auf Protokollebene separat für die Systemprotokolle Ihrer Funktion (die von Lambda generierten Protokolle) und Anwendungsprotokolle (die von Ihrem Funktionscode generierten Protokolle) konfigurieren.

Für the section called “Unterstützte Laufzeiten und Protokollierungsmethoden” müssen Sie keine Änderungen an Ihrem Funktionscode vornehmen, damit Lambda die Anwendungsprotokolle Ihrer Funktion filtert.

Für alle anderen Laufzeiten und Protokollierungsmethoden muss Ihr Funktionscode Protokollereignisse in `stdout` oder `stderr` als JSON-formatierte Objekte ausgeben, die ein Schlüssel-Wert-Paar mit dem Schlüssel `"level"` enthalten. Lambda interpretiert beispielsweise die folgende Ausgabe an `stdout` als ein Protokoll auf Ebene DEBUG.

```
print('{"level": "debug", "msg": "my debug log", "timestamp":
 "2023-11-02T16:51:31.587199Z"}')
```

Wenn das Feld für den `"level"`-Wert ungültig ist oder fehlt, weist Lambda der Protokollausgabe die Ebene INFO zu. Damit Lambda das Zeitstempelfeld verwenden kann, müssen Sie die Zeit im gültigen RFC 3339-Zeitstempelformat angeben. Wenn Sie keinen gültigen Zeitstempel angeben, weist Lambda dem Protokoll die Ebene INFO zu und fügt einen Zeitstempel für Sie hinzu.

Halten Sie sich bei der Benennung des Zeitstempelschlüssels an die Benennungskonventionen der Laufzeit, die Sie verwenden. Lambda unterstützt die meisten gängigen Namenskonventionen, die

von den verwalteten Laufzeiten verwendet werden. In Funktionen, die die .NET-Laufzeit verwenden, erkennt Lambda beispielsweise den Schlüssel `"Timestamp"`.

> **Note**
>
> Um die Filterung auf Protokollebene verwenden zu können, muss Ihre Funktion für die Verwendung des JSON-Protokollformats konfiguriert sein. Derzeit ist das Standard-Protokollformat für alle verwalteten Lambda-Laufzeiten das Klartextformat. Informationen zur Konfiguration des JASON-Protokollformats Ihrer Funktion finden Sie unter the section called “Festlegen des Protokollformats Ihrer Funktion”.

Bei Anwendungsprotokollen (den durch Ihren Funktionscode generierten Protokollen) können Sie zwischen den folgenden Protokollebenen wählen.

Protokollebene	Standardnutzung
TRACE (am detailliertesten)	Die detailliertesten Informationen, die verwendet werden, um den Ausführungspfad Ihres Codes nachzuverfolgen
DEBUG	Detaillierte Informationen für das System-De bugging
INFO	Meldungen, die den normalen Betrieb Ihrer Funktion erfassen
WARN	Meldungen über mögliche Fehler, die zu unerwartetem Verhalten führen können, wenn sie nicht behoben werden
ERROR	Meldungen über Probleme, die verhindern, dass der Code wie erwartet funktioniert
FATAL (am wenigsten Details)	Meldungen über schwerwiegende Fehler, die dazu führen, dass die Anwendung nicht mehr funktioniert

Wenn Sie eine Protokollebene auswählen, sendet Lambda Protokolle auf dieser Ebene und niedriger an CloudWatch Logs. Wenn Sie beispielsweise die Anwendungsprotokollebene einer Funktion auf WARN setzen, sendet Lambda keine Protokollausgaben auf den Protokollebenen INFO und DEBUG. Die Standardebene des Anwendungsprotokolls für die Protokollfilterung ist INFO.

Wenn Lambda die Anwendungsprotokolle Ihrer Funktion filtert, wird Protokollmeldungen ohne Ebene die Protokollebene INFO zugewiesen.

Für Systemprotokolle (die vom Lambda-Service generierten Protokolle) können Sie zwischen den folgenden Protokollebenen wählen.

Protokollebene	Verwendung
DEBUG (am detailliertesten)	Detaillierte Informationen für das System-De bugging
INFO	Meldungen, die den normalen Betrieb Ihrer Funktion erfassen
WARN (am wenigsten Details)	Meldungen über mögliche Fehler, die zu unerwartetem Verhalten führen können, wenn sie nicht behoben werden

Wenn Sie eine Protokollebene auswählen, sendet Lambda Protokolle auf dieser Ebene und niedriger. Wenn Sie beispielsweise die Protokollebene einer Funktion auf INFO setzen, sendet Lambda keine Protokollausgaben auf der Protokollebene DEBUG.

Standardmäßig setzt Lambda die Protokollebene des Systems auf INFO. Mit dieser Einstellung sendet `"start"` und `"report"` protokolliert Lambda automatisch Nachrichten an CloudWatch. Um mehr oder weniger detaillierte Systemprotokolle zu erhalten, ändern Sie die Protokollebene in DEBUG oder WARN. Eine Liste der Protokollebenen, denen Lambda verschiedene Systemprotokollereignisse zuordnet, finden Sie unter the section called “Zuordnung von Ereignissen auf Systemprotokollebene”.

Konfigurieren der Filterung auf Protokollebene

Um die Filterung auf Anwendungs- und Systemprotokollebene für Ihre Funktion zu konfigurieren, können Sie die Lambda-Konsole oder die AWS Command Line Interface () verwenden.AWS CLI

Sie können die Protokollebene einer Funktion auch mithilfe der API-Befehle CreateFunctionund UpdateFunctionConfiguration Lambda, der AWS::Serverless::FunctionRessource AWS Serverless Application Model (AWS SAM) und der AWS CloudFormation AWS::Lambda::FunctionRessource konfigurieren.

Beachten Sie, dass, wenn Sie die Protokollebene Ihrer Funktion in Ihrem Code festlegen, diese Einstellung Vorrang vor allen anderen von Ihnen konfigurierten Einstellungen auf Protokollebene hat. Wenn Sie beispielsweise die Python-Methode `logging setLevel()` verwenden, um die Protokollierungsebene Ihrer Funktion auf INFO zu setzen, hat diese Einstellung Vorrang vor der Einstellung WARN, die Sie mit der Lambda-Konsole konfigurieren.

So konfigurieren Sie die Anwendungs- oder Systemprotokollebene (Konsole) einer vorhandenen Funktion

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie auf der Konfigurationsseite der Funktion die Option Überwachungs- und Betriebstools aus.
4. Wählen Sie im Bereich Protokollierungskonfiguration die Option Bearbeiten aus.
5. Stellen Sie sicher, dass unter Protokollinhalt für Protokollformat JSON ausgewählt ist.
6. Wählen Sie mit den Optionsfeldern die gewünschte Anwendungsprotokollebene und die gewünschte Systemprotokollebene für Ihre Funktion aus.
7. Wählen Sie Speichern.

So konfigurieren Sie die Anwendungs- oder Systemprotokollebene einer vorhandenen Funktion (AWS CLI)

- Verwenden Sie den Befehl `update-function-configuration`, um die Anwendungs- oder Systemprotokollebene einer vorhandenen Funktion zu ändern. Legen Sie `--system-log-level` auf `DEBUG`, `INFO` oder `WARN` fest. Legen Sie `--application-log-level` auf `DEBUG`, `INFO`, `WARN`, `ERROR` oder `FATAL` fest.

```
aws lambda update-function-configuration \
--function-name myFunction --system-log-level WARN \
--application-log-level ERROR
```

So konfigurieren Sie die Filterung auf Protokollebene beim Erstellen einer Funktion

- Um die Filterung auf Protokollebene zu konfigurieren, wenn Sie eine neue Funktion erstellen, verwenden Sie die Optionen `--system-log-level` und `--application-log-level` im Befehl „create-function“. Legen Sie `--system-log-level` auf `DEBUG`, `INFO` oder `WARN` fest. Legen Sie `--application-log-level` auf `DEBUG`, `INFO`, `WARN`, `WARN` oder `FATAL` fest.

```
aws lambda create-function --function-name myFunction --runtime nodejs18.x \
--handler index.handler --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/LambdaRole --system-log-level WARN \
--application-log-level ERROR
```

Zuordnung von Ereignissen auf Systemprotokollebene

Für von Lambda generierte Protokollereignisse auf Systemebene ist in der folgenden Tabelle die Protokollebene definiert, die jedem Ereignis zugewiesen ist. Weitere Informationen zu den in der Tabelle aufgeführten Ereignissen finden Sie unter the section called “Referenz zum `Event`-Schema”

Ereignisname	Bedingung	Zugewiesene Protokollebene
initStart	„runtimeVersion“ ist festgelegt	INFO
initStart	„runtimeVersion“ ist nicht festgelegt	DEBUG
init RuntimeDone	status=success	DEBUG
init RuntimeDone	status!=success	WARN
initReport	initializationType=snapstart	INFO
initReport	initializationType!=snapstart	DEBUG
initReport	status!=success	WARN
restoreStart	„runtimeVersion“ ist festgelegt	INFO
restoreStart	„runtimeVersion“ ist nicht festgelegt	DEBUG

Ereignisname	Bedingung	Zugewiesene Protokollebene
wiederherstellen RuntimeDone	status=success	DEBUG
wiederherstellen RuntimeDone	status!=success	WARN
restoreReport	status=success	INFO
restoreReport	status!=success	WARN
start	-	INFO
runtimeDone	status=success	DEBUG
runtimeDone	status!=success	WARN
report	status=success	INFO
report	status!=success	WARN
extension	state=success	INFO
extension	state!=success	WARN
logSubscription	-	INFO
telemetrySubscription	-	INFO
logsDropped	-	WARN

> **Note**
>
> Die the section called “Telemetrie-API” gibt immer den vollständigen Satz von Plattformereignissen aus. Die Konfiguration der Ebene der Systemprotokolle, an die Lambda sendet, CloudWatch hat keinen Einfluss auf das Verhalten der Lambda-Telemetrie-API.

Filterung auf Anwendungsprotokollebene mit benutzerdefinierten Laufzeiten

Wenn Sie die Filterung auf Anwendungsprotokollebene für Ihre Funktion konfigurieren, legt Lambda hinter den Kulissen die Anwendungsprotokollebene in der Laufzeit mithilfe der Umgebungsvariable `AWS_LAMBDA_LOG_LEVEL` fest. Lambda legt auch das Protokollformat Ihrer Funktion mithilfe der Umgebungsvariable `AWS_LAMBDA_LOG_FORMAT` fest. Sie können diese Variablen verwenden, um erweiterte Lambda-Protokollierungsoptionen in eine benutzerdefinierte Laufzeit zu integrieren.

Um Protokollierungseinstellungen für eine Funktion konfigurieren zu können, die eine benutzerdefinierte Laufzeit mit der Lambda-Konsole und Lambda-APIs verwendet, konfigurieren Sie Ihre benutzerdefinierte Laufzeit so, dass sie den Wert dieser Umgebungsvariablen überprüft. AWS CLI Anschließend können Sie die Logger Ihrer Laufzeit gemäß dem von Ihnen ausgewählten Protokollformat und den von Ihnen ausgewählten Protokollebenen konfigurieren.

Konfiguration von Protokollgruppen CloudWatch

Standardmäßig wird CloudWatch automatisch eine nach Ihrer Funktion benannte Protokollgruppe erstellt, wenn diese `/aws/lambda/<function name>` zum ersten Mal aufgerufen wird. Um Ihre Funktion so zu konfigurieren, dass Protokolle an eine bestehende Protokollgruppe gesendet werden, oder um eine neue Protokollgruppe für Ihre Funktion zu erstellen, können Sie die Lambda-Konsole oder die AWS CLI verwenden. Sie können benutzerdefinierte Protokollgruppen auch mithilfe der Befehle CreateFunctionund UpdateFunctionConfiguration Lambda API und der Ressource AWS Serverless Application Model (AWS SAM) AWS: :Serverless: :Function konfigurieren.

Sie können mehrere Lambda-Funktionen so konfigurieren, dass sie Protokolle an dieselbe CloudWatch Protokollgruppe senden. Beispielsweise könnten Sie eine einzelne Protokollgruppe verwenden, um Protokolle für alle Lambda-Funktionen zu speichern, aus denen eine bestimmte Anwendung besteht. Wenn Sie eine benutzerdefinierte Protokollgruppe für eine Lambda-Funktion verwenden, enthalten die von Lambda erstellten Protokollstreams den Funktionsnamen und die Funktionsversion. Dadurch wird sichergestellt, dass die Zuordnung zwischen Protokollmeldungen und Funktionen erhalten bleibt, auch wenn Sie dieselbe Protokollgruppe für mehrere Funktionen verwenden.

Das Log-Stream-Benennungsformat für benutzerdefinierte Protokollgruppen folgt dieser Konvention:

```
YYYY/MM/DD/<function_name>[<function_version>][<execution_environment_GUID>]
```

Beachten Sie, dass bei der Konfiguration einer benutzerdefinierten Protokollgruppe der Name, den Sie für Ihre Protokollgruppe auswählen, den Benennungsregeln für CloudWatch Protokolle

entsprechen muss. Darüber hinaus dürfen benutzerdefinierte Protokollgruppennamen nicht mit der Zeichenfolge `aws/` beginnen. Wenn Sie eine benutzerdefinierte Protokollgruppe erstellen, die mit `aws/` beginnt, kann Lambda die Protokollgruppe nicht erstellen. Aus diesem Grund werden die Protokolle Ihrer Funktion nicht an gesendet CloudWatch.

So ändern Sie die Protokollgruppe einer Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie auf der Konfigurationsseite der Funktion die Option Überwachungs- und Betriebstools aus.
4. Wählen Sie im Bereich Protokollierungskonfiguration die Option Bearbeiten aus.
5. Wählen Sie im Bereich Protokollgruppe für CloudWatch Protokollgruppe die Option Benutzerdefiniert aus.
6. Geben Sie unter Benutzerdefinierte Protokollgruppe den Namen der CloudWatch Protokollgruppe ein, an die Ihre Funktion Protokolle senden soll. Wenn Sie den Namen einer vorhandenen Protokollgruppe eingeben, verwendet Ihre Funktion diese Gruppe. Wenn keine Protokollgruppe mit dem von Ihnen eingegebenen Namen existiert, erstellt Lambda eine neue Protokollgruppe für Ihre Funktion mit diesem Namen.

So ändern Sie die Protokollgruppe einer Funktion (AWS CLI)

- Verwenden Sie den Befehl `update-function-configuration`, um die Protokollgruppe einer vorhandenen Funktion zu ändern. Wenn Sie den Namen einer vorhandenen Protokollgruppe angeben, verwendet Ihre Funktion diese Gruppe. Wenn keine Protokollgruppe mit dem von Ihnen angegebenen Namen existiert, erstellt Lambda eine neue Protokollgruppe für Ihre Funktion mit diesem Namen.

```
aws lambda update-function-configuration \
--function-name myFunction --log-group myLogGroup
```

So geben Sie eine benutzerdefinierte Protokollgruppe an, wenn Sie eine Funktion erstellen (AWS CLI)

- Um eine benutzerdefinierte Protokollgruppe anzugeben, wenn Sie eine neue Lambda-Funktion mit dem erstellen AWS CLI, verwenden Sie die `--log-group` Option. Wenn Sie den Namen

einer vorhandenen Protokollgruppe angeben, verwendet Ihre Funktion diese Gruppe. Wenn keine Protokollgruppe mit dem von Ihnen angegebenen Namen existiert, erstellt Lambda eine neue Protokollgruppe für Ihre Funktion mit diesem Namen.

Mit dem folgenden Beispielbefehl wird eine Node.js-Lambda-Funktion erstellt, die Protokolle an eine Protokollgruppe mit dem Namen `myLogGroup` sendet.

```
aws lambda create-function --function-name myFunction --runtime nodejs18.x \
--handler index.handler --zip-file fileb://function.zip \
--role arn:aws:iam::123456789012:role/LambdaRole --log-group myLogGroup
```

Berechtigungen für die Ausführungsrolle

Damit Ihre Funktion Protokolle an Logs senden kann CloudWatch , muss sie über die `logs:PutLogEvents`entsprechende Berechtigung verfügen. Wenn Sie die Protokollgruppe Ihrer Funktion mithilfe der Lambda-Konsole konfigurieren und Ihre Funktion diese Berechtigung nicht besitzt, fügt Lambda sie standardmäßig der Ausführungsrolle der Funktion hinzu. Wenn Lambda diese Berechtigung hinzufügt, erteilt es der Funktion die Erlaubnis, Protokolle an jede CloudWatch Logs-Protokollgruppe zu senden.

Um zu verhindern, dass Lambda die Ausführungsrolle der Funktion automatisch aktualisiert, damit Sie diese stattdessen manuell bearbeiten, erweitern Sie Berechtigungen und deaktivieren Sie Erforderliche Berechtigungen hinzufügen.

Wenn Sie die Protokollgruppe Ihrer Funktion mithilfe von konfigurieren AWS CLI, fügt Lambda die `logs:PutLogEvents` Berechtigung nicht automatisch hinzu. Fügen Sie die Berechtigung zur Ausführungsrolle Ihrer Funktion hinzu, falls noch nicht geschehen. Diese Berechtigung ist in der AWSLambdaBasicExecutionRoleverwalteten Richtlinie enthalten.

Zugreifen auf Protokolle mit der Lambda-Konsole

Die Protokolle mithilfe der Lambda-Konsole anzeigen

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Überwachen aus.
4. Wählen Sie „Anmeldungen anzeigen CloudWatch“.

Zugreifen auf Protokolle mit dem AWS CLI

Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. Zur Durchführung der Schritte in diesem Abschnitt benötigen Sie Folgendes:

- AWS Command Line Interface (AWS CLI) Version 2
- AWS CLI — Schnelle Konfiguration mit `aws configure`

Sie können die AWS CLI verwenden, um Protokolle für einen Aufruf mit der `--log-type`-Befehlsoption abzurufen. Die Antwort enthält das Feld `LogResult`, das bis zu 4 KB base64-verschlüsselte Protokolle aus dem Aufruf enthält.

Example eine Log-ID abrufen

Das folgende Beispiel zeigt, wie eine Protokoll-ID aus dem `LogResult`-Feld für eine Funktion namens `my-function` abgerufen wird.

```
aws lambda invoke --function-name my-function out --log-type Tail
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "LogResult":
 "U1RBUlQgUmVxdWVzdElkOiA4N2QwNDRiOC1mMTU0LTExZTgtOGNkYS0yOTc0YzVlNGZiMjEgVmVyc2lvb...",
    "ExecutedVersion": "$LATEST"
}
```

Example entschlüsseln der Protokolle

Verwenden Sie in derselben Eingabeaufforderung das `base64`-Dienstprogramm, um die Protokolle zu entschlüsseln. Das folgende Beispiel zeigt, wie Base64-codierte Logs für abgerufen werde `my-function`.

```
aws lambda invoke --function-name my-function out --log-type Tail \
--query 'LogResult' --output text --cli-binary-format raw-in-base64-out | base64 --
decode
```

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Die Ausgabe sollte folgendermaßen aussehen:

```
START RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8 Version: $LATEST
"AWS_SESSION_TOKEN": "AgoJb3JpZ2luX2VjELj...", "_X_AMZN_TRACE_ID": "Root=1-5d02e5ca-
f5792818b6fe8368e5b51d50;Parent=191db58857df8395;Sampled=0"",ask/lib:/opt/lib",
END RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8
REPORT RequestId: 57f231fb-1730-4395-85cb-4f71bd2b87b8  Duration: 79.67 ms      Billed
 Duration: 80 ms         Memory Size: 128 MB     Max Memory Used: 73 MB
```

Das `base64`-Dienstprogramm ist unter Linux, macOS und Ubuntu auf Windowsverfügbar. macOS-Benutzer müssen möglicherweise `base64 -D` verwenden.

Example get-logs.sh-Skript

Verwenden Sie in derselben Eingabeaufforderung das folgende Skript, um die letzten fünf Protokollereignisse herunterzuladen. Das Skript verwendet `sed` zum Entfernen von Anführungszeichen aus der Ausgabedatei und wechselt 15 Sekunden lang in den Ruhezustand, um Zeit einzuräumen, damit Protokolle verfügbar werden können. Die Ausgabe enthält die Antwort von Lambda und die `get-log-events`Ausgabe des Befehls.

Kopieren Sie den Inhalt des folgenden Codebeispiels und speichern Sie es in Ihrem Lambda-Projektverzeichnis unter `get-logs.sh`.

Die cli-binary-format Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Um dies zur Standardeinstellung zu machen, führen Sie `aws configure set cli-binary-format raw-in-base64-out` aus. Weitere Informationen finden Sie unter Von AWS CLI unterstützte globale Befehlszeilenoptionen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

```
#!/bin/bash
aws lambda invoke --function-name my-function --cli-binary-format raw-in-base64-out --
payload '{"key": "value"}' out
sed -i'' -e 's/"//g' out
sleep 15
aws logs get-log-events --log-group-name /aws/lambda/my-function --log-stream-
name stream1 --limit 5
```

Example macOS und Linux (nur diese Systeme)

In derselben Eingabeaufforderung müssen macOS- und Linux-Benutzer möglicherweise den folgenden Befehl ausführen, um sicherzustellen, dass das Skript ausführbar ist.

```
chmod -R 755 get-logs.sh
```

Example die letzten fünf Protokollereignisse abrufen

Führen Sie an derselben Eingabeaufforderung das folgende Skript aus, um die letzten fünf Protokollereignisse abzurufen.

```
./get-logs.sh
```

Die Ausgabe sollte folgendermaßen aussehen:

```
{
    "StatusCode": 200,
    "ExecutedVersion": "$LATEST"
}
{
    "events": [
        {
            "timestamp": 1559763003171,
            "message": "START RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf Version:
 $LATEST\n",
            "ingestionTime": 1559763003309
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tENVIRONMENT VARIABLES\r{\r  \"AWS_LAMBDA_FUNCTION_VERSION\": \"$LATEST\",
\r ...",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003173,
            "message": "2019-06-05T19:30:03.173Z\t4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tINFO\tEVENT\r{\r  \"key\": \"value\"\r}\n",
            "ingestionTime": 1559763018353
        },
        {
```

```
            "timestamp": 1559763003218,
            "message": "END RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf\n",
            "ingestionTime": 1559763018353
        },
        {
            "timestamp": 1559763003218,
            "message": "REPORT RequestId: 4ce9340a-b765-490f-ad8a-02ab3415e2bf
\tDuration: 26.73 ms\tBilled Duration: 27 ms \tMemory Size: 128 MB\tMax Memory Used: 75
 MB\t\n",
            "ingestionTime": 1559763018353
        }
    ],
    "nextForwardToken": "f/34783877304859518393868359594929986069206639495374241795",
    "nextBackwardToken": "b/34783877303811383369537420289090800615709599058929582080"
}
```


Protokollierung von Laufzeitfunktionen

Um zu debuggen und zu validieren, dass Ihr Code wie erwartet funktioniert, können Sie Protokolle mit der Standardprotokollfunktionalität für Ihre Programmiersprache ausgeben. Die Lambda-Laufzeit lädt die Protokollausgabe Ihrer Funktion in Logs hoch. CloudWatch Sprachenspezifische Anweisungen finden Sie in den folgenden Themen:

- AWS Lambda Funktionsprotokollierung in Node.js
- AWS Lambda Funktionsprotokollierung in Python
- AWS Lambda Funktionsprotokollierung in Ruby
- AWS Lambda Funktionsprotokollierung in Java
- AWS Lambda Funktion protokollieren in Go
- Lambda-Funktionsprotokollierung in C#
- AWS Lambda Funktion einloggen PowerShell

Als nächstes

- Weitere Informationen zu Protokollgruppen und dem Zugriff auf diese Gruppen über die CloudWatch Konsole finden Sie unter Überwachungssystem, Anwendung und benutzerdefinierte Protokolldateien im CloudWatch Amazon-Benutzerhandbuch.

Protokollieren von AWS Lambda API-Aufrufen mit AWS CloudTrail

AWS Lambda ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst API-Aufrufe für Lambda als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe über die Lambda-Konsole und Codeaufrufe der Lambda-API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Lambda gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde, und weitere Details ermitteln.

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 Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Ob die Anfrage im Namen eines IAM Identity Center-Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Ereignisverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

> Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können einen Pfad mit einer oder mehreren Regionen erstellen, indem Sie den verwenden. AWS CLI Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten in Ihrem Konto AWS-Regionen erfassen. Wenn du einen Trail mit nur einer Region erstellst, kannst du dir nur die Ereignisse ansehen, die in den Trails protokolliert wurden. AWS-Region Weitere Informationen zu Trails finden Sie unter Einen Trail für Sie erstellen AWS-Konto und Einen Trail für eine Organisation erstellen im AWS CloudTrail Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3-Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail AWS CloudTrail Preisgestaltung.

Lambda-Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. Lesen oder Schreiben in ein Amazon-S3-Objekt). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Standardmäßig werden die meisten Datenereignisse CloudTrail nicht protokolliert, und der CloudTrail Ereignisverlauf zeichnet sie auch nicht auf.

Ein CloudTrail Datenereignis, das standardmäßig für unterstützte Dienste protokolliert wird, ist`LambdaESMDisabled`. Weitere Informationen zur Verwendung dieses Ereignisses zur Behebung von Problemen mit Lambda-Ereignisquellenzuordnungen finden Sie unter. the section called “Wird CloudTrail zur Fehlerbehebung bei deaktivierten Lambda-Ereignisquellen verwendet”

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur Preisgestaltung finden Sie unter CloudTrail Preise.AWS CloudTrail

Sie können Datenereignisse für den `AWS::Lambda::Function` Ressourcentyp mithilfe der CloudTrail Konsole oder CloudTrail API-Operationen protokollieren. AWS CLI Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit der AWS Management Console und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail Benutzerhandbuch.

In der folgenden Tabelle ist der Lambda-Ressourcentyp aufgeführt, für den Sie Datenereignisse protokollieren können. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, der aus der Liste Datenereignistyp auf der CloudTrail Konsole ausgewählt werden kann. In der Wertspalte resources.type wird der `resources.type` Wert angezeigt, den Sie angeben würden, wenn Sie erweiterte Event-Selektoren mithilfe der AWS CLI APIs oder konfigurieren würden. CloudTrail In der CloudTrail Spalte „Protokollierte Daten-APIs“ werden die API-Aufrufe angezeigt, die CloudTrail für den Ressourcentyp protokolliert wurden.

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten-APIs, bei denen die Anmeldung erfolgt CloudTrail
Lambda	`AWS::Lambda::Function`	Aufrufen

Sie können erweiterte Event-Selektoren so konfigurieren, dass sie nach den `resources.ARN` Feldern `eventNamereadOnly`, und filtern, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Das folgende Beispiel zeigt die JSON-Ansicht einer Datenereigniskonfiguration, in der nur Ereignisse für eine bestimmte Funktion protokolliert werden. Weitere Informationen zu diesen Feldern finden Sie AdvancedFieldSelectorin der AWS CloudTrail API-Referenz.

```
[
  {
    "name": "function-invokes",
    "fieldSelectors": [
      {
        "field": "eventCategory",
        "equals": [
          "Data"
        ]
      },
      {
        "field": "resources.type",
        "equals": [
```

```
          "AWS::Lambda::Function"
        ]
      },
      {
        "field": "resources.ARN",
        "equals": [
          "arn:aws:lambda:us-east-1:111122223333:function:hello-world"
        ]
      }
    ]
  }
]
```

Lambda-Management-Ereignisse in CloudTrail

Verwaltungsereignisse enthalten Informationen zu Verwaltungsvorgängen, die an Ressourcen in Ihrem AWS-Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. In der Standardeinstellung werden Verwaltungsereignisse CloudTrail protokolliert.

Lambda unterstützt die Protokollierung der folgenden Aktionen als Verwaltungsereignisse in CloudTrail Protokolldateien.

> **Note**
>
> In der CloudTrail Protokolldatei `eventName` können sie Datums- und Versionsinformationen enthalten, sie beziehen sich jedoch immer noch auf dieselbe öffentliche API-Aktion. Die `GetFunction` Aktion wird beispielsweise als angezeigt`GetFunction20150331v2`. In der folgenden Liste wird angegeben, wann sich der Ereignisname vom API-Aktionsnamen unterscheidet.

- AddLayerVersionPermission
- AddPermission(Name des Ereignisses:`AddPermission20150331v2`)
- CreateAlias(Name des Ereignisses:`CreateAlias20150331`)
- CreateEventSourceMapping(Name des Ereignisses:`CreateEventSourceMapping20150331`)
- CreateFunction(Name des Ereignisses:`CreateFunction20150331`)

  (Die `ZipFile` Parameter `Environment` und werden in den CloudTrail Protokollen für weggelassen`CreateFunction`.)

- CreateFunctionUrlConfig
- DeleteAlias(Name des Ereignisses:`DeleteAlias20150331`)
- DeleteCodeSigningConfig
- DeleteEventSourceMapping(Name des Ereignisses:`DeleteEventSourceMapping20150331`)
- DeleteFunction(Name des Ereignisses:`DeleteFunction20150331`)
- DeleteFunctionParallelität (Name des Ereignisses:`DeleteFunctionConcurrency20171031`)
- DeleteFunctionUrlConfig
- DeleteProvisionedConcurrencyConfig
- GetAlias(Name des Ereignisses:`GetAlias20150331`)
- GetEventSourceMapping
- GetFunction
- GetFunctionUrlConfig
- GetFunctionKonfiguration
- GetLayerVersionPolicy
- GetPolicy
- ListEventSourceMappings
- ListFunctions
- ListFunctionUrlConfigs
- PublishLayerVersion (Name des Ereignisses:`PublishLayerVersion20181031`)

  (Der `ZipFile` Parameter wird in den CloudTrail Protokollen für weggelassen`PublishLayerVersion`.)
- PublishVersion(Name des Ereignisses:`PublishVersion20150331`)
- PutFunctionParallelität (Name des Ereignisses:`PutFunctionConcurrency20171031`)
- PutFunctionCodeSigningConfig
- PutFunctionEventInvokeConfig
- PutProvisionedConcurrencyConfig
- PutRuntimeManagementConfig
- RemovePermission(Name des Ereignisses:`RemovePermission20150331v2`)
- TagResource(Name des Ereignisses:`TagResource20170331v2`)
- UntagResource(Name des Ereignisses:`UntagResource20170331v2`)

- UpdateAlias(Name des Ereignisses:`UpdateAlias20150331`)
- UpdateCodeSigningConfig
- UpdateEventSourceMapping(Name des Ereignisses:`UpdateEventSourceMapping20150331`)
- UpdateFunctionCode (Name des Ereignisses:`UpdateFunctionCode20150331v2`)

  (Der `ZipFile` Parameter wird in den CloudTrail Protokollen für weggelassen`UpdateFunctionCode`.)
- UpdateFunctionKonfiguration (Name des Ereignisses:`UpdateFunctionConfiguration20150331v2`)

  (Der `Environment` Parameter wird in den CloudTrail Protokollen für weggelassen`UpdateFunctionConfiguration`.)
- UpdateFunctionEventInvokeConfig
- UpdateFunctionUrlConfig

Wird CloudTrail zur Fehlerbehebung bei deaktivierten Lambda-Ereignisquellen verwendet

Wenn Sie den Status einer Ereignisquellenzuordnung mithilfe der UpdateEventSourceMappingAPI-Aktion ändern, wird der API-Aufruf als Verwaltungsereignis protokolliert. CloudTrail Zuordnungen von Ereignisquellen können aufgrund von Fehlern auch direkt in den `Disabled` Status übergehen.

Für die folgenden Dienste veröffentlicht Lambda das `LambdaESMDisabled` Datenereignis, CloudTrail wenn Ihre Ereignisquelle in den Status Deaktiviert übergeht:

- Amazon-Simple-Queue-Service (Amazon SQS)
- Amazon-DynamoDB
- Amazon Kinesis

Lambda unterstützt dieses Ereignis nicht für andere Zuordnungstypen von Ereignisquellen.

Um Benachrichtigungen zu erhalten, wenn Ereignisquellenzuordnungen für unterstützte Dienste in den `Disabled` Status wechseln, richten Sie in Amazon einen Alarm ein, der das `LambdaESMDisabled` CloudTrail Ereignis CloudWatch verwendet. Weitere Informationen zum Einrichten eines CloudWatch Alarms finden Sie unter CloudWatch Alarme für CloudTrail Ereignisse erstellen: Beispiele.

Die `serviceEventDetails` Entität in der `LambdaESMDisabled` Ereignismeldung enthält einen der folgenden Fehlercodes.

`RESOURCE_NOT_FOUND`

Die in der Anforderung angegebene Ressource ist nicht vorhanden.

`FUNCTION_NOT_FOUND`

Die an die Ereignisquelle angefügte Funktion ist nicht vorhanden.

`REGION_NAME_NOT_VALID`

Ein Regionsname, der der Ereignisquelle oder -funktion zur Verfügung gestellt wird, ist ungültig.

`AUTHORIZATION_ERROR`

Es wurden keine Berechtigungen festgelegt oder sie wurden falsch konfiguriert.

`FUNCTION_IN_FAILED_STATE`

Der Funktionscode wird nicht kompiliert, hat eine nicht wiederherstellbare Ausnahme festgestellt oder eine fehlerhafte Bereitstellung ist aufgetreten.

Beispiele für Lambda-Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt CloudTrail Protokolleinträge für die `DeleteFunction` Aktionen `GetFunction` und.

> **Note**
>
> Die `eventName` kann Datums- und Versionsinformationen enthalten, wie z. B. die `"GetFunction20150331"`, aber sie bezieht sich immer noch auf dieselbe öffentliche API.

```
{
  "Records": [
    {
```

```
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "lambda.amazonaws.com",
      "eventName": "GetFunction",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::111122223333:user/myUserName is not
 authorized to perform: lambda:GetFunction on resource: arn:aws:lambda:us-
west-2:111122223333:function:other-acct-function",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "lambda.amazonaws.com",
      "eventName": "DeleteFunction20150331",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "functionName": "basic-node-task"
```

```
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalte.

Visualisieren Sie Lambda-Funktionsaufrufe mit AWS X-Ray

Sie können AWS X-Ray es verwenden, um die Komponenten Ihrer Anwendung zu visualisieren, Leistungsengpässe zu identifizieren und Anfragen zu beheben, die zu einem Fehler geführt haben. Ihre Lambda-Funktionen senden Ablaufverfolgungs-Daten an X-Ray und X-Ray verarbeitet die Daten, um eine Service-Map und durchsuchbare Ablaufverfolgungs-Zusammenfassungen zu generieren.

Wenn Sie die X-Ray-Verfolgung in einem Service aktiviert haben, der Ihre Funktion aufruft, sendet Lambda automatisch Ablaufverfolgungen an X-Ray. Der Upstream-Service, z. B. Amazon API Gateway oder eine Anwendung auf Amazon EC2, die mit dem X-Ray-SDK instrumentiert ist, entnimmt eingehenden Anforderungen Proben und fügt einen Ablaufverfolfungs-Header hinzu, der angibt, ob Lambda Ablaufverfolgungen senden soll oder nicht. Traces von Upstream-Nachrichtenproduzenten wie Amazon SQS werden automatisch mit Traces von nachgeschalteten Lambda-Funktionen verknüpft, sodass eine end-to-end Ansicht der gesamten Anwendung entsteht. Weitere Informationen finden Sie unter Ablaufverfolgung ereignisgesteuerter Anwendungen im AWS X-Ray -Entwicklerhandbuch.

> **Note**
>
> X-Ray Tracing wird derzeit nicht für Lambda-Funktionen mit Amazon Managed Streaming für Apache Kafka (Amazon MSK), selbstverwaltetem Apache Kafka, Amazon MQ mit ActiveMQ und RabbitMQ oder Zuordnungen von Amazon-DocumentDB-Ereignisquellen unterstützt.

Gehen Sie folgendermaßen vor, um die aktive Nachverfolgung Ihrer Lambda-Funktion mit der Konsole umzuschalten:

So aktivieren Sie die aktive Nachverfolgung

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Configuration (Konfiguration) und dann Monitoring and operations tools (Überwachungs- und Produktionstools).
4. Wählen Sie Bearbeiten aus.
5. Schalten Sie unter X-Ray Active tracing (Aktive Nachverfolgung) ein.
6. Wählen Sie Speichern.

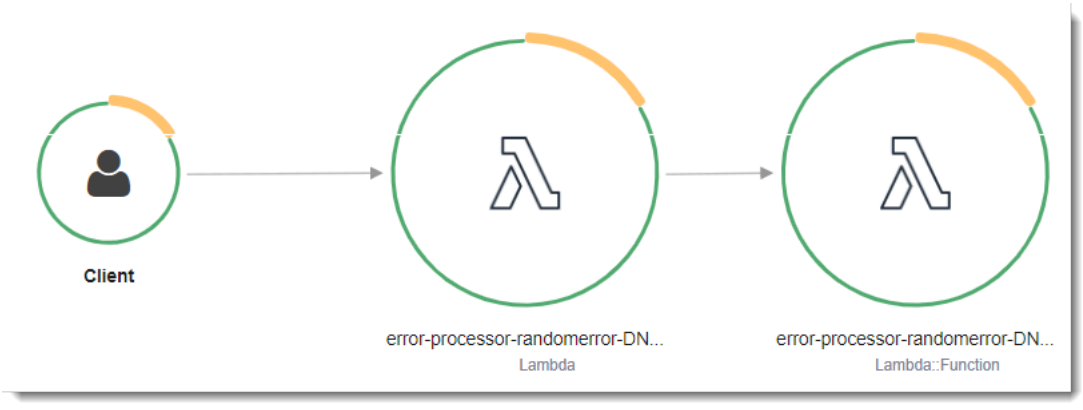
> **Preisgestaltung**
>
> Im Rahmen des kostenlosen Kontingents können Sie X-Ray Tracing jeden Monat bis zu einem bestimmten Limit AWS kostenlos nutzen. Über den Schwellenwert hinaus berechnet X-Ray Gebühren für die Speicherung und den Abruf der Nachverfolgung. Weitere Informationen finden Sie unter AWS X-Ray Preise.

Ihre Funktion benötigt die Berechtigung zum Hochladen von Trace-Daten zu X-Ray.
Wenn Sie die aktive Nachverfolgung in der Lambda-Konsole aktivieren, fügt Lambda der Ausführungsrolle Ihrer Funktion die erforderlichen Berechtigungen hinzu. Andernfalls fügen Sie die AWSXRayDaemonWriteAccessRichtlinie der Ausführungsrolle hinzu.

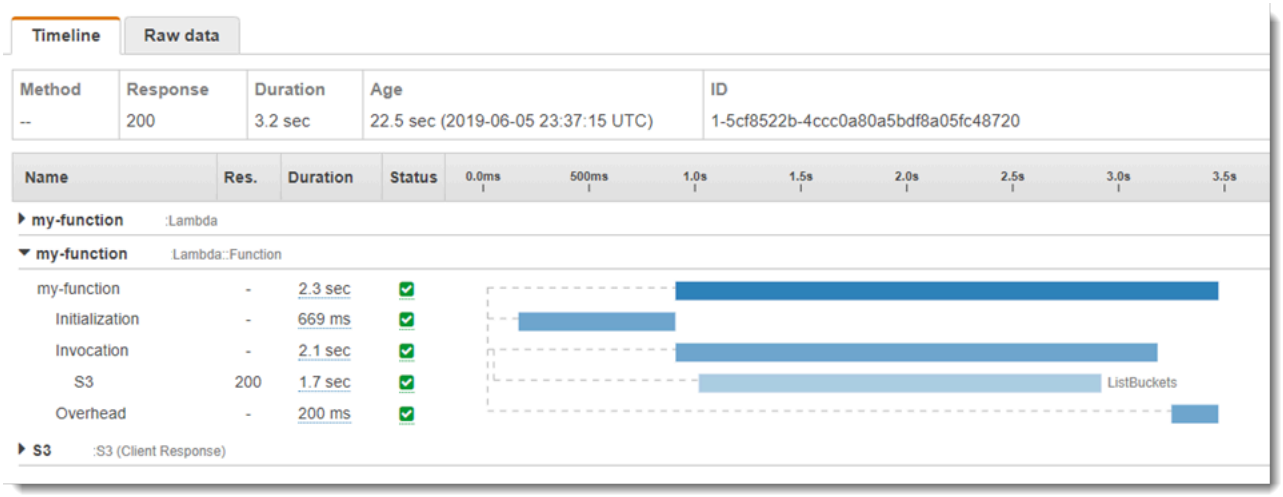
X-Ray verfolgt nicht alle Anfragen an Ihre Anwendung nach. X-Ray wendet einen Sampling-Algorithmus an, um sicherzustellen, dass die Nachverfolgung effizient ist, und stellt dennoch ein repräsentatives Beispiel aller Anfragen bereit. Die Samplingrate beträgt 1 Anforderung pro Sekunde und 5 Prozent aller weiteren Anforderungen.

> **Note**
>
> Sie können die X-Ray-Samplingrate nicht für Ihre Funktionen konfigurieren.

In X-Ray, zeichnet eine Ablaufverfolgung Informationen zu einer Anforderung auf, die von einem oder mehreren Services verarbeitet wird. Lambda zeichnet 2 Segmente pro Trace auf, wodurch zwei Knoten im Service-Graph erstellt werden. In der folgenden Abbildung werden diese beiden Knoten hervorgehoben:



Der erste Knoten auf der linken Seite stellt den Lambda-Service dar, der die Aufrufanforderung empfängt. Der zweite Knoten stellt Ihre spezifische Lambda-Funktion dar. Das folgende Beispiel zeigt eine Nachverfolgung mit diesen zwei Segmenten. Beide haben den Namen my-function, aber eine hat einen Ursprung von `AWS::Lambda` und die andere hat einen Ursprung von`AWS::Lambda::Function`. Wenn das `AWS::Lambda` Segment einen Fehler anzeigt, hatte der Lambda-Service ein Problem. Wenn das `AWS::Lambda::Function` Segment einen Fehler anzeigt, ist bei Ihrer Funktion ein Problem aufgetreten.



Das Funktionssegment (`AWS::Lambda::Function`) enthält Untersegmente für`Initialization`,`Invocation`, `Restore` (Lambda SnapStartnur) und`Overhead`. Weitere Informationen finden Sie unter Lebenszyklus der Lambda-Ausführungsumgebung.

> **Note**
>
> X-Ray verarbeitet unbehandelte Ausnahmen in Ihrer Lambda-Funktion als `Error`-Status. X-Ray zeichnet die `Fault`-Status nur dann auf, wenn bei Lambda interne Serverfehler auftreten. Weitere Informationen finden Sie unter Fehler, Störungen und Ausnahmen im X-Ray-Entwicklerhandbuch.

Das `Initialization`-Teilsegment stellt die Init-Phase des Lebenszyklus der Lambda-Ausführungsumgebung dar. Während dieser Phase erstellt oder gibt Lambda eine Ausführungsumgebung mit den von Ihnen konfigurierten Ressourcen frei, lädt den Funktionscode und alle Ebenen herunter, initialisiert Erweiterungen, initialisiert die Laufzeit und führt den Initialisierungscode der Funktion aus.

Das `Invocation`-Teilsegment stellt die Aufrufphase dar, in welcher der Lambda-Funktionshandler aufgerufen wird. Dies beginnt mit der Laufzeit- und Erweiterungsregistrierung und endet, wenn die Laufzeit bereit ist, die Antwort zu senden.

(nur Lambda SnapStart): Das Teilsegment `Restore` zeigt die Zeit an, die Lambda benötigt, um einen Snapshot wiederherzustellen, die Laufzeit (JVM) zu laden und alle `afterRestore`-Laufzeit-Hooks auszuführen. Der Prozess der Wiederherstellung von Snapshots kann Zeit beinhalten, die für Aktivitäten außerhalb der MicroVM aufgewendet wird. Diese Zeit wird im `Restore`-Untersegment erfasst. Die Zeit, die Sie außerhalb der microVM für die Wiederherstellung eines Snapshots aufwenden, wird Ihnen nicht in Rechnung gestellt.

Das `Overhead`-Teilsegment stellt die Phase dar, die zwischen dem Zeitpunkt, zu dem die Laufzeit die Antwort sendet, und dem Signal für den nächsten Aufruf auftritt. Während dieser Zeit beendet die Laufzeit alle Aufgaben im Zusammenhang mit einem Aufruf und bereitet sich auf das Einfrieren der Sandbox vor.

> **Note**
>
> Gelegentlich bemerken Sie in Ihren X-Ray-Ablaufverfolgungen eine große Lücke zwischen den Phasen der Funktionsinitialisierung und des Funktionsaufrufs. Bei Funktionen, die bereitgestellte Gleichzeitigkeit verwenden, liegt dass daran, dass Lambda Ihre Funktions-Instances lange vor dem Aufruf initialisiert. Für Funktionen, die unreservierte (On-demand) Gleichzeitigkeit verwenden, kann Lambda eine Funktions-Instance proaktiv initialisieren, auch wenn kein Aufruf erfolgt. Visuell werden diese beiden Fälle als Zeitlücke zwischen der Initialisierungs- und der Aufrufphase angezeigt.

> **Important**
>
> In Lambda können Sie das X-Ray-SDK verwenden, um das `Invocation`-Teilsegment mit zusätzlichen Teilsegmenten für nachgeschaltete Aufrufe, Anmerkungen und Metadaten zu erweitern. Sie können nicht direkt auf das Funktionssegment zugreifen oder Arbeiten außerhalb des Handler-Aufruffunktionsbereichs aufzeichnen.

In den folgenden Themen finden Sie eine sprachspezifische Einführung in die Ablaufverfolgung in Lambda:

- Instrumentierung von Node.js Code in AWS Lambda
- Instrumentierung von Python-Code in AWS Lambda
- Instrumentierung von Ruby-Code in AWS Lambda
- Instrumentierung von Java-Code in AWS Lambda
- Go-Code instrumentieren AWS Lambda
- Instrumentierung von C#-Code in AWS Lambda

Eine vollständige Liste der Dienste, die Active Instrumentation unterstützen, finden Sie im AWS X-Ray Developer Guide unter Unterstützte AWS Dienste.

Sections

- Berechtigungen für die Ausführungsrolle
- Der AWS X-Ray Dämon
- Aktivieren der aktiven Ablaufverfolgung mit der Lambda-API
- Aktiviert die aktive Ablaufverfolgung mit AWS CloudFormation

Berechtigungen für die Ausführungsrolle

Lambda benötigt die folgenden Berechtigungen, um Ablaufverfolgungsdaten an X-Ray zu senden. Fügen Sie sie der Ausführungsrolle Ihrer Funktion hinzu.

- xray: Segmente PutTrace
- xray: Aufzeichnungen PutTelemetry

Diese Berechtigungen sind in der AWSXRayDaemonWriteAccessverwalteten Richtlinie enthalten.

Der AWS X-Ray Dämon

Anstatt Ablaufverfolgungsdaten direkt an die X-Ray-API zu senden, verwendet das X-Ray-SDK einen Daemon-Prozess. Der AWS X-Ray -Daemon ist eine Anwendung, die in der Lambda-Umgebung ausgeführt wird und auf UDP-Datenverkehr wartet, der Segmente und Teilsegmente enthält. Sie puffert eingehende Daten und schreibt sie in X-Ray in Batches, wodurch der Verarbeitungs- und Speicheraufwand reduziert wird, der zum Nachverfolgen von Aufrufen erforderlich ist.

Die Lambda-Laufzeit erlaubt dem Daemon bis zu 3 Prozent des konfigurierten Speichers Ihrer Funktion oder 16 MB, je nachdem, welcher Wert größer ist. Wenn Ihre Funktion während des Aufrufs nicht genügend Arbeitsspeicher hat, beendet die Laufzeitumgebung zuerst den Daemon-Prozess, um Speicher freizugeben.

Der Daemon-Prozess wird vollständig von Lambda verwaltet und kann nicht vom Benutzer konfiguriert werden. Alle Segmente, die durch Funktionsaufrufe generiert werden, werden im selben Konto wie die Lambda-Funktion aufgezeichnet. Der Daemon kann nicht so konfiguriert werden, dass er sie an ein anderes Konto umleitet.

Weitere Informationen finden Sie unter X-Ray-Daemon im X-Ray-Entwicklerhandbuch.

Aktivieren der aktiven Ablaufverfolgung mit der Lambda-API

Verwenden Sie die folgenden API-Operationen, um die Ablaufverfolgungskonfiguration mit dem AWS SDK AWS CLI oder zu verwalten:

- UpdateFunctionKonfiguration
- GetFunctionKonfiguration
- CreateFunction

Der folgende AWS CLI Beispielbefehl aktiviert die aktive Ablaufverfolgung für eine Funktion namens my-function.

```
aws lambda update-function-configuration \
--function-name my-function \
--tracing-config Mode=Active
```

Der Ablaufverfolgungsmodus ist Teil der versionsspezifischen Konfiguration, wenn Sie eine Version Ihrer Funktion veröffentlichen. Sie können den Ablaufverfolgungsmodus für eine veröffentlichte Version nicht ändern.

Aktiviert die aktive Ablaufverfolgung mit AWS CloudFormation

Verwenden Sie die Eigenschaft, um die Ablaufverfolgung `AWS::Lambda::Function` für eine Ressource in einer AWS CloudFormation Vorlage zu aktivieren. `TracingConfig`

Example function-inline.yml – Ablaufverfolgungskonfiguration

```
Resources:
```

```
  function:
    Type: AWS::Lambda::Function
    Properties:
      TracingConfig:
        Mode: Active
      ...
```

Verwenden Sie für eine `AWS::Serverless::Function` Ressource AWS Serverless Application Model (AWS SAM) die `Tracing` Eigenschaft.

Example template.yml – Ablaufverfolgungskonfiguration

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Tracing: Active
      ...
```

Überwachen Sie die Funktionsleistung mit Amazon CloudWatch Lambda Insights

Amazon CloudWatch Lambda Insights sammelt und aggregiert Leistungskennzahlen und Protokolle zur Laufzeit von Lambda-Funktionen für Ihre serverlosen Anwendungen. Auf dieser Seite wird beschrieben, wie Sie Lambda Insights aktivieren und verwenden, um Probleme mit Ihren Lambda-Funktionen zu diagnostizieren.

Abschnitte

Wie Lambda Insights Serverless-Anwendungen überwacht

CloudWatch Lambda Insights ist eine Überwachungs- und Fehlerbehebungslösung für serverlose Anwendungen, die auf ausgeführt werden. AWS Lambda Die Lösung erfasst, aggregiert und fasst Metriken auf Systemebene zusammen, einschließlich CPU-Zeit, Arbeitsspeicher, Datenträger- und Netzwerknutzung. Sie erfasst, aggregiert und fasst Diagnoseinformationen wie Kaltstart und Lambda-Worker-Abschaltungen zusammen, um Probleme mit Ihren Lambda-Funktionen zu isolieren und schnell zu beheben.

Lambda Insights verwendet eine neue CloudWatch Lambda Insights-Erweiterung, die als Lambda-Schicht bereitgestellt wird. Wenn Sie diese Erweiterung für eine Lambda-Funktion für eine unterstützte Laufzeit aktivieren, sammelt sie Metriken auf Systemebene und gibt für jeden Aufruf dieser Lambda-Funktion ein einziges Leistungsprotokollereignis aus. CloudWatch verwendet eine eingebettete Metrikformatierung, um Metriken aus den Protokollereignissen zu extrahieren. Weitere Informationen finden Sie unter AWS Lambda Erweiterungen verwenden.

Die Lambda-Insights-Ebene erweitert die `CreateLogStream` und `PutLogEvents` für die `/aws/lambda-insights/`-Protokollgruppe.

Preisgestaltung

Wenn Sie Lambda Insights für Ihre Lambda-Funktion aktivieren, meldet Lambda Insights 8 Metriken pro Funktion, und bei jedem Funktionsaufruf werden etwa 1 KB Protokolldaten an gesendet. CloudWatch Sie zahlen nur für die Metriken und Protokolle, die Lambda Insights für Ihre Funktion gemeldet haben. Es fallen keine Mindestgebühren oder Mindestnutzungsanforderungen an. Sie zahlen nicht für Lambda Insights, wenn die Funktion nicht aufgerufen wird. Ein Preisbeispiel finden Sie unter CloudWatch Amazon-Preise.

Unterstützte Laufzeiten

Sie können Lambda Insights mit jeder Laufzeitumgebung verwenden, die Lambda-Erweiterungen unterstützen.

Lambda Insights in der Lambda-Konsole aktivieren

Sie können die erweiterte Lambda-Insights-Überwachung neuer und vorhandener Lambda-Funktionen aktivieren. Wenn Sie Lambda Insights auf einer Funktion in der Lambda-Konsole für eine unterstützte Laufzeit aktivieren, fügt Lambda die Lambda-Insights-Erweiterung als Ebene Ihrer Funktion hinzu und überprüft die `CloudWatchLambdaInsightsExecutionRolePolicy`-Richtlinie oder versucht, diese der Ausführungsrolle Ihrer Funktion zuzuweisen.

Lambda Insights in der Lambda-Konsole aktivieren

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Ihre Funktion.
3. Wählen Sie die Registerkarte Konfiguration aus.
4. Wählen Sie im linken Menü die Option Überwachungs- und Betriebstools aus.
5. Wählen Sie im Bereich Zusätzliche Überwachungstools die Option Bearbeiten aus.
6. Aktivieren Sie unter CloudWatch Lambda Insights die Option Enhanced Monitoring.
7. Wählen Sie Save aus.

Programmgesteuertes Aktivieren von Lambda Insights

Sie können Lambda Insights auch mithilfe der CLI AWS Command Line Interface (AWS CLI), AWS Serverless Application Model (SAM) oder der AWS Cloud Development Kit (AWS CDK) aktivieren. AWS CloudFormationWenn Sie Lambda Insights programmgesteuert für eine Funktion für eine unterstützte Laufzeit aktivieren, CloudWatch hängt die `CloudWatchLambdaInsightsExecutionRolePolicy`Richtlinie der Ausführungsrolle Ihrer Funktion an.

Weitere Informationen finden Sie unter Erste Schritte mit Lambda Insights im CloudWatch Amazon-Benutzerhandbuch.

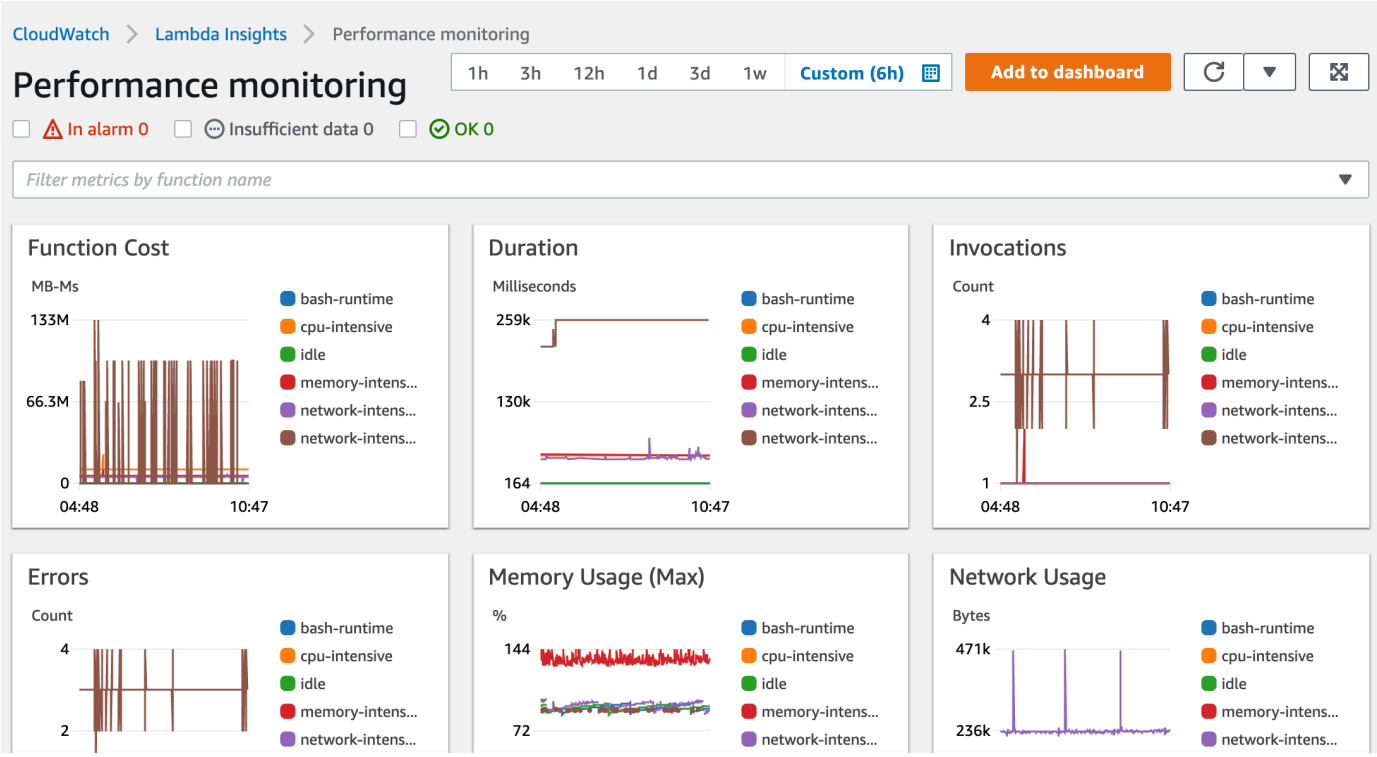
Verwenden des Lambda-Insights-Dashboards

Das Lambda Insights-Dashboard hat zwei Ansichten in der CloudWatch Konsole: die Multifunktionsübersicht und die Einzelfunktionsansicht. In der Multifunktionsübersicht werden die Laufzeitmetriken für die Lambda-Funktionen im AWS Girokonto und in der Region zusammengefasst. Die Einzelfunktionsansicht zeigt die verfügbaren Laufzeit-Metriken für eine einzelne Lambda-Funktion an.

Sie können die Multifunktionsübersicht des Lambda Insights-Dashboards in der CloudWatch Konsole verwenden, um zu stark oder zu wenig genutzte Lambda-Funktionen zu identifizieren. Sie können die Einzelfunktionsansicht des Lambda Insights-Dashboards in der CloudWatch Konsole verwenden, um einzelne Anfragen zu beheben.

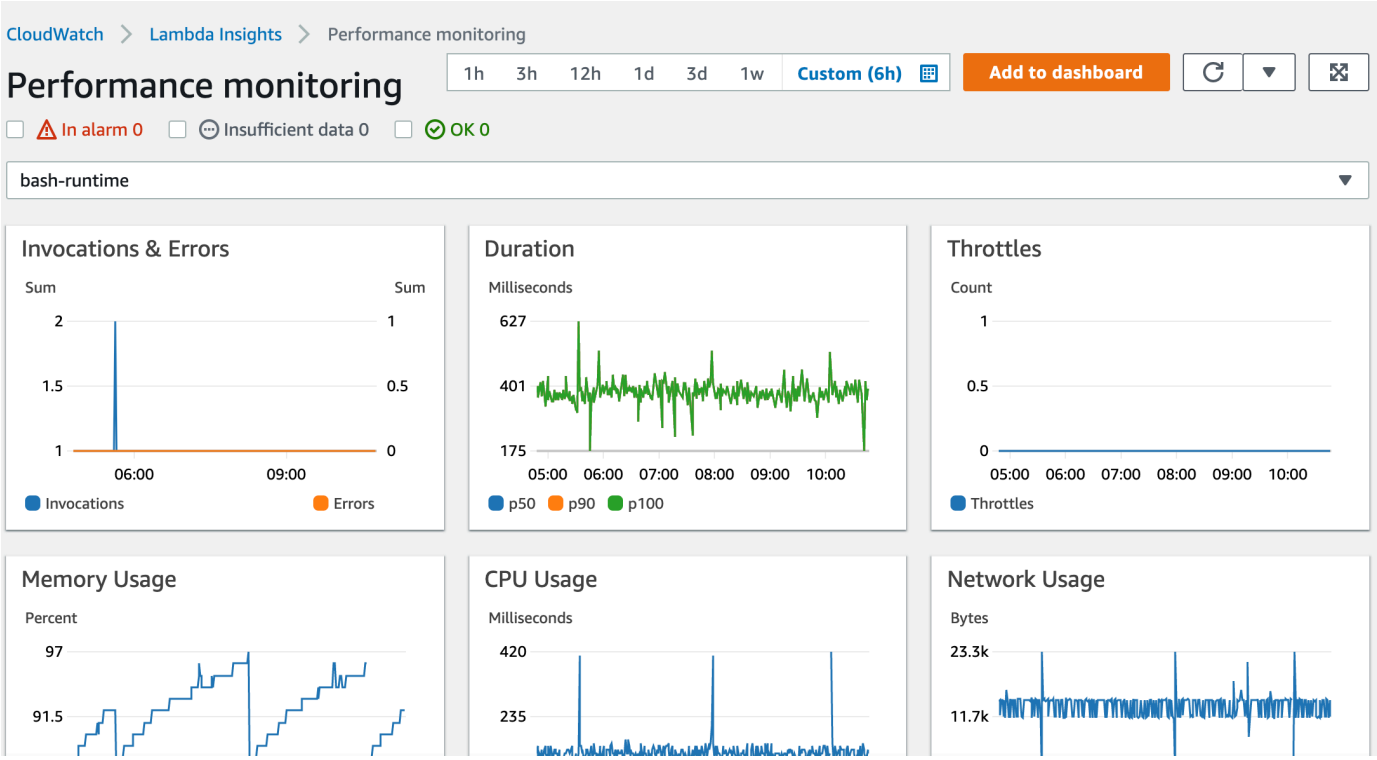
So zeigen Sie die Laufzeit-Metriken für alle Funktionen an:

1. Öffnen Sie die Multifunktionsseite in der Konsole. CloudWatch
2. Wählen Sie aus den vordefinierten Zeitbereichen oder wählen Sie einen benutzerdefinierten Zeitbereich aus.
3. (Optional) Wählen Sie Zum Dashboard hinzufügen, um die Widgets zu Ihrem CloudWatch Dashboard hinzuzufügen.



So zeigen Sie die Laufzeit-Metriken einer einzelnen Funktion an:

1. Öffnen Sie die Einzelfunktionsseite in der CloudWatch Konsole.
2. Wählen Sie aus den vordefinierten Zeitbereichen oder wählen Sie einen benutzerdefinierten Zeitbereich aus.
3. (Optional) Wählen Sie Zum Dashboard hinzufügen, um die Widgets zu Ihrem CloudWatch Dashboard hinzuzufügen.



Weitere Informationen finden Sie unter Widgets auf CloudWatch Dashboards erstellen und damit arbeiten.

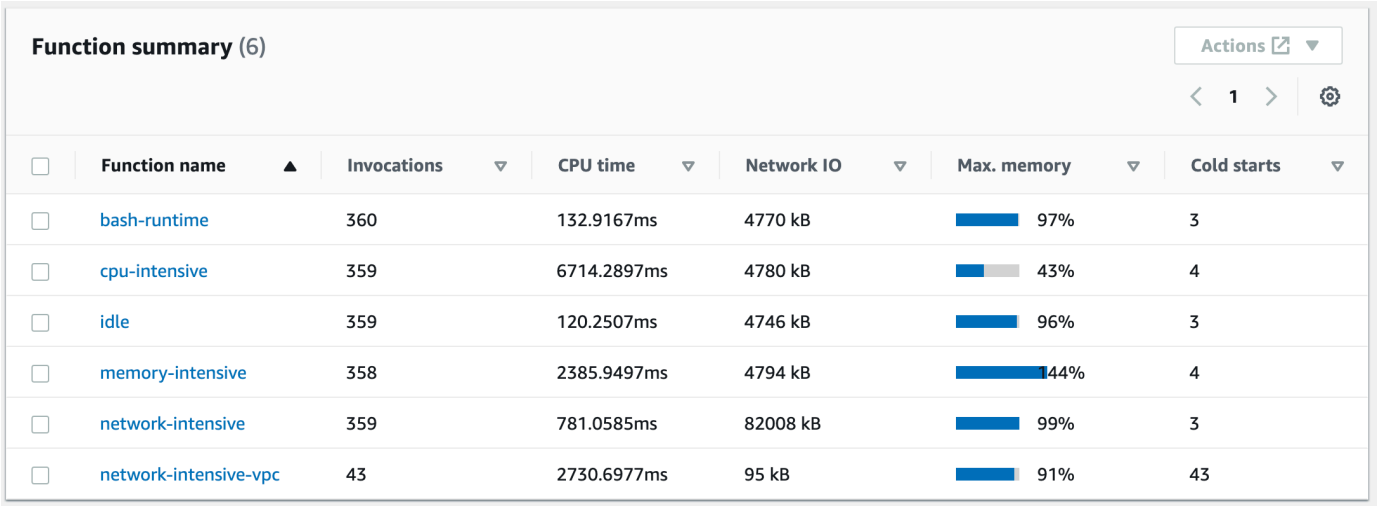
Beispiel-Workflow zum Erkennen von Funktionsanomalien

Sie können die Multifunktionsübersicht auf dem Lambda-Insights-Dashboard verwenden, um Anomalien des Rechenspeichers mit Ihrer Funktion zu identifizieren und zu erkennen. Wenn beispielsweise die Multifunktionsübersicht anzeigt, dass eine Funktion eine große Menge Speicher verwendet, können Sie detaillierte Metriken zur Speicherauslastung im Bereich Memory Usage (Speicherverwendung) anzeigen. Sie können dann zum Metrik-Dashboard wechseln, um die Anomalieerkennung zu aktivieren oder einen Alarm zu erstellen.

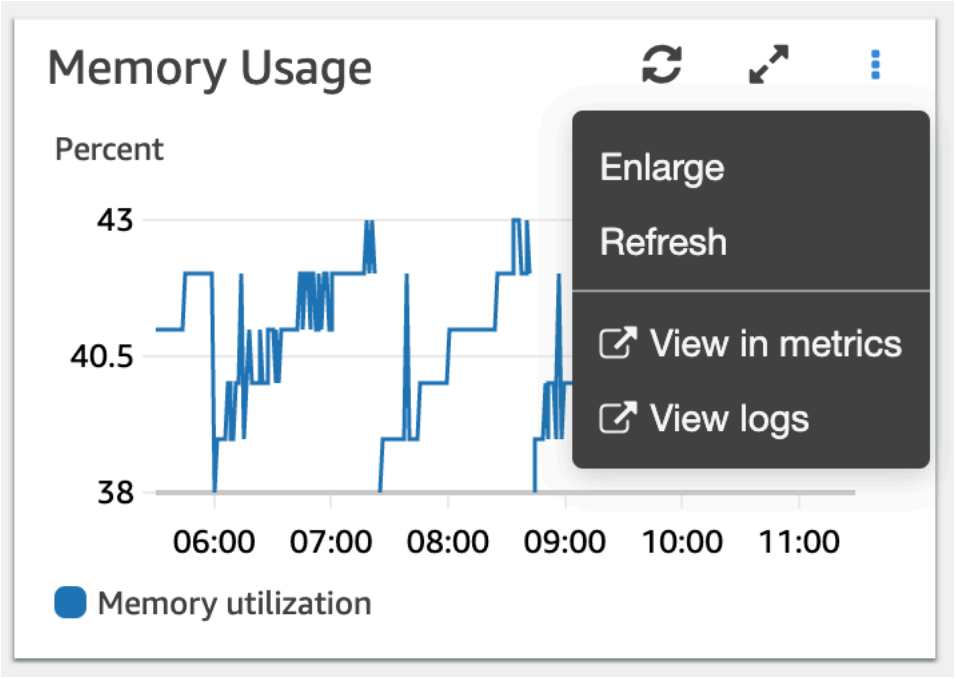
So aktivieren Sie die Anomalieerkennung für eine Funktion:

1. Öffnen Sie die Multifunktionsseite in der CloudWatch Konsole.
2. Wählen Sie unter Function summary (Funktionsübersicht) den Namen Ihrer Funktion aus.

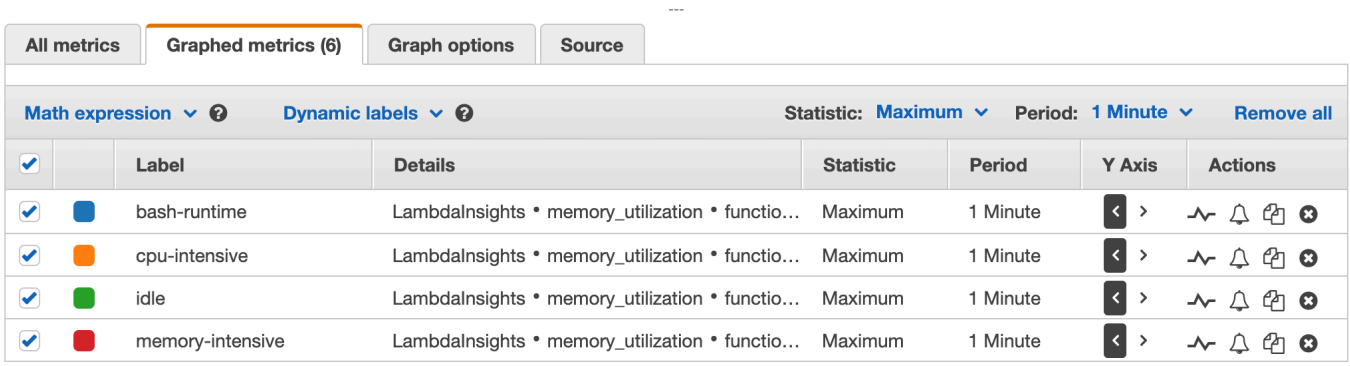
   Die Einzelfunktionsansicht wird mit den Funktionslaufzeitmetriken geöffnet.



3. Wählen Sie im Bereich Memory Usage (Speicherverwendung) die drei vertikalen Punkte aus, und wählen Sie dann View in metrics (In Metriken anzeigen), um das Metrics (Metriken)-Dashboard zu öffnen.



4. Wählen Sie auf der Registerkarte Graphed metrics (Metriken mit Diagrammen) in der Spalte Actions (Aktionen) das erste Symbol aus, um die Anomalieerkennung für die Funktion zu aktivieren.



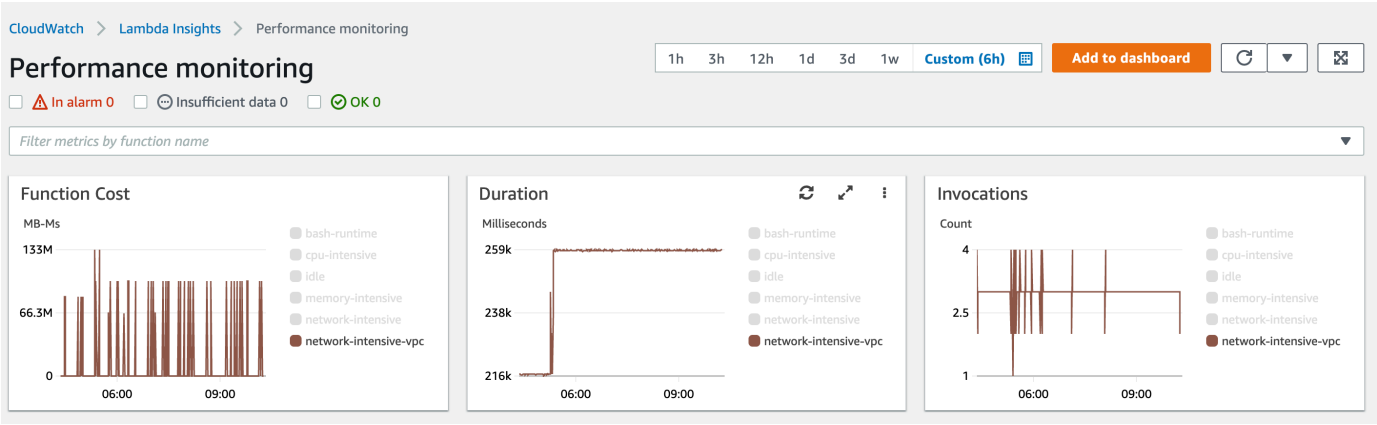
Weitere Informationen finden Sie unter Verwenden der CloudWatch Anomalieerkennung.

Beispiel-Workflow mit Abfragen zur Fehlerbehebung einer Funktion

Sie können die Einzelfunktionsansicht im Lambda-Insights-Dashboard verwenden, um die Ursache eines Spitzenwerts der Funktionsdauer zu ermitteln. Wenn beispielsweise die Multifunktionsübersicht eine starke Erhöhung der Funktionsdauer anzeigt, können Sie jede Funktion im Bereich Duration (Dauer) anhalten oder auswählen, um festzustellen, welche Funktion die Erhöhung verursacht. Sie können dann zur Einzelfunktionsansicht wechseln und die Anwendungsprotokolle überprüfen, um die Ursache zu ermitteln.

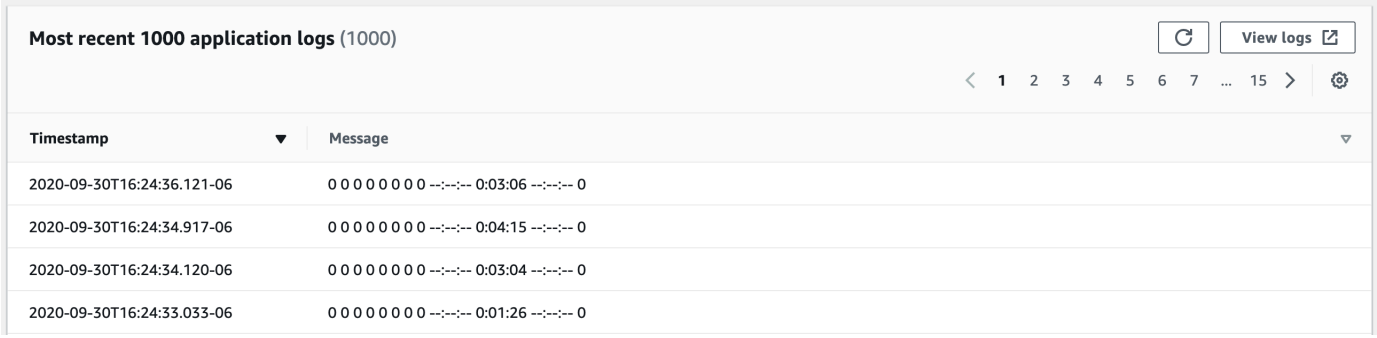
So führen Sie Abfragen für eine Funktion aus:

1. Öffnen Sie die Multifunktionsseite in der CloudWatch Konsole.
2. Wählen Sie im Bereich Duration (Dauer) Ihre Funktion aus, um die Dauer-Metriken zu filtern.

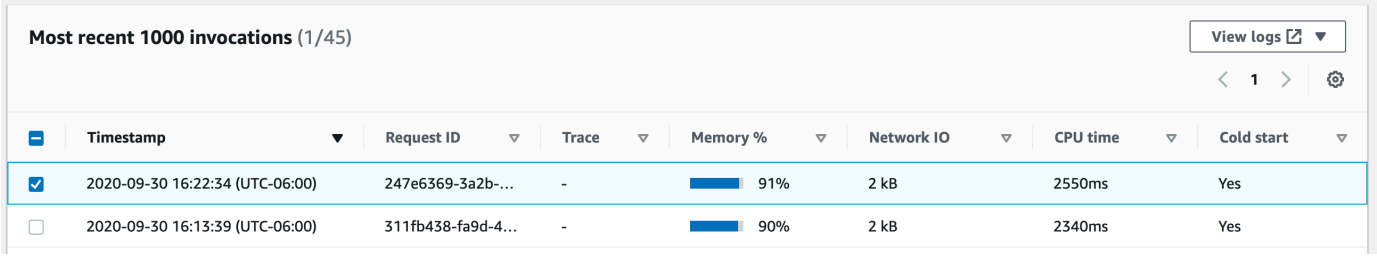


3. Öffnen Sie die Seite Einzelfunktionsansicht.
4. Wählen Sie die Dropdown-Liste Filter metrics by function name (Metriken nach Funktionsnamen filtern) und wählen Sie dann Ihre Funktion aus.

5. Um die neuesten 1000 Anwendungsprotokolle anzuzeigen, wählen Sie die Registerkarte Application logs (Anwendungsprotokolle).
6. Überprüfen Sie den Zeitstempel und die Meldung um die Aufrufanforderung zu identifizieren, für die Sie Fehler beheben möchten.

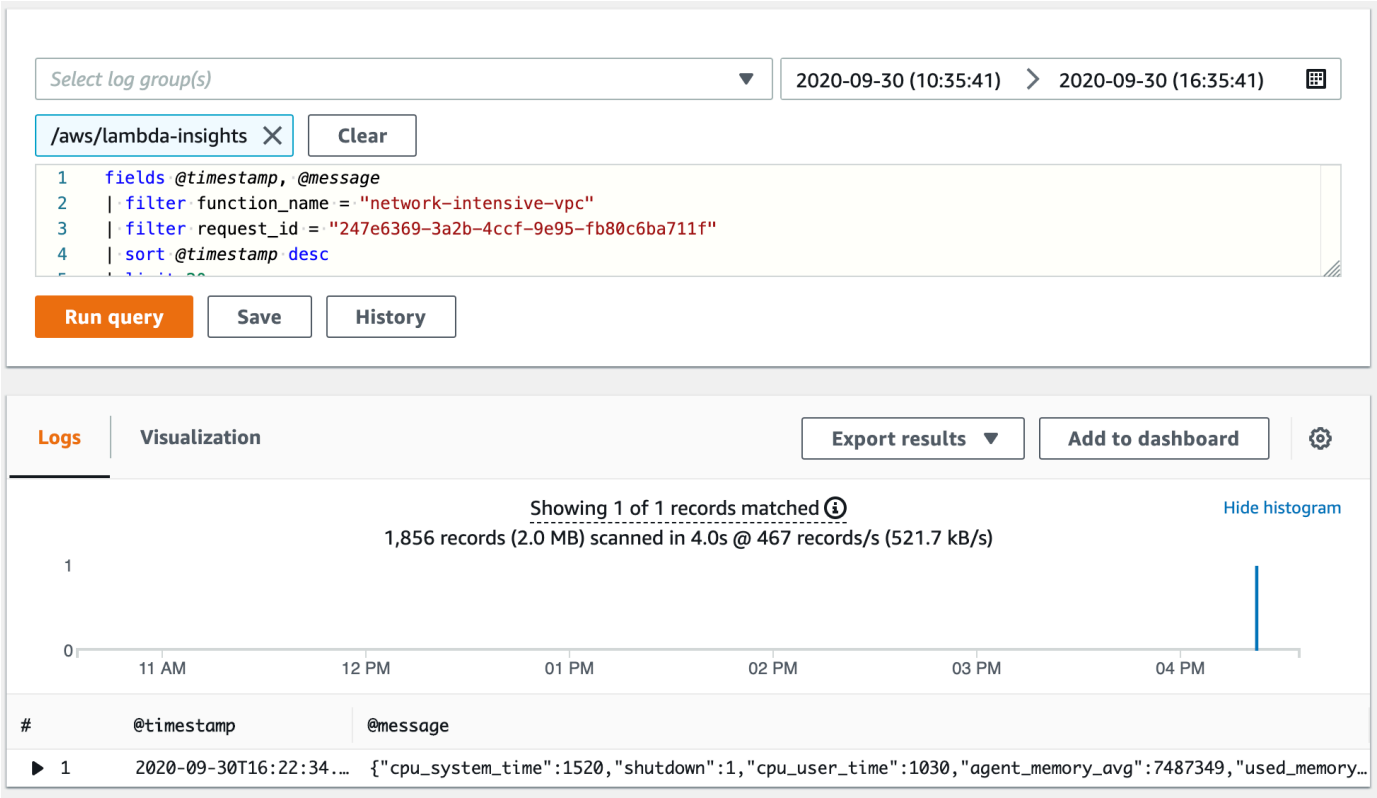


7. Um die letzten 1000 Aufrufe anzuzeigen, wählen Sie die Registerkarte Invocations (Aufrufe).
8. Wählen Sie den Zeitstempel oder die Meldung für die Aufrufanforderung aus, für die Sie Fehler beheben möchten.



9. Wählen Sie die Dropdown-Liste View logs (Protokolle anzeigen) und wählen Sie dann View performance logs (Leistungsprotokolle anzeigen) aus.

   Im Dashboard Logs Insights (Protokolleinblicke) wird eine automatisch generierte Abfrage für Ihre Funktion geöffnet.
10. Wählen Sie Run query (Abfrage ausführen), um eine Logs (Protokolle)-Meldung für die Aufrufanforderung zu generieren.



Als nächstes

- Weitere Informationen zum Erstellen eines CloudWatch Logs-Dashboards finden Sie unter Create a Dashboard im CloudWatch Amazon-Benutzerhandbuch.
- Weitere Informationen zum Hinzufügen von Abfragen zu einem CloudWatch Logs-Dashboard finden Sie unter „Abfrage zum Dashboard hinzufügen“ oder „Abfrageergebnisse exportieren“ im CloudWatch Amazon-Benutzerhandbuch.

Verwenden von CodeGuru Profiler mit Ihrer Lambda-Funktion

Sie können Amazon CodeGuru Profiler verwenden, um Einblicke in die Laufzeitleistung Ihrer Lambda-Funktionen zu erhalten. Auf dieser Seite wird beschrieben, wie Sie CodeGuru Profiler über die Lambda-Konsole aktivieren.

Sections

Unterstützte Laufzeiten

Sie können CodeGuru Profiler über die Lambda-Konsole aktivieren, wenn die Laufzeit Ihrer Funktion Python3.8, Python3.9, Java 8 mit Amazon Linux 2, Java 11 oder Java 17 ist. Für zusätzliche Laufzeitversionen können Sie CodeGuru Profiler manuell aktivieren.

- Informationen zu Java-Laufzeiten finden Sie unter Profilerstellung Ihrer Java-Anwendungen, die auf AWS Lambda ausgeführt werden.
- Informationen zu Python-Laufzeiten finden Sie unter Profilerstellung Ihrer Python-Anwendungen, die auf AWS Lambda ausgeführt werden.

> **Note**
>
> CodeGuru Profiler unterstützt derzeit nur Funktionen, die die x86_64-Architektur verwenden.

Aktivieren von CodeGuru Profiler über die Lambda-Konsole

In diesem Abschnitt wird beschrieben, wie Sie CodeGuru Profiler über die Lambda-Konsole aktivieren.

So aktivieren Sie CodeGuru Profiler über die Lambda-Konsole

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.

2. Wählen Sie Ihre Funktion.
3. Wählen Sie die Registerkarte Konfiguration aus.
4. Wählen Sie im Bereich Überwachungstools und Produktionstools die Option Bearbeiten.
5. Aktivieren Sie unter Amazon CodeGuru Profiler die Code-Profilerstellung.
6. Wählen Sie Speichern.

Nach der Aktivierung erstellt CodeGuru automatisch eine Profilergruppe mit dem Namen `aws-lambda-<your-function-name>`. Sie können den Namen über die CodeGuru Konsole ändern.

Was passiert, wenn Sie CodeGuru Profiler über die Lambda-Konsole aktivieren?

Wenn Sie CodeGuru Profiler über die Konsole aktivieren, führt Lambda automatisch Folgendes in Ihrem Namen aus:

- Lambda fügt Ihrer Funktion eine CodeGuru Profiler-Ebene hinzu. Weitere Informationen finden Sie unter Verwenden von AWS Lambda Ebenen im Amazon- CodeGuru Profiler-Benutzerhandbuch.
- Lambda fügt Ihrer Funktion auch Umgebungsvariablen hinzu. Der genaue Wert variiert je nach Laufzeit.

  Umgebungsvariablen

Laufzeiten	Schlüssel	Value
java8.al2, java11	`JAVA_TOOL_OPTIONS`	`-javaagent:/opt/codeguru-profiler-java-agent-standalone.jar`
python3.8, python3.9	`AWS_LAMBDA_EXEC_WRAPPER`	`/opt/codeguru_profiler_lambda_exec`

- Lambda fügt die `AmazonCodeGuruProfilerAgentAccess`-Richtlinie mit der Ausführungsrolle Ihrer Funktion hinzu.

> **Note**
>
> Wenn Sie CodeGuru Profiler über die Konsole deaktivieren, entfernt Lambda die CodeGuru Profiler-Ebene automatisch aus Ihrer Funktion. Lambda entfernt jedoch nicht die Umgebungsvariablen oder die `AmazonCodeGuruProfilerAgentAccess`-Richtlinie von Ihrer Ausführungsrolle.

Als nächstes

- Weitere Informationen zu den von Ihrer Profilergruppe gesammelten Daten finden Sie unter Arbeiten mit Visualisierungen im Amazon- CodeGuru Profiler-Benutzerhandbuch.

Beispiel-Workflows mit anderen AWS-Services

AWS Lambda lässt sich in andere AWS-Services integrieren, die Ihnen helfen, Ihre Lambda-Funktionen zu überwachen, zu verfolgen, zu debuggen und Fehler an ihnen zu beheben. Diese Seite zeigt Workflows, die Sie mit AWS X-Ray und AWS Trusted Advisor verwenden können, um Ihre Lambda-Funktionen zu verfolgen und Fehler an ihnen zu beheben.

Sections

Voraussetzungen

Im folgenden Abschnitt werden die Schritte zur Verwendung von AWS X-Ray und Trusted Advisor, um Fehler mit Lambda-Funktionen zu beheben, beschrieben.

benutze AWS X-Ray

AWS X-Ray muss auf der Lambda-Konsole aktiviert sein, um die AWS X-Ray-Workflows auf dieser Seite abzuschließen. Wenn Ihre Ausführungsrolle nicht über die erforderlichen Berechtigungen verfügt, versucht die Lambda-Konsole, sie Ihrer Ausführungsrolle hinzuzufügen.

So aktivieren Sie AWS X-Ray auf der Lambda-Konsole

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie Ihre Funktion.
3. Wählen Sie die Registerkarte Konfiguration aus.
4. Wählen Sie im Bereich Monitoring tools (Überwachungstools) die Option Edit (Bearbeiten).
5. Aktivieren Sie unter AWS X-Ray Active tracing (Aktive Nachverfolgung).
6. Wählen Sie Save aus.

benutze AWS Trusted Advisor

AWS Trusted Advisor überprüft Ihre AWS-Umgebung und gibt Empfehlungen für Methoden ab, wie Sie Geld sparen, die Systemverfügbarkeit und -leistung verbessern und Sicherheitslücken schließen können. Sie können Trusted Advisor-Überprüfungen zur Bewertung der Lambda-Funktionen und -Anwendungen in Ihrem AWS-Konto verwenden. Die Prüfungen bieten empfohlene Schritte und Ressourcen für weitere Informationen.

- Weitere Informationen zu AWS-Supportplänen für Trusted Advisor-Überprüfungen finden Sie unter Support-Pläne.
- Weitere Informationen über die Überprüfungen für Lambda finden Sie unter AWS Trusted Advisor Checkliste für bewährte Methoden.
- Weitere Informationen zur Verwendung der Trusted Advisor-Konsole finden Sie unter Erste Schritte mit AWS Trusted Advisor.
- Anweisungen zum Zulassen und Verweigern des Konsolenzugriffs auf Trusted Advisor finden Sie unter Beispiele für IAM-Richtlinien.

Preisgestaltung

- Mit AWS X-Ray zahlen Sie nur für das, was Sie nutzen, basierend auf der Anzahl an aufgezeichneten, abgerufenen und gescannten Traces. Weitere Informationen finden Sie unter AWS X-Ray- Preise.
- Trusted Advisor-Überprüfungen zur Kostenoptimierung sind in den Supportabonnements von AWS Business und Enterprise enthalten. Weitere Informationen finden Sie unter AWS Trusted Advisor-Preise.

Beispiel eines AWS X-Ray-Workflows zum Anzeigen einer Trace-Map

Wenn Sie aktiviert habenAWS X-Ray, können Sie eine Ablaufverfolgungs-Übersicht in der -CloudWatch Konsole anzeigen. Eine Trace-Map zeigt Service-Endpunkte und -Ressourcen als „Knoten“ an und informiert über den Datenverkehr, die Latenz und die Fehler für jeden Knoten und seine Verbindungen.

Sie können einen Knoten auswählen, um detaillierte Einblicke in die korrelierten Metriken, Protokolle und Ablaufverfolgungen anzuzeigen, die mit diesem Teil des Services verknüpft sind. Auf diese Weise können Sie Probleme und deren Auswirkungen auf eine Anwendung untersuchen.

So zeigen Sie Ablaufverfolgungszuordnungen und Ablaufverfolgungen mithilfe der CloudWatch Konsole an

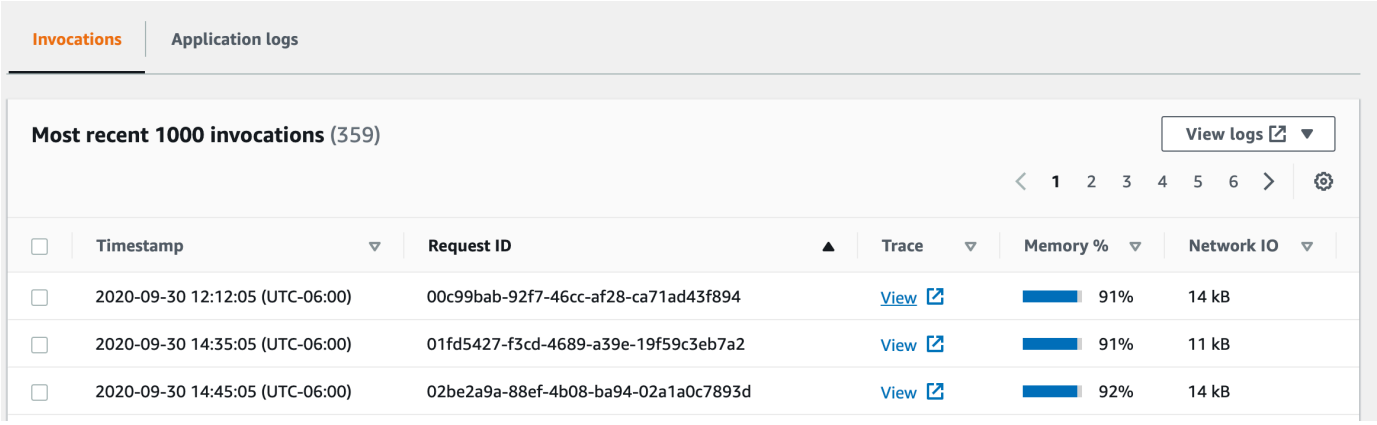
1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie Monitoring.
4. Wählen Sie Traces in X-Ray anzeigen aus.
5. Wählen Sie im linken Navigationsbereich unter X-Ray-Traces die Option Trace-Map aus.
6. Wählen Sie aus den vordefinierten Zeitbereichen oder wählen Sie einen benutzerdefinierten Zeitbereich aus.
7. Um Fehler bei Anfragen zu beheben, wählen Sie einen Filter aus.

Beispiel eines AWS X-Ray-Workflows zum Anzeigen von Nachverfolgungsdetails

Wenn Sie aktiviert habenAWS X-Ray, können Sie die Einzelfunktionsansicht im CloudWatch Lambda-Insights-Dashboard verwenden, um die verteilten Ablaufverfolgungsdaten eines Funktionsaufruffehlers anzuzeigen. Wenn die Anwendungsprotokollmeldung einen Fehler anzeigt, können Sie die Trace-Map öffnen, um die verteilten Trace-Daten und die Services anzuzeigen, die die Transaktion ausführen.

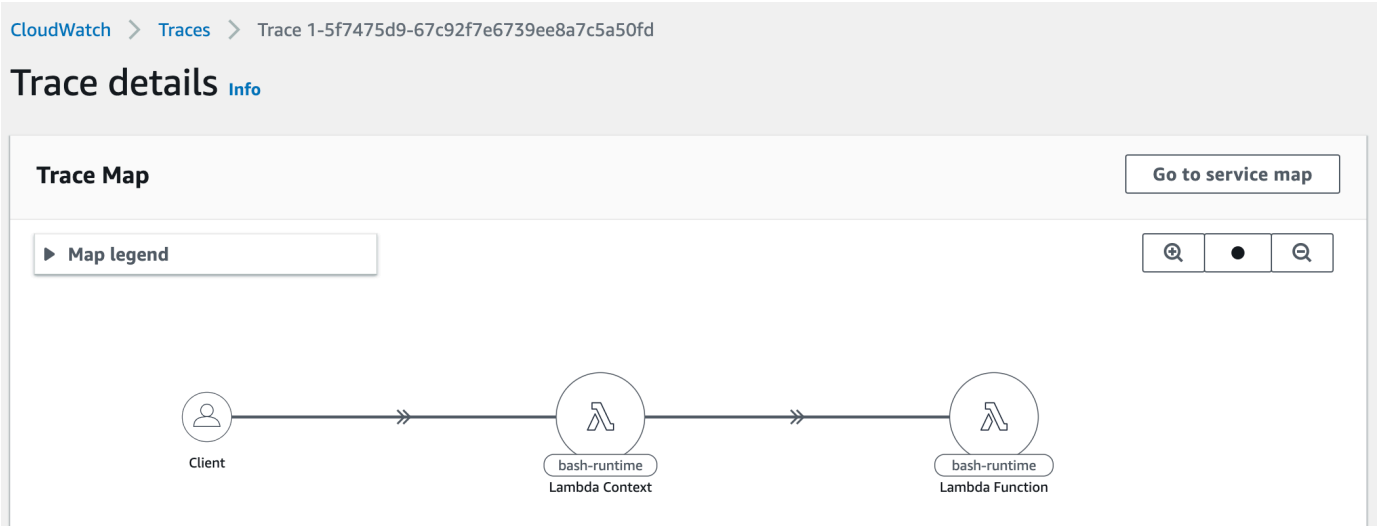
So zeigen Sie Nachverfolgungsdetails einer Funktion an

1. Öffnen Sie die Einzelfunktionsansicht in der - CloudWatch Konsole.
2. Wählen Sie die Registerkarte Application logs (Anwendungsprotokolle) aus.
3. Verwenden Sie den Zeitstempel oder die Meldung, um die Aufrufanforderung zu identifizieren, für die Sie Fehler beheben möchten.
4. Um die letzten 1000 Aufrufe anzuzeigen, wählen Sie die Registerkarte Invocations (Aufrufe).



5. Wählen Sie die Spalte Request ID (Anforderungs-ID) aus, um Einträge in aufsteigender alphabetischer Reihenfolge zu sortieren.
6. Wählen Sie in der Spalte Trace (Nachverfolgung) die Option View (Ansicht) aus.

   Die Seite Trace-Details wird in der Trace-Map-Ansicht geöffnet.



Beispiel eines AWS Trusted Advisor-Workflows zur Anzeige von Empfehlungen

Trusted Advisor prüft Lambda-Funktionen in allen AWS-Regionen, um Funktionen mit den höchsten potenziellen Kosteneinsparungen zu identifizieren und umsetzbare Optimierungsempfehlungen zu liefern. Es analysiert Ihre Lambda-Nutzungsdaten wie Funktionsausführungszeit, abgerechnete Dauer, verwendeter Speicher, konfigurierter Speicher, Timeoutkonfiguration und Fehler.

Die Prüfung von Lambda Functions mit hoher Fehlerrate empfiehlt beispielsweise, dass Sie AWS X-Ray oder verwenden, CloudWatch um Fehler bei Ihren Lambda-Funktionen zu erkennen.

So suchen Sie nach Funktionen mit hohen Fehlerraten

1. Öffnen Sie die Trusted Advisor-Konsole.
2. Wählen Sie die Kategorie Kostenoptimierung aus.
3. Scrollen Sie nach unten zu AWS Lambda-Funktionen mit hohen Fehlerraten. Erweitern Sie den Abschnitt, um die Ergebnisse und die empfohlenen Maßnahmen zu sehen.

Als nächstes

- Unter Verwenden der X-Ray-Trace-Map finden Sie weitere Informationen zur Integration von Traces, Metriken, Protokollen und Alarmen.
- Erfahren Sie in Trusted Advisor als einen Webservice verwenden mehr darüber, wie Sie eine Liste von Trusted Advisor-Überprüfungen erhalten.

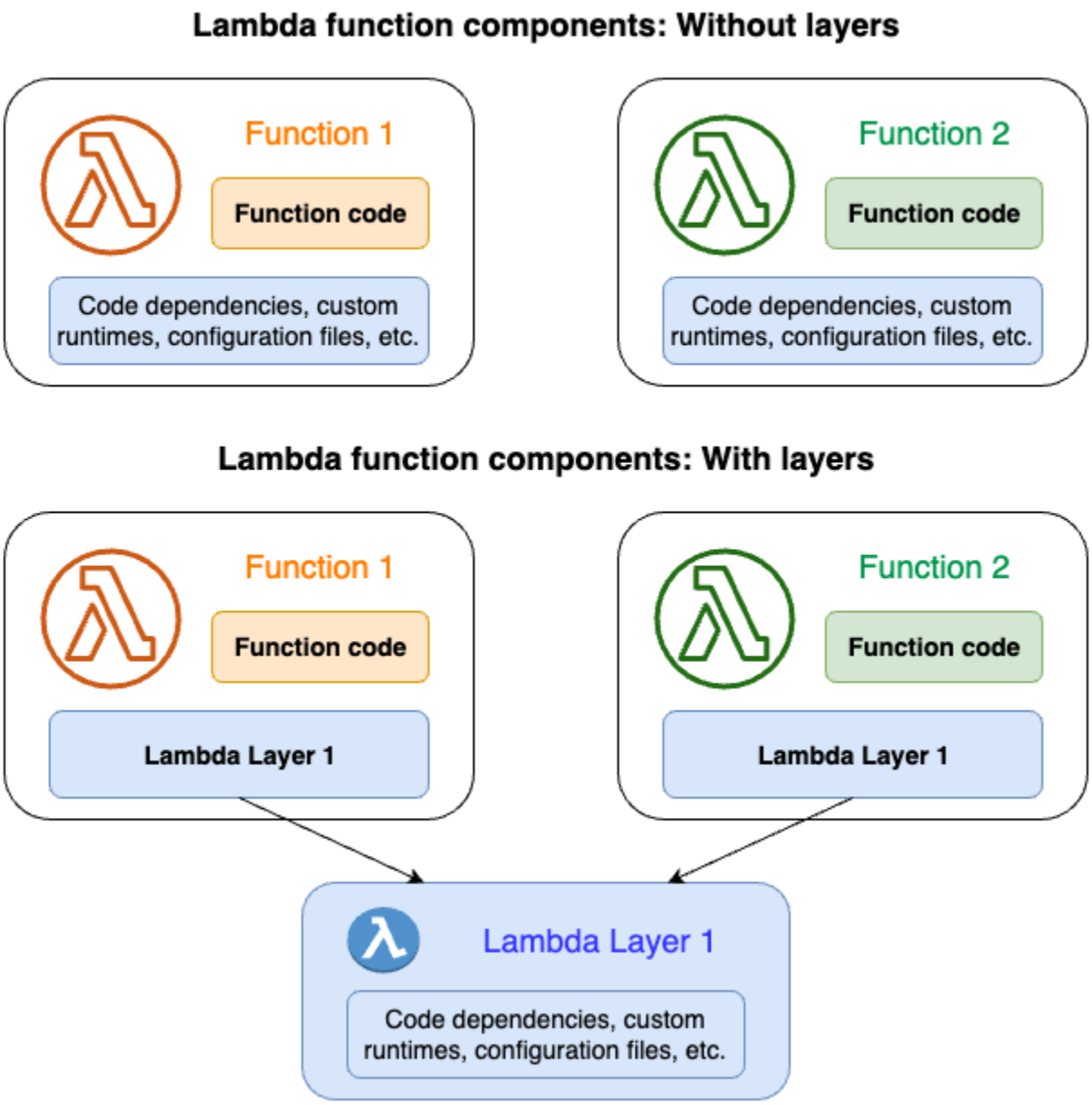
Verwaltung von Lambda-Abhängigkeiten mit Ebenen

Eine Lambda-Ebene ist ein ZIP-Dateiarchiv mit ergänzendem Code oder ergänzenden Daten. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien.

Die Verwendung von Ebenen ermöglicht Folgendes:

- Verringern der Größe Ihrer Bereitstellungspakete: Platzieren Sie Ihre Funktionsabhängigkeiten in einer Ebene, anstatt sie zusammen mit Ihrem Funktionscode in Ihr Bereitstellungspaket einzuschließen. So bleiben Bereitstellungspakete klein und übersichtlich.
- Trennen von grundlegender Funktionslogik und Abhängigkeiten: Mit Ebenen können Sie Ihre Funktionsabhängigkeiten unabhängig von Ihrem Funktionscode aktualisieren (und umgekehrt). Dies trägt zur Trennung von Belangen bei und hilft Ihnen dabei, sich auf Ihre Funktionslogik zu konzentrieren.
- Verwenden von Abhängigkeiten für mehrere Funktionen: Erstellte Ebenen können auf eine beliebige Anzahl von Funktionen in Ihrem Konto angewendet werden. Ohne Ebenen müssen die gleichen Abhängigkeiten in jedes einzelne Bereitstellungspaket eingefügt werden.
- Verwenden des Code-Editors der Lambda-Konsole: Der Code-Editor ist ein praktisches Tool zum schnellen Testen kleinerer Funktionscode-Aktualisierungen. Sie können den Editor jedoch nicht verwenden, wenn Ihr Bereitstellungspaket zu groß ist. Die Verwendung von Ebenen verringert die Paketgröße und kann die Nutzung des Code-Editors ermöglichen.

Das folgende Diagramm veranschaulicht die allgemeinen architektonischen Unterschiede zwischen zwei Funktionen mit gemeinsamen Abhängigkeiten. Bei einer Variante werden Lambda-Ebenen verwendet, bei der anderen nicht.



Wenn Sie einer Funktion eine Ebene hinzufügen, extrahiert Lambda die Inhalte der Ebene in das Verzeichnis `/opt` in der Ausführungsumgebung Ihrer Funktion. Alle nativ unterstützten Lambda-Laufzeiten enthalten Pfade zu spezifischen Verzeichnissen innerhalb des Verzeichnisses `/opt`. Dadurch erhält die Funktion Zugriff auf Ihre Ebeneninhalte. Weitere Informationen zu diesen spezifischen Pfaden und zum richtigen Verpacken Ihrer Ebenen finden Sie unter the section called “Verpacken von Ebenen”.

Sie können pro Funktion bis zu fünf Ebenen einschließen. Ebenen können zudem nur mit Lambda-Funktionen verwendet werden, die als ZIP-Dateiarchiv bereitgestellt werden. Bei als Container-Image

definierten Funktionen werden Ihre bevorzugte Laufzeit und alle Codeabhängigkeiten beim Erstellen des Container-Images verpackt. Weitere Informationen finden Sie im AWS Compute-Blog unter Arbeiten mit Lambda-Layern und Erweiterungen in Container-Images.

Themen

Verwenden von Ebenen

Zum Erstellen einer Ebene müssen Sie Ihre Abhängigkeiten in einer ZIP-Datei verpacken – ähnlich wie beim Erstellen eines normalen Bereitstellungspakets. Genauer gesagt umfasst der allgemeine Prozess der Erstellung und Verwendung von Ebenen die drei folgenden Schritte:

- Verpacken Sie zuerst Ihren Ebeneninhalt. Erstellen Sie also ein ZIP-Dateiarchiv. Weitere Informationen finden Sie unter the section called “Verpacken von Ebenen”.
- Erstellen Sie als Nächstes die Ebene in Lambda. Weitere Informationen finden Sie unter the section called “Erstellen und Löschen von Ebenen”.
- Fügen Sie die Ebene Ihren Funktionen hinzu. Weitere Informationen finden Sie unter the section called “Hinzufügen von Ebenen”.

Ebenen und Ebenenversionen

Eine Ebenenversion ist eine unveränderliche Momentaufnahme einer spezifischen Version einer Ebene. Wenn Sie eine neue Ebene erstellen, erstellt Lambda eine neue Ebenenversion mit der Versionsnummer 1. Bei jeder Veröffentlichung einer Aktualisierung für die Ebene erhöht Lambda die Versionsnummer und erstellt eine neue Ebenenversion.

Jede Ebenenversion wird durch einen eindeutigen Amazon-Ressourcennamen (ARN) identifiziert. Beim Hinzufügen einer Ebene zur Funktion muss die exakte Ebenenversion angegeben werden, die Sie verwenden möchten.

Verpacken Ihres Ebeneninhalts

Eine Lambda-Ebene ist ein ZIP-Dateiarchiv mit ergänzendem Code oder ergänzenden Daten. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien.

In diesem Abschnitt erfahren Sie, wie Sie Ihren Ebeneninhalt ordnungsgemäß verpacken. Weitere konzeptionelle Informationen zu Ebenen sowie dazu, warum Sie ggf. welche verwenden sollten, finden Sie unter Lambda-Ebenen.

Der erste Schritt beim Erstellen einer Ebene besteht darin, den gesamten Ebeneninhalt in einem ZIP-Dateiarchiv zu bündeln. Da Lambda-Funktionen unter Amazon Linux ausgeführt werden, muss Ihr Ebeneninhalt in einer Linux-Umgebung kompiliert und erstellt werden können.

Um sicherzustellen, dass Ihr Layer-Inhalt in einer Linux-Umgebung ordnungsgemäß funktioniert, empfehlen wir, Ihren Layer-Inhalt mit einem Tool wie Docker oder AWS Cloud9zu erstellen. AWS Cloud9 ist eine cloudbasierte integrierte Entwicklungsumgebung (IDE), die integrierten Zugriff auf einen Linux-Server zum Ausführen und Testen von Code bietet. Weitere Informationen finden Sie im AWS -Computing-Blog unter Verwenden von Lambda-Ebenen zur Vereinfachung Ihres Entwicklungsprozesses.

Themen

- Ebenenpfade für jede Lambda-Laufzeit

Ebenenpfade für jede Lambda-Laufzeit

Wenn Sie einer Funktion eine Ebene hinzufügen, lädt Lambda den Ebeneninhalt in das Verzeichnis `/opt` der Ausführungsumgebung. Für jede Lambda-Laufzeit enthält die Variable `PATH` bereits spezifische Ordnerpfade innerhalb des Verzeichnisses `/opt`. Um sicherzustellen, dass die `PATH` Variable Ihren Layer-Inhalt aufnimmt, sollte Ihre Layer-.zip-Datei ihre Abhängigkeiten in den folgenden Ordnerpfaden haben:

Ebenenpfade für jede Lambda-Laufzeit

Laufzeit	Pfad
Node.js	`nodejs/node_modules`
	`nodejs/node14/node_modules` (`NODE_PATH`)

Laufzeit	Pfad
	`nodejs/node16/node_modules` (`NODE_PATH`)
	`nodejs/node18/node_modules` (`NODE_PATH`)
Python	`python`
	`python/lib/` *`python3.x`* `/site-packages` (Site-Verzeichnisse)
Java	`java/lib` (`CLASSPATH`)
Ruby	`ruby/gems/3.2.0` (`GEM_PATH`)
	`ruby/lib` (`RUBYLIB`)
Alle Laufzeiten	`bin` (`PATH`)
	`lib` (`LD_LIBRARY_PATH`)

Die folgenden Beispiele zeigen, wie Sie die Ordner im ZIP-Archiv Ihrer Ebene strukturieren können.

Node.js

Example Dateistruktur für das AWS X-Ray SDK für Node.js

```
xray-sdk.zip
# nodejs/node_modules/aws-xray-sdk
```

Python

Example Dateistruktur für die Requests-Bibliothek

```
layer_content.zip
# python
    # lib
        # python3.11
            # site-packages
                # requests
                # <other_dependencies> (i.e. dependencies of the requests package)
```

```
                # ...
```

Ruby

Example Dateistruktur für das JSON-Gem

```
json.zip
# ruby/gems/2.7.0/
               | build_info
               | cache
               | doc
               | extensions
               | gems
               | # json-2.1.0
               # specifications
                 # json-2.1.0.gemspec
```

Java

Example Dateistruktur für Jackson-JAR-Datei

```
layer_content.zip
# java
    # lib
        # jackson-core-2.17.0.jar
        # <other potential dependencies>
        # ...
```

All

Example Dateistruktur für jq-Bibliothek

```
jq.zip
# bin/jq
```

Sprachspezifische Anweisungen zum Verpacken, Erstellen und Hinzufügen einer Ebene finden Sie auf den folgenden Seiten:

- Python – the section called “Ebenen”
- Java — the section called “Ebenen”

Erstellen und Löschen von Ebenen in Lambda

Eine Lambda-Ebene ist ein ZIP-Dateiarchiv mit ergänzendem Code oder ergänzenden Daten. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien.

In diesem Abschnitt erfahren Sie, wie Sie Ebenen in Lambda erstellen und löschen. Weitere konzeptionelle Informationen zu Ebenen sowie dazu, warum Sie ggf. welche verwenden sollten, finden Sie unter Lambda-Ebenen.

Nach dem Verpacken Ihres Ebeneninhalts muss die Ebene in Lambda erstellt werden. In diesem Abschnitt wird nur gezeigt, wie Ebenen mithilfe der Lambda-Konsole oder mithilfe der Lambda-API erstellt und gelöscht werden. Eine Anleitung zum Erstellen einer Ebene mithilfe von AWS CloudFormation finden Sie unter the section called “Ebenen mit AWS CloudFormation”. Eine Anleitung zum Erstellen einer Ebene mithilfe von AWS Serverless Application Model (AWS SAM) finden Sie unter the section called “Ebenen mit AWS SAM”.

Themen

- Erstellen einer Ebene
- Löschen einer Ebenen-Version

Erstellen einer Ebene

Zum Erstellen einer Ebene können Sie das ZIP-Archiv entweder über Ihren lokalen Computer oder über Amazon Simple Storage Service (Amazon S3) hochladen. Lambda extrahiert den Ebenen-Inhalt in das `/opt`-Verzeichnis, wenn die Ausführungsumgebung für die Funktion eingerichtet wird.

Ebenen können eine oder mehrere Ebenenversionen haben. Wenn Sie eine Ebene erstellen, legt Lambda die Ebenen-Version auf Version 1 fest. Die Berechtigungen für eine bereits vorhandene Ebenenversion können jederzeit geändert werden. Um den Code zu aktualisieren oder andere Konfigurationsänderungen vorzunehmen, müssen Sie allerdings eine neue Version der Ebene erstellen.

So erstellen Sie eine Ebene (Konsole)

1. Öffnen Sie die Seite Ebenen der Lambda-Konsole.
2. Wählen Sie Create Layer (Ebene erstellen) aus.
3. Geben Sie unter Ebenen-Konfiguration unter Name einen Namen für Ihre Ebene ein.

4. (Optional) Geben Sie im Feld Description (Beschreibung) eine Beschreibung für Ihre Ebene ein.
5. Um Ihren Ebenen-Code upzuloaden, führen Sie einen der folgenden Schritte aus:
   - Um eine ZIP-Datei von Ihrem Computer upzuloaden, wählen Sie Eine .zip-Datei hochladen. Wählen Sie Upload, um Ihre lokale ZIP-Datei auszuwählen.
   - Um eine Datei aus Amazon S3 upzuloaden, wählen Sie Hochladen einer Datei aus Amazon S3 aus. Geben Sie dann für Amazon-S3-Link-URL einen Link zu der Datei ein.
6. (Optional) Für Kompatible Architekturen, wählen Sie einen Wert oder beide Werte aus. Weitere Informationen finden Sie unter the section called “Befehlssätze (ARM/x86)”.
7. (Optional) Wählen Sie unter Kompatible Laufzeiten die Laufzeiten aus, mit denen Ihre Ebene kompatibel ist.
8. (Optional) Für License (Lizenz) geben Sie alle erforderlichen Lizenzinformationen ein.
9. Wählen Sie Erstellen.

Alternativ können Sie auch die PublishLayerVersion-API verwenden, um eine Ebene zu erstellen. Sie können beispielsweise den AWS Command Line Interface (CLI)-Befehl `publish-layer-version` mit Angaben für Name, Beschreibung und ZIP-Dateiarchiv verwenden. Die Parameter für Lizenzinformationen, kompatible Laufzeiten und kompatible Architektur sind optional.

```
aws lambda publish-layer-version --layer-name my-layer \
    --description "My layer" \
    --license-info "MIT" \
    --zip-file fileb://layer.zip \
    --compatible-runtimes python3.10 python3.11 \
    --compatible-architectures "arm64" "x86_64"
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "Content": {
        "Location": "https://awslambda-us-east-2-layers.s3.us-east-2.amazonaws.com/
snapshots/123456789012/my-layer-4aaa2fbb-ff77-4b0a-ad92-5b78a716a96a?
versionId=27iWyA73cCAYqyH...",
        "CodeSha256": "tv9jJO+rPbXUUXuRKi7CwHzKtLDkDRJLB3cC3Z/ouXo=",
        "CodeSize": 169
    },
    "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
    "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:1",
    "Description": "My layer",
```

```
    "CreatedDate": "2023-11-14T23:03:52.894+0000",
    "Version": 1,
    "CompatibleArchitectures": [
        "arm64",
        "x86_64"
     ],
    "LicenseInfo": "MIT",
    "CompatibleRuntimes": [
        "python3.10",
        "python3.11"
    ]
}
```

Mit jedem Aufruf von `publish-layer-version` wird eine neue Version der Ebene erstellt.

Löschen einer Ebenen-Version

Um eine Ebenenversion zu löschen, verwenden Sie die DeleteLayerVersion-API. Sie können beispielsweise den CLI-Befehl `delete-layer-version` mit Angaben für Ebenenname und Ebenenversion verwenden.

```
aws lambda delete-layer-version --layer-name my-layer --version-number 1
```

Wenn Sie eine Ebenenversion löschen, können Sie keine Lambda-Funktionen mehr für deren Verwendung konfigurieren. Funktionen, die diese Version bereits vorhanden, können jedoch weiterhin darauf zugreifen. Außerdem werden Versionsnummern für einen Ebenennamen nie von Lambda wiederverwendet.

Hinzufügen von Ebenen zu Funktionen

Eine Lambda-Ebene ist ein ZIP-Dateiarchiv mit ergänzendem Code oder ergänzenden Daten. Ebenen enthalten üblicherweise Bibliotheksabhängigkeiten, eine benutzerdefinierte Laufzeit oder Konfigurationsdateien.

In diesem Abschnitt erfahren Sie, wie Sie einer Lambda-Funktion eine Ebene hinzufügen. Weitere konzeptionelle Informationen zu Ebenen sowie dazu, warum Sie ggf. welche verwenden sollten, finden Sie unter Lambda-Ebenen.

Bevor Sie eine Lambda-Funktion für die Verwendung einer Ebene konfigurieren können, ist Folgendes erforderlich:

- Verpacken Ihres Ebeneninhalts
- Erstellen einer Ebene in Lambda
- Stellen Sie sicher, dass Sie über die Berechtigung zum Aufrufen der GetLayerVersion API auf der Ebenenversion verfügen. Für Funktionen in Ihrem AWS-Konto-Konto muss diese Berechtigung in Ihrer Benutzerrichtlinie enthalten sein. Um eine Ebene in einem anderen Konto zu verwenden, muss der Eigentümer des anderen Kontos Ihrem Konto die Berechtigung in einer ressourcenbasierten Richtlinie erteilen. Beispiele finden Sie unter the section called “Gewähren des Ebenenzugriffs für andere Konten”.

Sie können bis zu fünf Ebenen zu einer Lambda-Funktion hinzufügen. Die entpackte Gesamtgröße der Funktion und aller Ebenen darf das Größenlimit des entpackten Bereitstellungspakets von 250 MB nicht überschreiten. Weitere Informationen finden Sie unter Lambda-Kontingente.

Ihre Funktionen können eine beliebige Ebenenversion, die Sie bereits hinzugefügt haben, weiterhin nutzen, auch wenn diese Ebenenversion gelöscht wurde oder Ihnen die Zugriffsberechtigung für die Ebene entzogen wurde. Sie können jedoch keine neue Funktion erstellen, die eine Version einer gelöschten Ebene verwendet.

> **Note**
>
> Achten Sie darauf, dass die Ebenen, die Sie einer Funktion hinzufügen, mit der Laufzeit und der Befehlssatzarchitektur der Funktion kompatibel sind.

So fügen Sie einer Funktion eine Ebene hinzu (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die zu konfigurierende Funktion aus.
3. Wählen Sie unter Ebenen die Option Ebene hinzufügen
4. Wählen Sie unter Ebene auswählen eine Ebenenquelle aus:

    a. Wählen Sie für die Ebenenquelle AWS-Ebenen oder Benutzerdefinierte Ebenen eine Ebene aus dem Pull-Down-Menü aus. UNDERVersion, wählen Sie eine Ebenenversion aus dem Pulldown-Menü aus.

    b. Geben Sie für die Ebenenquelle ARN angeben einen ARN in das Textfeld ein und wählen Sie anschließend Überprüfen aus. Wählen Sie dann Hinzufügen aus.

Die Reihenfolge, in der Sie die Ebenen hinzufügen, ist die Reihenfolge, in der Lambda den Ebeneninhalt in der Ausführungsumgebung zusammenführt. Sie können die Reihenfolge für Zusammenführungen der Layers mit der -Konsole ändern.

So aktualisieren Sie die Zusammenführungsreihenfolge von Ebenen für Ihre Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie die zu konfigurierende Funktion aus.
3. Wählen Sie unter Ebenen die Option Bearbeiten
4. Wählen Sie eine der Ebenen aus.
5. Klicken Sie aufFrüher MergeoderSpäter Zusammenführungenum die Reihenfolge der Ebenen anzupassen.
6. Wählen Sie Speichern.

Ebenen werden versioniert. Der Inhalt jeder Ebenenversion ist unveränderlich. Der Besitzer einer Ebene kann neue Ebenenversionen veröffentlichen, um aktualisierte Inhalte bereitzustellen.
Sie können die Konsole verwenden, um die mit Ihren Funktionen verknüpfte Ebenenversion zu aktualisieren.

So aktualisieren Sie Ebenenversionen für Ihre Funktion (Konsole)

1. Öffnen Sie die Seite Ebenen der Lambda-Konsole.
2. Wählen Sie die Ebene aus, für die Sie die Version aktualisieren möchten.

3. Wählen Sie die Registerkarte Funktionen mit dieser Version aus.
4. Wählen Sie die Funktionen aus, die Sie ändern möchten, und wählen Sie anschließend Bearbeiten aus.
5. Wählen Sie unter Ebenenversion die Ebenenversion aus, zu der Sie wechseln möchten.
6. Klicken Sie auf Funktionen aktualisieren.

Die Ebenenversionen von Funktionen kann nicht über AWS-Konten hinweg aktualisiert werden.

Themen

Zugriff auf Ebeneninhalte von Ihrer Funktion

Wenn Ihre Lambda-Funktion Ebenen enthält, extrahiert Lambda die Ebeneninhalte in das Verzeichnis `/opt` in der Ausführungsumgebung der Funktion. Lambda extrahiert die Schichten in der von der Funktion aufgeführten Reihenfolge (niedrig bis hoch). Lambda führt Ordner mit dem gleichen Namen zusammen. Wenn dieselbe Datei in mehreren Ebenen angezeigt wird, verwendet die Funktion die Version in der letzten extrahierten Ebene.

Jede Lambda-Laufzeit fügt der Variablen `PATH` spezifische `/opt`-Verzeichnisordner hinzu. Ihr Funktionscode kann auf den Ebeneninhalt zugreifen, ohne den Pfad angeben zu müssen. Weitere Informationen zu Pfadeinstellungen in der Lambda-Ausführungsumgebung finden Sie unter the section called “Definierte Laufzeitumgebungsvariablen”.

Informationen dazu, wo Sie Ihre Bibliotheken beim Erstellen einer Ebene einschließen müssen, finden Sie unter the section called “Ebenenpfade für jede Lambda-Laufzeit”.

Bei Verwendung einer Node.js- oder Python-Laufzeit können Sie den integrierten Code-Editor in der Lambda-Konsole verwenden. Es sollte möglich sein, jede beliebige Bibliothek zu importieren, die Sie der aktuellen Funktion als Ebene hinzugefügt haben.

Suche nach Ebeneninformationen

Verwenden Sie die -ListLayersAPI, um Ebenen in Ihrem Konto zu finden, die mit der Laufzeit Ihrer Funktion kompatibel sind. Sie können z. B. den folgenden AWS Command Line Interface (CLI)-Befehl vom Typ `list-layers` verwenden:

```
aws lambda list-layers --compatible-runtime python3.9
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "Layers": [
        {
            "LayerName": "my-layer",
            "LayerArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer",
            "LatestMatchingVersion": {
                "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
                "Version": 2,
                "Description": "My layer",
                "CreatedDate": "2023-11-15T00:37:46.592+0000",
                "CompatibleRuntimes": [
                    "python3.9",
                    "python3.10",
                    "python3.11",
                ]
            }
        }
    ]
}
```

Wenn Sie alle Ebenen in Ihrem Konto auflisten möchten, lassen Sie die Option `--compatible-runtime` weg. Die Antwortdetails enthalten jeweils die neueste Version der einzelnen Ebenen.

Sie können auch die neueste Version einer Ebene mit der ListLayerVersions-API abrufen. Sie können z. B. den folgenden CLI-Befehl vom Typ `list-layer-versions` verwenden:

```
aws lambda list-layer-versions --layer-name my-layer
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
{
    "LayerVersions": [
        {
            "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:2",
            "Version": 2,
```

```
            "Description": "My layer",
            "CreatedDate": "2023-11-15T00:37:46.592+0000",
            "CompatibleRuntimes": [
                "java11"
            ]
        },
        {
            "LayerVersionArn": "arn:aws:lambda:us-east-2:123456789012:layer:my-
layer:1",
            "Version": 1,
            "Description": "My layer",
            "CreatedDate": "2023-11-15T00:27:46.592+0000",
            "CompatibleRuntimes": [
                "java11"
            ]
        }
    ]
}
```

AWS CloudFormation Mit Ebenen verwenden

Sie können verwenden AWS CloudFormation , um eine Ebene zu erstellen und die Ebene mit Ihrer Lambda-Funktion zu verknüpfen. Die folgende Beispielvorlage erstellt eine Ebene mit dem Namen `my-lambda-layer` und fügt sie mithilfe der Eigenschaft Layers an die Lambda-Funktion an.

```
---
Description: CloudFormation Template for Lambda Function with Lambda Layer
Resources:
  MyLambdaLayer:
    Type: AWS::Lambda::LayerVersion
    Properties:
      LayerName: my-lambda-layer
      Description: My Lambda Layer
      Content:
        S3Bucket: DOC-EXAMPLE-BUCKET
        S3Key: my-layer.zip
      CompatibleRuntimes:
        - python3.9
        - python3.10
        - python3.11

  MyLambdaFunction:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: my-lambda-function
      Runtime: python3.9
      Handler: index.handler
      Timeout: 10
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
      Layers:
        - !Ref MyLambdaLayer
```

AWS SAM Mit Ebenen verwenden

Sie können das AWS Serverless Application Model (AWS SAM) verwenden, um die Erstellung von Ebenen in Ihrer Anwendung zu automatisieren. Der Ressourcentyp `AWS::Serverless::LayerVersion` erstellt eine Ebenenversion, auf die Sie in Ihrer Lambda-Funktionskonfiguration verweisen können.

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: AWS SAM Template for Lambda Function with Lambda Layer

Resources:
  MyLambdaLayer:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: my-lambda-layer
      Description: My Lambda Layer
      ContentUri: s3://DOC-EXAMPLE-BUCKET/my-layer.zip
      CompatibleRuntimes:
        - python3.9
        - python3.10
        - python3.11

  MyLambdaFunction:
    Type: AWS::Serverless::Function
    Properties:
      FunctionName: MyLambdaFunction
      Runtime: python3.9
      Handler: app.handler
      CodeUri: s3://DOC-EXAMPLE-BUCKET/my-function
      Layers:
        - !Ref MyLambdaLayer
```

Erweitern Sie Lambda-Funktionen mithilfe von Lambda-Erweiterungen

Sie können Lambda-Erweiterungen verwenden, um Ihre Lambda-Funktionen zu erweitern. Verwenden Sie beispielsweise Lambda-Erweiterungen, um Funktionen in Ihre bevorzugten Überwachungs-, Beobachtbarkeits-, Sicherheits- und Governance-Tools zu integrieren. Sie können aus einer Vielzahl von Tools wählen, die von AWS Lambda -Partnern bereitgestellt werden, oder Sie können Ihre eigenen Lambda-Erweiterungen erstellen.

Lambda unterstützt externe und interne Erweiterungen. Eine externe Erweiterung wird als unabhängiger Prozess in der Ausführungsumgebung ausgeführt und wird weiterhin ausgeführt, nachdem der Funktionsaufruf vollständig verarbeitet wurde. Da Erweiterungen als separate Prozesse ausgeführt werden, können Sie sie in einer anderen Sprache als die Funktion schreiben. Alle Lambda-Laufzeiten unterstützen Erweiterungen.

Eine interne Erweiterung wird als Teil des Laufzeitprozesses ausgeführt. Ihre Funktion greift auf interne Erweiterungen zu, indem Sie Wrapper-Skripte oder In-Process-Mechanismen wie verwende `JAVA_TOOL_OPTIONS`. Weitere Informationen finden Sie unter Ändern der Laufzeitumgebung.

Sie können einer Funktion Erweiterungen hinzufügen, indem Sie die Lambda-Konsole, die Dienste AWS Command Line Interface (AWS CLI) oder Infrastructure as Code (IaC) und Tools wie AWS CloudFormation, AWS Serverless Application Model (AWS SAM) und Terraform verwenden.

Ihnen wird die Ausführungszeit berechnet, die von der Erweiterung verbraucht wird (in Schritten von 1 ms). Es fallen keine Kosten für die Installation eigener Erweiterungen an. Weitere Informationen zur Preisgestaltung für Erweiterungen finden Sie unter AWS Lambda -Preise. Preisinformationen zu Partnererweiterungen finden Sie auf den Websites dieser Partner. Eine Liste der offiziellen Partnererweiterungen finden Sie unter the section called “Partner für Erweiterungen”.

Ein Tutorial zu Erweiterungen und deren Verwendung mit Ihren Lambda-Funktionen finden Sie im AWS Lambda Extensions Workshop.

Themen

- AWS Lambda Partner für Erweiterungen
- Verwenden der Lambda Extensions API zum Erstellen von Erweiterungen
- Lambda-Telemetrie-API

Ausführungsumgebung

Lambda ruft Ihre Funktion in einer Ausführungsumgebung auf, die eine sichere und isolierte Laufzeitumgebung bereitstellt. Die Ausführungsumgebung verwaltet die Ressourcen, die zum Ausführen Ihrer Funktion erforderlich sind, und bietet Lebenszyklusunterstützung für die Laufzeit und die Erweiterungen der Funktion.

Der Lebenszyklus der Ausführungsumgebung umfasst die folgenden Phasen:

- **`Init`**: In dieser Phase erstellt oder hebt Lambda eine Ausführungsumgebung mit den konfigurierten Ressourcen auf, lädt den Code für die Funktion und alle Ebenen herunter, initialisiert alle Erweiterungen, initialisiert die Laufzeit und führt dann den Initialisierungscode der Funktion (der Code außerhalb des Haupthandlers) aus. Die Phase `Init` erfolgt entweder während des ersten Aufrufs oder vor Funktionsaufrufen, wenn Sie die bereitgestellte Parallelität aktiviert haben.

  Die `Init`-Phase ist in drei Unterphasen unterteilt: `Extension init`, `Runtime init` und `Function init`. Diese Unterphasen stellen sicher, dass alle Erweiterungen und die Laufzeit ihre Einrichtungs-Aufgaben abschließen, bevor der Funktionscode ausgeführt wird.

  Wenn Lambda SnapStart aktiviert ist, findet die `Init`-Phase statt, wenn Sie eine Funktionsversion veröffentlichen. Lambda speichert einen Snapshot des Arbeitsspeichers und des Festplattenzustands der initialisierten Ausführungsumgebung, speichert den verschlüsselten Snapshot und speichert ihn im Cache für den Zugriff mit geringer Latenz. Wenn Sie über einen `beforeCheckpoint`-Laufzeit-Hook verfügen, wird der Code am Ende der `Init`-Phase ausgeführt.
- **`Restore`**(SnapStart nur): Wenn Sie eine SnapStartFunktion zum ersten Mal aufrufen und die Funktion skaliert wird, nimmt Lambda neue Ausführungsumgebungen aus dem persistenten Snapshot wieder auf, anstatt die Funktion von Grund auf neu zu initialisieren. Wenn Sie über einen `afterRestore()`-Laufzeit-Hook verfügen, wird der Code am Ende der `Restore`-Phase ausgeführt. Die Dauer von `afterRestore()`-Laufzeit-Hooks wird Ihnen in Rechnung gestellt. Die Laufzeit (JVM) muss geladen werden und `afterRestore()`-Laufzeit-Hooks müssen innerhalb des Timeout-Limits(10 Sekunden) abgeschlossen werden. Andernfalls erhalten Sie

eine. SnapStartTimeoutException Wenn die `Restore`-Phase abgeschlossen ist, ruft Lambda den Funktionshandler (Invoke-Phase) auf.

- **`Invoke`**: In dieser Phase ruft Lambda den Funktionshandler auf. Nachdem die Funktion vollständig ausgeführt wurde, bereitet sich Lambda auf die Verarbeitung eines weiteren Funktionsaufrufs vor.
- **`Shutdown`**: Diese Phase wird ausgelöst, wenn die Lambda-Funktion für einen bestimmten Zeitraum keine Aufrufe empfängt. In dieser `Shutdown`-Phase fährt Lambda die Laufzeit herunter, warnt die Erweiterungen, damit sie sauber beendet werden können und entfernt dann die Umgebung. Lambda sendet ein `Shutdown`-Ereignis an jede Erweiterung, das der Erweiterung mitteilt, dass die Umgebung beendet wird.

Während der `Init`-Phase extrahiert Lambda Ebenen, die Erweiterungen enthalten, in das `/opt`-Verzeichnis in der Ausführungsumgebung. Lambda sucht im `/opt/extensions/`-Verzeichnis nach Erweiterungen, interpretiert jede Datei als ausführbaren Bootstrap zum Starten der Erweiterung und startet alle Erweiterungen parallel.

Auswirkungen auf Leistung und Ressourcen

Die Größe der Erweiterungen Ihrer Funktion zählt für die Größenbeschränkung des Bereitstellungspakets. Bei einem ZIP-Dateiarchiv darf die entpackte Gesamtgröße der Funktion und sämtlicher Erweiterungen das Limit des entpackten Bereitstellungspakets von 250 MB nicht überschreiten.

Erweiterungen können sich auf die Leistung Ihrer Funktion auswirken, da sie Funktionsressourcen wie CPU, Arbeitsspeicher und Speicher gemeinsam nutzen. Wenn eine Erweiterung beispielsweise rechenintensive Operationen ausführt, kann die Ausführungsdauer Ihrer Funktion erhöht werden.

Jede Erweiterung muss ihre Initialisierung abschließen, bevor Lambda die Funktion aufruft. Daher kann eine Erweiterung, die erhebliche Initialisierungszeit verbraucht, die Latenz des Funktionsaufrufs erhöhen.

Um die zusätzliche Zeit zu messen, die die Erweiterung nach der Funktionsausführung benötigt, können Sie die Funktionsmetrik `PostRuntimeExtensionsDuration` verwenden. Um die Zunahme des verwendeten Speichers zu messen, können Sie die `MaxMemoryUsed`-Metrik verwenden. Um die Auswirkungen einer bestimmten Erweiterung zu verstehen, können Sie verschiedene Versionen Ihrer Funktionen nebeneinander ausführen.

Berechtigungen

Erweiterungen haben Zugriff auf die gleichen Ressourcen wie Funktionen. Da Erweiterungen in derselben Umgebung wie die Funktion ausgeführt werden, werden Berechtigungen von der Funktion und der Erweiterung gemeinsam genutzt.

Für ein ZIP-Dateiarchiv können Sie eine AWS CloudFormation Vorlage erstellen, um das Anhängen derselben Erweiterungskonfiguration — einschließlich AWS Identity and Access Management (IAM-) Berechtigungen — an mehrere Funktionen zu vereinfachen.

Konfigurieren von Lambda-Erweiterungen

Konfigurieren von Erweiterungen (ZIP-Dateiarchiv)

Sie können Ihrer Funktion eine Erweiterung als Lambda-Ebene hinzufügen. Mithilfe von Ebenen können Sie Erweiterungen in Ihrer Organisation oder in der gesamten Lambda-Entwicklercommunity freigeben. Sie können einer Ebene eine oder mehrere Erweiterungen hinzufügen. Sie können bis zu 10 Erweiterungen für eine Funktion registrieren.

Sie fügen die Erweiterung zu Ihrer Funktion hinzu, indem Sie dieselbe Methode verwenden wie für jede Ebene. Weitere Informationen finden Sie unter Lambda-Ebenen.

Hinzufügen einer Erweiterung zu Ihrer Funktion (Konsole)

1. Öffnen Sie die Seite Funktionen der Lambda-Konsole.
2. Wählen Sie eine Funktion aus.
3. Wählen Sie die Registerkarte Code aus, falls sie noch nicht ausgewählt ist.
4. Wählen Sie unter Ebenen die Option Bearbeiten aus.
5. Geben Sie unter Choose a layer (Ebene auswählen) Specify an ARN (Einen ARN angeben).
6. Geben Sie unter Specify an ARN (Einen ARN angeben), den Amazon-Ressourcennamen (ARN) einer Erweiterungsebene ein.
7. Wählen Sie Add aus.

Verwenden von Erweiterungen in Container-Images

Sie können Ihrem Container-Image Erweiterungen hinzufügen. Die Container-Image-Einstellung ENTRYPOINT gibt den Hauptprozess für die Funktion an. Konfigurieren Sie die Einstellung ENTRYPOINT im Dockerfile oder als Überschreibung in der Funktionskonfiguration.

Sie können mehrere Prozesse in einem Container ausführen. Lambda verwaltet den Lebenszyklus des Hauptprozesses und aller zusätzlichen Prozesse. Lambda verwendet die Erweiterungs-API, um den Erweiterungslebenszyklus zu verwalten.

Beispiel: Hinzufügen einer externen Erweiterung

Eine externe Erweiterung wird in einem separaten Prozess von der Lambda-Funktion ausgeführt. Lambda startet einen Prozess für jede Erweiterung im `/opt/extensions/`-Verzeichnis. Lambda

verwendet die Erweiterungs-API, um den Erweiterungslebenszyklus zu verwalten. Nachdem die Funktion bis zum Abschluss ausgeführt wurde, sendet Lambda ein `Shutdown`-Ereignis an jede externe Erweiterung.

Example Hinzufügen einer externen Erweiterung zu einem Python-Basis-Image

```
FROM public.ecr.aws/lambda/python:3.11

# Copy and install the app
COPY /app /app
WORKDIR /app
RUN pip install -r requirements.txt

# Add an extension from the local directory into /opt
ADD my-extension.zip /opt
CMD python ./my-function.py
```

Nächste Schritte

Um mehr über Erweiterungen zu erfahren, empfehlen wir die folgenden Ressourcen:

- Ein grundlegendes Arbeitsbeispiel finden Sie unter Erweiterungen erstellen für AWS Lambda im AWS-Compute-Blog.
- Informationen zu Erweiterungen, die AWS Lambda-Partner bereitstellen, finden Sie unter Einführung von AWS Lambda-Erweiterungen im AWS Compute Blog.
- Informationen zum Anzeigen verfügbarer Beispielerweiterungen und Wrapper-Skripte finden Sie unter AWS Lambda Erweiterungen im AWS Samples- GitHub Repository.

AWS Lambda Partner für Erweiterungen

AWS Lambda hat in Zusammenarbeit mit mehreren Drittanbieter-Entitäten Erweiterungen zur Integration in Ihre Lambda-Funktionen bereitgestellt. In der folgenden Liste werden Erweiterungen von Drittanbietern aufgeführt, die Sie jederzeit verwenden können.

- AppDynamics – Bietet die automatische Instrumentierung von Node.js- oder Python-Lambda-Funktionen und bietet Sichtbarkeit und Warnungen zur Funktionsleistung.
- Check Point CloudGuard – Eine erweiterungsbasierte Laufzeitlösung, die vollständige Lebenszyklus-Sicherheit für Serverless-Anwendungen bietet.
- Datadog – Bietet umfassende Echtzeit-Transparenz für Ihre Serverless-Anwendungen durch die Verwendung von Metriken, Nachverfolgungen und Protokollen.
- Dynatrace – Bietet Einblick in Nachverfolgungen und Metriken und nutzt KI für die automatisierte Fehlererkennung und Ursachenanalyse über den gesamten Anwendungs-Stack.
- Elastic – Bietet Application Performance Monitoring (APM) zur Identifizierung und Behebung von Ursachenproblemen mithilfe korrelierter Traces, Metriken und Logs.
- Epsagon – Hört sich Aufrufereignisse an, speichert Nachverfolgungen und sendet sie parallel an Lambda-Funktionsausführungen.
- Fastly – Schützt Ihre Lambda-Funktionen vor verdächtigen Aktivitäten wie Angriffen im Injektionsstil, Kontoübernahme durch Ausfüllen von Anmeldeinformationen, böswilligen Bots und API-Missbrauch.
- HashiCorp Vault – Verwaltet Geheimnisse und stellt sie Entwicklern zur Verwendung im Funktionscode zur Verfügung, ohne Funktionen vaultbewusst zu machen.
- Honeycomb – Beobachtbarkeits-Tool zum Debuggen Ihres App-Stacks.
- Lumigo – Profiliert Lambda-Funktionsaufrufe und sammelt Metriken zur Behebung von Problemen in Serverless- und Microservice-Umgebungen.
- New Relic – Läuft zusammen mit Lambda-Funktionen und sammelt, verbessert und transportiert Telemetriedaten automatisch zur einheitlichen Beobachtungsplattform von New Relic.
- Sedai – Eine autonome, auf KI/ML basierende Cloud-Management-Plattform, die eine kontinuierliche Optimierung für Cloud-Betriebsteams ermöglicht, um Cloud-Kosteneinsparungen, Leistung und Verfügbarkeit im großen Maßstab zu maximieren.
- Sentry – Diagnostizieren, beheben und optimieren Sie die Leistung von Lambda-Funktionen.
- Site24x7 – Erreichen Sie Echtzeit-Beobachtbarkeit in Ihren Lambda-Umgebungen

- Splunk – Sammelt hochauflösende Metriken mit niedriger Latenz für eine effiziente und effektive Überwachung von Lambda-Funktionen.
- Sumo Logic – Bietet Einblick in den Zustand und die Leistung von Serverless-Anwendungen.
- Thundra – Bietet asynchrone Telemetrieberichte wie Nachverfolgungen, Metriken und Protokolle.
- Salt-Sicherheit – Vereinfacht die Verwaltung des API-Status und die API-Sicherheit für Lambda-Funktionen durch automatisierte Einrichtung und Unterstützung für verschiedene Laufzeiten.

AWS Von verwaltete Erweiterungen

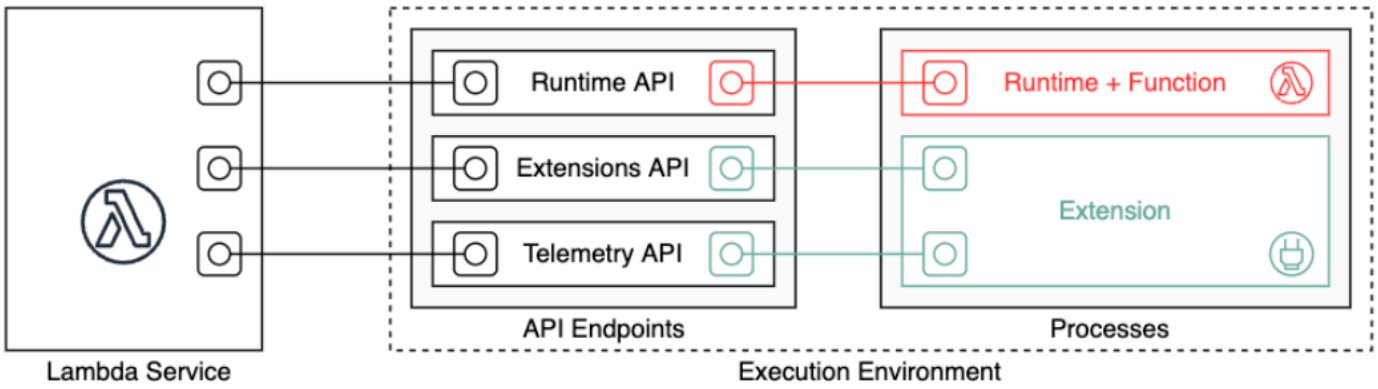
AWS bietet eigene verwaltete Erweiterungen, darunter:

- AWS AppConfig – Verwenden Sie Feature-Flags und dynamische Daten, um Ihre Lambda-Funktionen zu aktualisieren. Sie können diese Erweiterung auch verwenden, um andere dynamische Konfigurationen wie Ops-Drosselung und Optimierung zu aktualisieren.
- Amazon CodeGuru Profiler – Verbessert die Anwendungsleistung und senkt die Kosten, indem die teuerste Codezeile einer Anwendung lokalisiert und Empfehlungen zur Codeverbesserung bereitgestellt werden.
- CloudWatch Lambda Insights – Überwachen, beheben und optimieren Sie die Leistung Ihrer Lambda-Funktionen über automatisierte Dashboards.
- AWS Distro for OpenTelemetry (ADOT) – Ermöglicht Funktionen, Ablaufverfolgungsdaten an AWS Überwachungsservices wie AWS X-Ray und an Ziele OpenTelemetry wie Honeycomb und Lightstep zu senden.
- AWS Parameter und Secrets – Ermöglicht Kunden das sichere Abrufen von Parametern aus dem AWS Systems Manager Parameter Store und Secrets aus AWS Secrets Manager.

Weitere Erweiterungs-Beispiele und Demo-Projekte finden Sie unter Erweiterungen für AWS Lambda.

Verwenden der Lambda Extensions API zum Erstellen von Erweiterungen

Lambda-Funktionsautoren verwenden Erweiterungen, um Lambda in ihre bevorzugten Tools zur Überwachung, Beobachtbarkeit, Sicherheit und Governance zu integrieren. Funktionsautoren können Erweiterungen von AWS, AWS Partnern und Open-Source-Projekten verwenden. Weitere Informationen zur Verwendung von Erweiterungen finden Sie unter Einführung in AWS Lambda Erweiterungen im AWS Compute-Blog. In diesem Abschnitt wird beschrieben, wie Sie die Lambda-Erweiterungs-API, den Lebenszyklus der Lambda-Ausführungsumgebung und die Lambda-Erweiterungs-API-Referenz verwenden.



Als Erweiterungsautor können Sie die Lambda-Erweiterungs-API verwenden, um sich tief in die Lambda-Ausführungsumgebung zu integrieren. Ihre Erweiterung kann sich für Lebenszyklusereignisse für Funktions- und Ausführungsumgebung registrieren. Als Reaktion auf diese Ereignisse können Sie neue Prozesse starten, Logik ausführen und alle Phasen des Lambda-Lebenszyklus steuern und an ihnen teilnehmen: Initialisierung, Aufruf und Herunterfahren. Darüber hinaus können Sie die Laufzeitprotokoll-API verwenden, um einen Stream von Protokollen zu erhalten.

Eine Erweiterung wird als unabhängiger Prozess in der Ausführungsumgebung ausgeführt und kann weiterhin ausgeführt werden, nachdem der Funktionsaufruf vollständig verarbeitet wurde. Da Erweiterungen als Prozesse ausgeführt werden, können Sie diese in einer anderen Sprache als die Funktion schreiben. Es wird empfohlen, Erweiterungen mit einer kompilierten Sprache zu implementieren. In diesem Fall handelt es sich bei der Erweiterung um eine eigenständige Binärdatei, die mit unterstützten Laufzeiten kompatibel ist. Alle Lambda-Laufzeiten unterstützen Erweiterungen. Wenn Sie eine nicht kompilierte Sprache verwenden, stellen Sie sicher, dass Sie eine kompatible Laufzeit in die Erweiterung aufnehmen.

Lambda unterstützt auch interne Erweiterungen. Eine interne Erweiterung wird als separater Thread im Laufzeitprozess ausgeführt. Die Laufzeit startet und stoppt die interne Erweiterung. Eine alternative Möglichkeit zur Integration in die Lambda-Umgebung ist die Verwendung sprachspezifischer Umgebungsvariablen und Wrapper-Skripte. Sie können diese nutzen, um die Laufzeitumgebung zu konfigurieren und das Startup-Verhalten des Laufzeitprozesses zu verändern.

Sie können einer Funktion auf zwei Arten Erweiterungen hinzufügen. Bei einer Funktion, die als .zip-Dateiarchivbereitgestellt wird, stellen Sie Ihre Erweiterung als Ebenebereit. Bei einer Funktion, die als Container-Image definiert ist, fügen Sie die Erweiterungen Ihrem Container-Image hinzu.

> **Note**
>
> Beispiele für Erweiterungen und Wrapper-Skripte finden Sie unter AWS Lambda Erweiterungen im AWS GitHub Samples-Repository.

Themen

- Lebenszyklus der Lambda-Ausführungsumgebung
- Erweiterungs-API-Referenz

Lebenszyklus der Lambda-Ausführungsumgebung

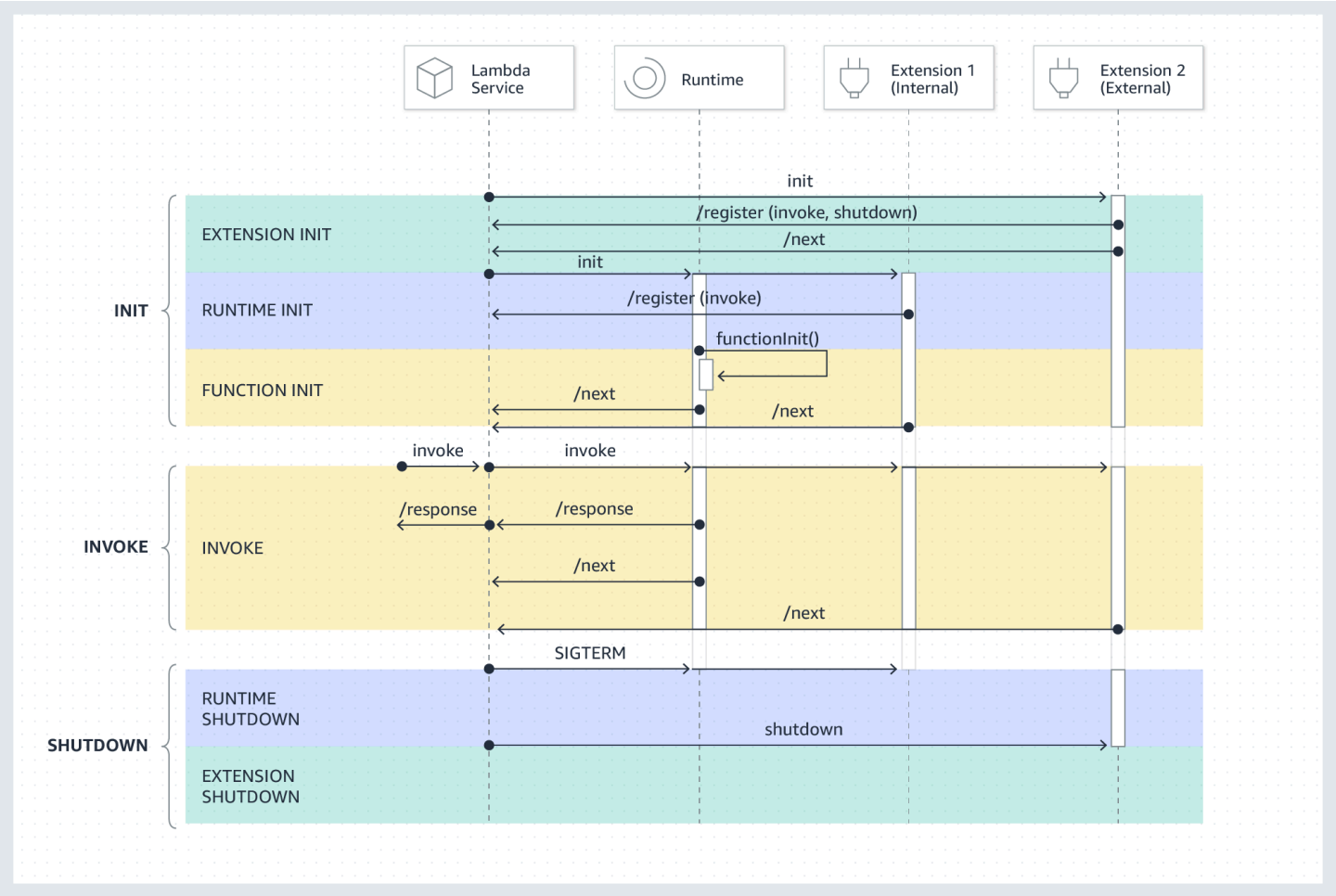
Der Lebenszyklus der Ausführungsumgebung umfasst die folgenden Phasen:

- **`Init`**: In dieser Phase erstellt oder hebt Lambda eine Ausführungsumgebung mit den konfigurierten Ressourcen auf, lädt den Code für die Funktion und alle Ebenen herunter, initialisiert alle Erweiterungen, initialisiert die Laufzeit und führt dann den Initialisierungscode der Funktion (der Code außerhalb des Haupthandlers) aus. Die Phase `Init` erfolgt entweder während des ersten Aufrufs oder vor Funktionsaufrufen, wenn Sie die bereitgestellte Parallelität aktiviert haben.

  Die `Init`-Phase ist in drei Unterphasen unterteilt: `Extension init`, `Runtime init` und `Function init`. Diese Unterphasen stellen sicher, dass alle Erweiterungen und die Laufzeit ihre Einrichtungs-Aufgaben abschließen, bevor der Funktionscode ausgeführt wird.
- **`Invoke`**: In dieser Phase ruft Lambda den Funktionshandler auf. Nachdem die Funktion vollständig ausgeführt wurde, bereitet sich Lambda auf die Verarbeitung eines weiteren Funktionsaufrufs vor.
- **`Shutdown`**: Diese Phase wird ausgelöst, wenn die Lambda-Funktion für einen bestimmten Zeitraum keine Aufrufe empfängt. In dieser `Shutdown`-Phase fährt Lambda die Laufzeit herunter,

warnt die Erweiterungen, damit sie sauber beendet werden können und entfernt dann die Umgebung. Lambda sendet ein `Shutdown`-Ereignis an jede Erweiterung, das der Erweiterung mitteilt, dass die Umgebung beendet wird.

Jede Phase beginnt mit einem Ereignis von Lambda zur Laufzeit und zu allen registrierten Erweiterungen. Die Laufzeit und jede Erweiterung zeigen den Abschluss durch Senden einer `Next`-API-Anfrage an. Lambda friert die Ausführungsumgebung ein, wenn jeder Prozess abgeschlossen ist und keine ausstehenden Ereignisse vorhanden sind.



Themen

- Init-Phase
- Invoke-Phase
- Shutdown-Phase
- Berechtigungen und Konfiguration

- Fehlerbehandlung
- Fehlerbehebung bei Erweiterungen

Init-Phase

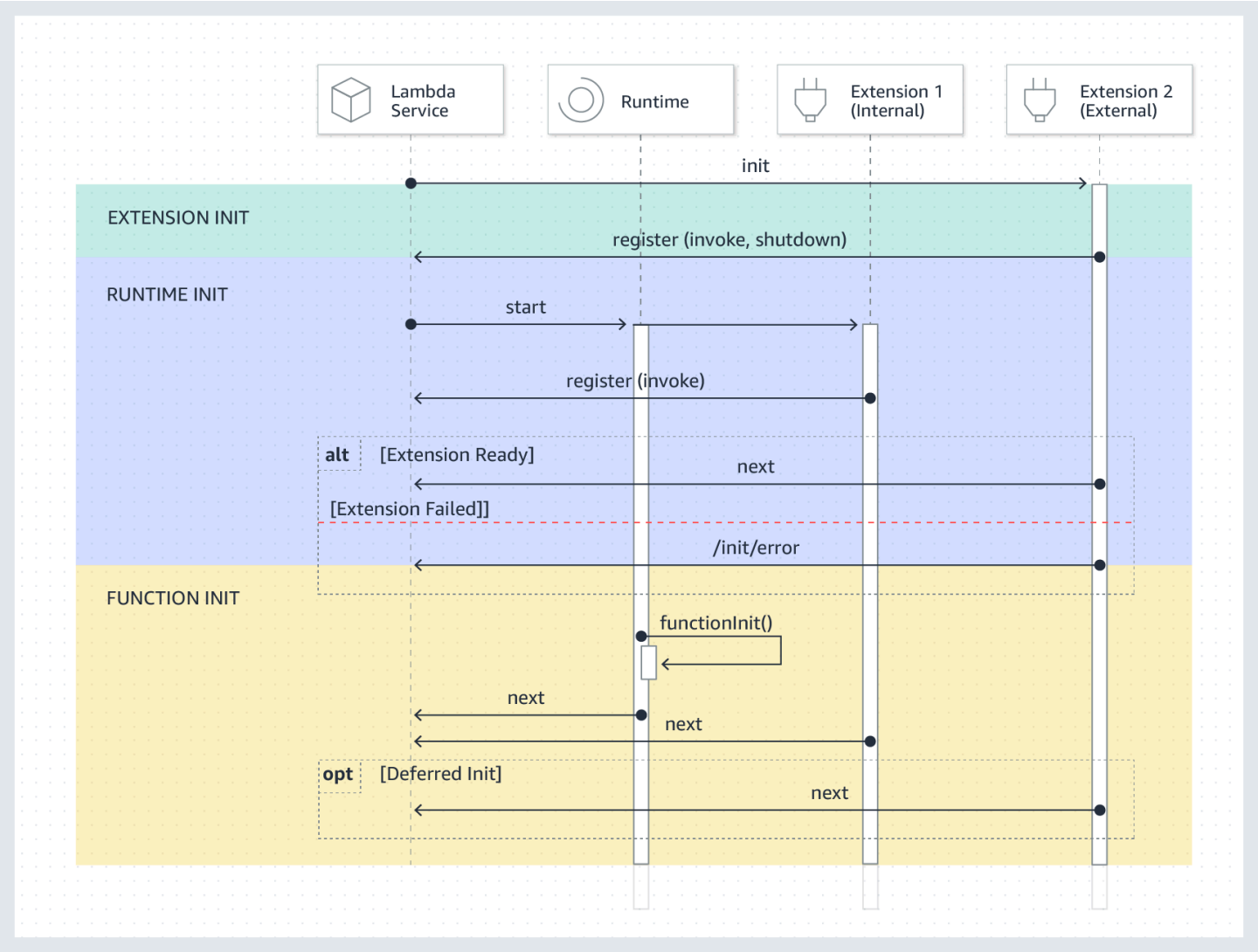
Während dieser `Extension init`-Phase muss sich jede Erweiterung bei Lambda registrieren, um Ereignisse zu empfangen. Lambda verwendet den vollständigen Dateinamen der Erweiterung, um zu überprüfen, ob die Erweiterung die Bootstrap-Sequenz abgeschlossen hat. Daher muss jeder `Register`-API-Aufruf den `Lambda-Extension-Name`-Header mit dem vollständigen Dateinamen der Erweiterung enthalten.

Sie können bis zu 10 Erweiterungen für eine Funktion registrieren. Dieses Limit wird durch den `Register`-API-Aufruf erzwungen.

Nachdem jede Erweiterung registriert ist, startet Lambda die `Runtime init`-Phase. Der Laufzeitprozess ruft `functionInit` auf, um die `Function init`-Phase zu starten.

Die `Init`-Phase wird nach der Laufzeit abgeschlossen und jede registrierte Erweiterung zeigt den Abschluss durch Senden einer `Next`-API-Anforderung an.

> **Note**
>
> Erweiterungen können ihre Initialisierung an jedem beliebigen Punkt in der `Init`-Phase abschließen.



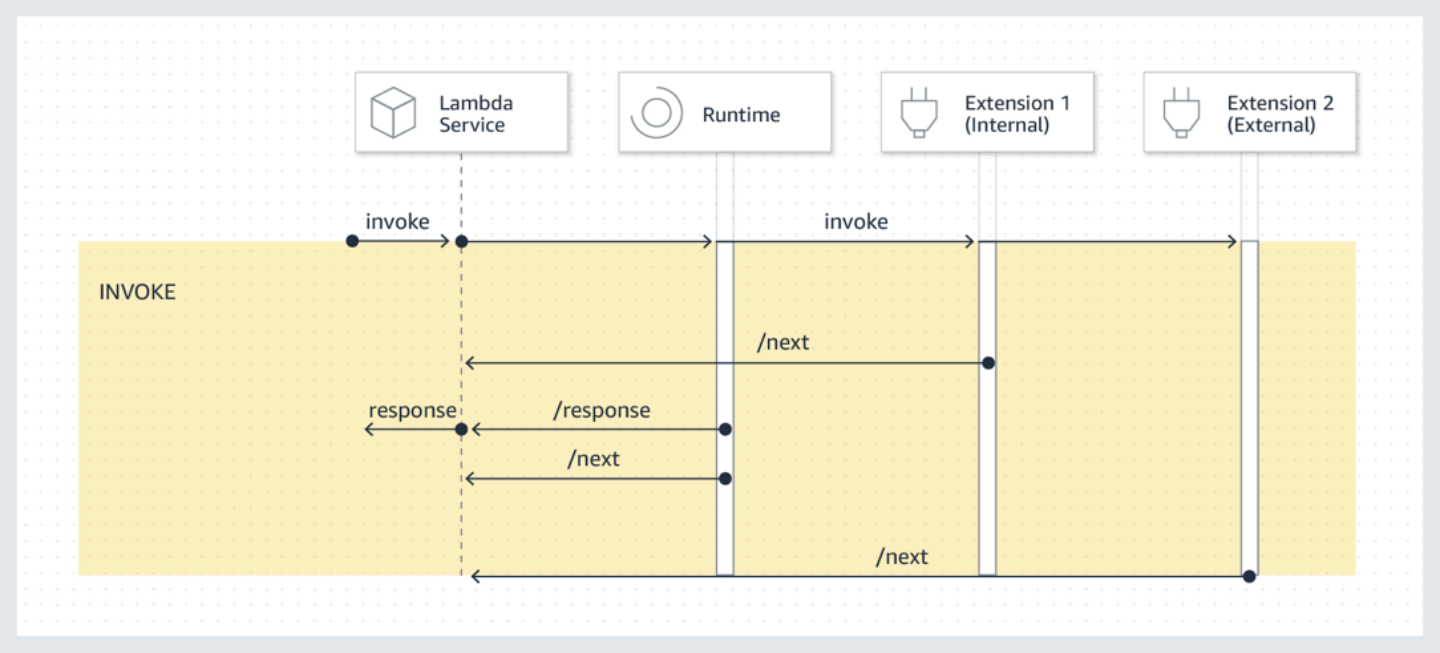
Invoke-Phase

Wenn eine Lambda-Funktion als Antwort auf eine `Next`-API-Anforderung aufgerufen wird, sendet Lambda ein `Invoke`-Ereignis an die Laufzeitumgebung und an jede Erweiterung, die für das `Invoke`-Ereignis registriert ist.

Während des Aufrufs werden externe Erweiterungen parallel zur Funktion ausgeführt. Sie werden auch weiter ausgeführt, nachdem die Funktion abgeschlossen ist. Auf diese Weise können Sie Diagnoseinformationen erfassen oder Protokolle, Metriken und Traces an einen Ort Ihrer Wahl senden.

Nachdem Erhalt der Funktionsantwort von der Laufzeitumgebung wird die Antwort von Lambda an den Client zurückgegeben, selbst wenn noch Erweiterungen ausgeführt werden.

Die `Invoke`-Phase endet nach der Laufzeit und alle Erweiterungen signalisieren durch Senden einer `Next`-API-Anforderung, dass sie ausgeführt wurden.



Ereignisnutzlast: Das Ereignis, das an die Laufzeit (und die Lambda-Funktion) gesendet wird, trägt die gesamte Anforderung, Header (z. B. `RequestId`) und Nutzlast. Das an jede Erweiterung gesendete Ereignis enthält Metadaten, die den Ereignisinhalt beschreiben. Dieses Lebenszyklusereignis umfasst den Typ des Ereignisses, die Zeit, zu der das Timeout der Funktion (`deadlineMs`), das `requestId`, die aufgerufene Funktion, den Amazon Resource Name (ARN) der aufgerufenen Funktion und die Tracing-Header.

Erweiterungen, die auf den Funktionsereigniskörper zugreifen möchten, können ein In-Laufzeit-SDK verwenden, das mit der Erweiterung kommuniziert. Funktionsentwickler verwenden das In-Laufzeit-SDK, um die Nutzlast an die Erweiterung zu senden, wenn die Funktion aufgerufen wird.

Hier ist ein Beispiel für eine Nutzlast:

```
{
    "eventType": "INVOKE",
    "deadlineMs": 676051,
    "requestId": "3da1f2dc-3222-475e-9205-e2e6c6318895",
    "invokedFunctionArn": "arn:aws:lambda:us-
east-1:123456789012:function:ExtensionTest",
    "tracing": {
        "type": "X-Amzn-Trace-Id",
```

```
        "value":
"Root=1-5f35ae12-0c0fec141ab77a00bc047aa2;Parent=2be948a625588e32;Sampled=1"
    }
}
```

Begrenzung der Dauer: Die Timeout-Einstellung der Funktion begrenzt die Dauer der gesamten `Invoke`-Phase. Wenn Sie beispielsweise die Zeitüberschreitung für die Funktion auf 360 Sekunden festlegen, müssen die Funktion und alle Erweiterungen innerhalb von 360 Sekunden abgeschlossen werden. Beachten Sie, dass es keine unabhängige Post-Invoke-Phase gibt. Die Dauer ist die Gesamtzeit, die Ihre Laufzeit und alle Aufrufe Ihrer Erweiterungen benötigen. Sie wird erst berechnet, wenn die Funktion und alle Erweiterungen vollständig ausgeführt wurden.

Performance impact and extension overhead (Leistungsauswirkungen und Erweiterungsoverhead): Erweiterungen können sich auf die Funktionsleistung auswirken. Als Autor einer Erweiterung haben Sie die Kontrolle über die Auswirkungen Ihrer Erweiterung auf die Leistung. Ein Beispiel: Eine Erweiterung führt rechenintensive Operationen aus. In diesem Fall könnten Sie feststellen, dass die Dauer des Aufrufs Ihrer Funktion zunimmt, da Erweiterung und Funktion sich CPU-Ressourcen teilen. Wenn Ihre Erweiterung umfangreiche Operationen ausführt, nachdem der Funktionsaufruf abgeschlossen ist, verlängert sich die Dauer des Funktionsaufrufs, da die `Invoke`-Phase fortgesetzt wird, bis alle Erweiterungen signalisieren, dass sie abgeschlossen sind.

> **Note**
>
> Lambda weist CPU-Leistung im Verhältnis zur Speichereinstellung der Funktion zu. Bei niedrigeren Speichereinstellungen wird möglicherweise eine erhöhte Ausführungs- und Initialisierungsdauer angezeigt, da die Funktions- und Erweiterungsprozesse um die gleichen CPU-Ressourcen konkurrieren. Erhöhen Sie die Speichereinstellung, um die Ausführungs- und Initialisierungsdauer zu reduzieren.

Um die Leistungsbeeinträchtigung zu identifizieren, die durch Erweiterungen in der `Invoke`-Phase verursacht wird, gibt Lambda die `PostRuntimeExtensionsDuration`-Metrik aus. Diese Metrik misst die kumulative Zeit, die zwischen der `Next`-Laufzeit-API-Anforderung und der letzten `Next`-Erweiterungs-API-Anforderung vergeht. Verwenden Sie die `MaxMemoryUsed`-Metrik, um die Zunahme des verwendeten Speichers zu messen. Weitere Informationen zu Funktionsmetriken finden Sie unter Arbeiten mit Lambda-Funktionsmetriken.

Funktionsentwickler können verschiedene Versionen ihrer Funktionen nebeneinander ausführen, um die Auswirkungen einer bestimmten Erweiterung zu verstehen. Wir empfehlen, dass

Erweiterungsautoren den erwarteten Ressourcenverbrauch veröffentlichen, um Funktionsentwicklern die Auswahl einer geeigneten Erweiterung zu erleichtern.

Shutdown-Phase

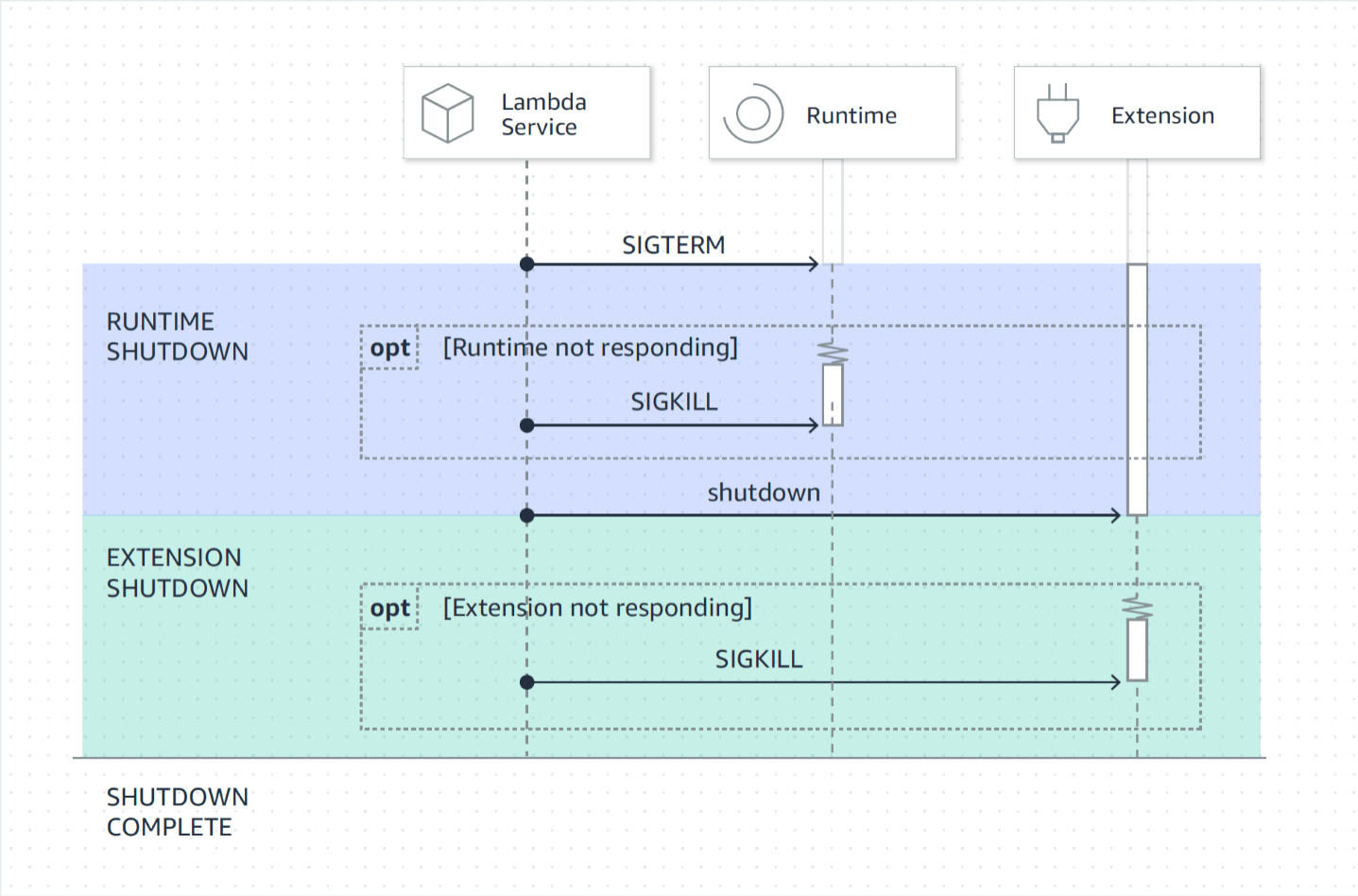
Wenn Lambda dabei ist, die Laufzeit zu beenden, sendet es ein `Shutdown` an die Laufzeitumgebung und dann an jede registrierte externe Erweiterung. Erweiterungen können diese Zeit für abschließende Bereinigungsaufgaben verwenden. Das `Shutdown`-Ereignis wird als Antwort auf eine `Next`-API-Anforderung gesendet.

Duration Limit (Begrenzung der Dauer): Die maximale Dauer der `Shutdown`-Phase hängt von der Konfiguration der registrierten Erweiterungen ab:

- 0 ms – Eine Funktion ohne registrierte Erweiterungen
- 500 ms – Eine Funktion mit einer registrierten internen Erweiterung
- 2.000 ms – Eine Funktion mit einer oder mehreren registrierten externen Erweiterungen

Für eine Funktion mit externen Erweiterungen reserviert Lambda bis zu 300 ms (500 ms für eine Laufzeit mit einer internen Erweiterung) für den Laufzeitprozess, um ein ordnungsgemäßes Abschalten durchführen zu können. Lambda weist den Rest der 2.000-ms-Grenze für das Herunterfahren externer Erweiterungen zu.

Wenn die Laufzeit oder eine Erweiterung nicht innerhalb des Limits auf das `Shutdown`-Ereignis reagiert, beendet Lambda den Prozess mit einem `SIGKILL`-Signal.



Event Payload (Ereignis-Nutzlast): Das `Shutdown`-Ereignis enthält den Grund für das Abschalten und die verbleibende Zeit in Millisekunden.

Das `shutdownReason` beinhaltet die folgenden Werte:

- SPINDOWN – Normale Abschaltung
- TIMEOUT – Zeitlimit abgelaufen
- FAILURE – Fehlerzustand, etwa ein `out-of-memory`-Ereignis

```
{
  "eventType": "SHUTDOWN",
  "shutdownReason": "reason for shutdown",
  "deadlineMs": "the time and date that the function times out in Unix time
 milliseconds"
}
```

Berechtigungen und Konfiguration

Erweiterungen werden in derselben Ausführungsumgebung wie die Lambda-Funktion ausgeführt. Erweiterungen teilen auch Ressourcen mit der Funktion, wie CPU, Arbeitsspeicher und `/tmp`-Datenträgerspeicher. Darüber hinaus verwenden Erweiterungen dieselbe AWS Identity and Access Management (IAM-) Rolle und denselben Sicherheitskontext wie die Funktion.

File system and network access permissions (Dateisystem- und Netzwerkzugriffsberechtigungen): Erweiterungen werden in demselben Dateisystem- und Netzwerk-Namespace wie die Funktionslaufzeit ausgeführt. Dies bedeutet, dass Erweiterungen mit dem zugehörigen Betriebssystem kompatibel sein müssen. Wenn für eine Erweiterung zusätzliche ausgehende Netzwerkverkehrsregeln erforderlich sind, müssen Sie diese Regeln auf die Funktionskonfiguration anwenden.

> **Note**
>
> Da das Funktionscode-Verzeichnis schreibgeschützt ist, können Erweiterungen den Funktionscode nicht ändern.

Environment variables (Umgebungsvariablen): Erweiterungen können auf die Umgebungsvariablen der Funktion zugreifen, mit Ausnahme der folgenden Variablen, die für den Laufzeitprozess spezifisch sind:

- `AWS_EXECUTION_ENV`
- `AWS_LAMBDA_LOG_GROUP_NAME`
- `AWS_LAMBDA_LOG_STREAM_NAME`
- `AWS_XRAY_CONTEXT_MISSING`
- `AWS_XRAY_DAEMON_ADDRESS`
- `LAMBDA_RUNTIME_DIR`
- `LAMBDA_TASK_ROOT`
- `_AWS_XRAY_DAEMON_ADDRESS`
- `_AWS_XRAY_DAEMON_PORT`

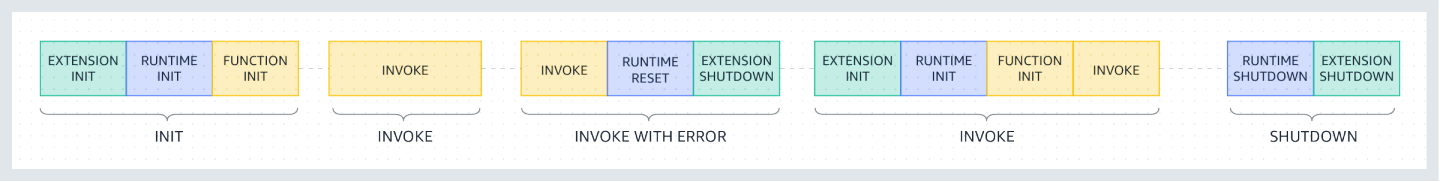
- `_HANDLER`

Fehlerbehandlung

Initialization failures (Initialisierungsfehler): Wenn eine Erweiterung fehlschlägt, startet Lambda die Ausführungsumgebung neu, um konsistentes Verhalten zu erzwingen und Fail Fast für Erweiterungen zu unterstützen. Für einige Kunden müssen die Erweiterungen auch geschäftskritische Anforderungen wie Protokollierung, Sicherheit, Governance und Telemetrieerfassung erfüllen.

Invoke failures (Aufruffehler) (z. B. kein Speicher mehr, Funktions-Timeout): Da Erweiterungen Ressourcen mit der Laufzeit gemeinsam nutzen, sind sie eventuell von Speichermangel betroffen. Wenn die Laufzeit ausfällt, nehmen alle Erweiterungen und die Laufzeit selbst an der `Shutdown`-Phase teil. Darüber hinaus wird die Laufzeitumgebung entweder automatisch als Teil des aktuellen Aufrufs oder über einen verzögerten Neuinitialisierungsmechanismus neu gestartet.

Wenn bei `Invoke` ein Fehler (z. B. eine Funktions-Zeitüberschreitung oder Laufzeitfehler) auftritt, führt der Lambda-Service einen Neustart durch. Der Reset verhält sich wie ein `Shutdown`-Ereignis. Zuerst beendet Lambda die Laufzeit und sendet dann ein `Shutdown`-Ereignis an jede registrierte externe Erweiterung. Das Ereignis enthält den Grund für das Abschalten. Wenn diese Umgebung für einen neuen Aufruf verwendet wird, werden die Erweiterung und die Laufzeit als Teil des nächsten Aufrufers neu initialisiert.



Eine ausführlichere Erläuterung des vorherigen Diagramms finden Sie unter Fehler während der Aufrufphase.

Erweiterungsprotokolle: Lambda sendet die Protokollausgabe von Erweiterungen an CloudWatch Logs. Lambda generiert auch ein zusätzliches Protokollereignis für jede Erweiterung während `Init`. Das Protokollereignis zeichnet den Namen und die Registrierungseinstellung (Ereignis, Konfiguration) bei Erfolg oder die Fehlerursache bei einem Fehler auf.

Fehlerbehebung bei Erweiterungen

- Wenn eine `Register`-Anforderung fehlschlägt, stellen Sie sicher, dass der `Lambda-Extension-Name`-Header im `Register`-API-Aufruf den vollständigen Dateinamen der Erweiterung enthält.

- Wenn die `Register`-Anforderung für eine interne Erweiterung fehlschlägt, stellen Sie sicher, dass sich die Anforderung nicht für das `Shutdown`-Ereignis registriert.

Erweiterungs-API-Referenz

Die OpenAPI-Spezifikation für die Erweiterungs-API Version 2020-01-01 finden Sie hier: extensions-api.zip

Sie können den Wert des API-Endpunkts aus der `AWS_LAMBDA_RUNTIME_API`-Umgebungsvariablen abrufen. Um eine `Register`-Anforderung zu senden, verwenden Sie das Präfix `2020-01-01/` vor jedem API-Pfad. Zum Beispiel:

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
```

API-Methoden

- Registrieren
- Next
- Init-Fehler
- Exit-Fehler

Registrieren

Während `Extension init` müssen sich alle Erweiterungen bei Lambda registrieren, um Ereignisse zu empfangen. Lambda verwendet den vollständigen Dateinamen der Erweiterung, um zu überprüfen, ob die Erweiterung die Bootstrap-Sequenz abgeschlossen hat. Daher muss jeder `Register`-API-Aufruf den `Lambda-Extension-Name`-Header mit dem vollständigen Dateinamen der Erweiterung enthalten.

Interne Erweiterungen werden vom Laufzeitprozess gestartet und gestoppt, sodass sie sich nicht für das `Shutdown`-Ereignis registrieren können.

Pfad – `/extension/register`

Methode – POST

Anfordern von Headern

- `Lambda-Extension-Name` – Der vollständige Dateiname der Erweiterung. Erforderlich: ja Typ: Zeichenkette
- `Lambda-Extension-Accept-Feature` – Verwenden Sie dies, um optionale Erweiterungsfunktionen bei der Registrierung anzugeben. Erforderlich: Nein. Typ: durch Kommas getrennte Zeichenfolge. Funktionen, die mit dieser Einstellung angegeben werden können:
  - `accountId` – Falls angegeben, enthält die Registrierungsantwort der Erweiterung die Konto-ID, die der Lambda-Funktion zugeordnet ist, für die Sie die Erweiterung registrieren.

Anfrage von Textparametern

- `events` – Array der Ereignisse, für die die Registrierung durchgeführt werden soll. Erforderlich: Nein Typ: Zeichenfolge-Array Gültige Zeichenfolgen: `INVOKE`, `SHUTDOWN`.

Antwort-Header

- `Lambda-Extension-Identifier` – Generierte eindeutige Agent-ID (UUID-Zeichenfolge), die für alle nachfolgenden Anforderungen erforderlich ist.

Antwortcodes

- 200 – Antworttext enthält den Funktionsnamen, die Funktionsversion und den Namen des Handlers.
- 400 – Ungültige Anfrage
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Erweiterung sollte umgehend beendet werden.

Example Beispielanfragetext

```
{
    'events': [ 'INVOKE', 'SHUTDOWN']
}
```

Example Beispielantworttext

```
{
```

```
    "functionName": "helloWorld",
    "functionVersion": "$LATEST",
    "handler": "lambda_function.lambda_handler"
}
```

Example Beispiel-Antworttext mit optionaler AccountID-Funktion

```
{
    "functionName": "helloWorld",
    "functionVersion": "$LATEST",
    "handler": "lambda_function.lambda_handler",
    "accountId": "123456789012"
}
```

Next

Erweiterungen senden eine `Next`-API-Anforderung für den Empfang des nächsten Ereignisses, bei dem es sich um ein `Invoke`-Ereignis oder ein `Shutdown`-Ereignis handeln kann. Der Antworttext enthält die Nutzlast, bei der es sich um ein JSON-Dokument handelt, das Ereignisdaten enthält.

Die Erweiterung sendet eine `Next`-API-Anforderung, um zu signalisieren, dass sie bereit ist, neue Ereignisse zu empfangen. Das ist ein blockierender Aufruf.

Legen Sie für den GET-Aufruf kein Timeout fest, da die Erweiterung für einen bestimmten Zeitraum angehalten werden kann, bis ein Ereignis zurückgegeben werden soll.

Pfad – `/extension/event/next`

Methode – GET

Anfordern von Headern

- `Lambda-Extension-Identifier` – Eindeutiger Bezeichner für die Erweiterung (UUID-Zeichenfolge). Erforderlich: ja Typ: UUID-Zeichenfolge

Antwort-Header

- `Lambda-Extension-Event-Identifier` – Eindeutiger Bezeichner für das Ereignis (UUID-Zeichenfolge).

Antwortcodes

- 200 – Die Antwort enthält Informationen über das nächste Ereignis (`EventInvoke` oder `EventShutdown`).
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Erweiterung sollte umgehend beendet werden.

Init-Fehler

Die Erweiterung verwendet diese Methode, um einen Initialisierungsfehler an Lambda zu melden. Rufen Sie sie auf, wenn die Erweiterung nach der Registrierung nicht initialisiert werden kann. Nachdem der Fehler von Lambda empfangen wurde, sind keine weiteren API-Aufrufe erfolgreich. Die Erweiterung sollte beendet werden, nachdem sie die Antwort von Lambda erhalten hat.

Pfad – `/extension/init/error`

Methode – POST

Anfordern von Headern

- `Lambda-Extension-Identifier` – Eindeutiger Bezeichner für die Erweiterung. Erforderlich: ja Typ: UUID-Zeichenfolge
- `Lambda-Extension-Function-Error-Type` – Der Fehlertyp, auf den die Erweiterung gestoßen ist. Erforderlich: ja Dieser Header besteht aus einem Zeichenfolgen-Wert. Lambda akzeptiert jede Zeichenfolge, aber wir empfehlen ein Format von <category.reason>. Beispielsweise:
  - Erweiterung. NoSuchHandler
  - Erweiterung.API gefunden KeyNot
  - Erweiterung. ConfigInvalid
  - Erweiterung. UnknownReason

Anfrage von Textparametern

- `ErrorRequest` – Informationen über den Fehler. Erforderlich: Nein

Dieses Feld ist ein JSON-Objekt mit der folgenden Struktur:

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Beachten Sie, dass Lambda jeden Wert für `errorType` akzeptiert.

Das folgende Beispiel zeigt eine Lambda-Funktionsfehlermeldung, in der die Funktion die im Aufruf bereitgestellten Ereignisdaten nicht analysieren konnte.

Example Funktionsfehler

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Antwortcodes

- 202 – Akzeptiert
- 400 – Ungültige Anfrage
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Erweiterung sollte umgehend beendet werden.

Exit-Fehler

Die Erweiterung verwendet diese Methode, um Lambda vor dem Beenden einen Fehler zu melden. Rufen Sie sie auf, wenn ein unerwarteter Fehler auftritt. Nachdem der Fehler von Lambda empfangen wurde, sind keine weiteren API-Aufrufe erfolgreich. Die Erweiterung sollte beendet werden, nachdem sie die Antwort von Lambda erhalten hat.

Pfad – `/extension/exit/error`

Methode – POST

Anfordern von Headern

- `Lambda-Extension-Identifier` – Eindeutiger Bezeichner für die Erweiterung. Erforderlich: ja Typ: UUID-Zeichenfolge
- `Lambda-Extension-Function-Error-Type` – Der Fehlertyp, auf den die Erweiterung gestoßen ist. Erforderlich: ja Dieser Header besteht aus einem Zeichenfolgen-Wert. Lambda akzeptiert jede Zeichenfolge, aber wir empfehlen ein Format von <category.reason>. Beispielsweise:
  - Erweiterung. NoSuchHandler
  - Erweiterung.API gefunden KeyNot
  - Erweiterung. ConfigInvalid
  - Erweiterung. UnknownReason

Anfrage von Textparametern

- `ErrorRequest` – Informationen über den Fehler. Erforderlich: Nein

Dieses Feld ist ein JSON-Objekt mit der folgenden Struktur:

```
{
      errorMessage: string (text description of the error),
      errorType: string,
      stackTrace: array of strings
}
```

Beachten Sie, dass Lambda jeden Wert für `errorType` akzeptiert.

Das folgende Beispiel zeigt eine Lambda-Funktionsfehlermeldung, in der die Funktion die im Aufruf bereitgestellten Ereignisdaten nicht analysieren konnte.

Example Funktionsfehler

```
{
      "errorMessage" : "Error parsing event data.",
      "errorType" : "InvalidEventDataException",
      "stackTrace": [ ]
}
```

Antwortcodes

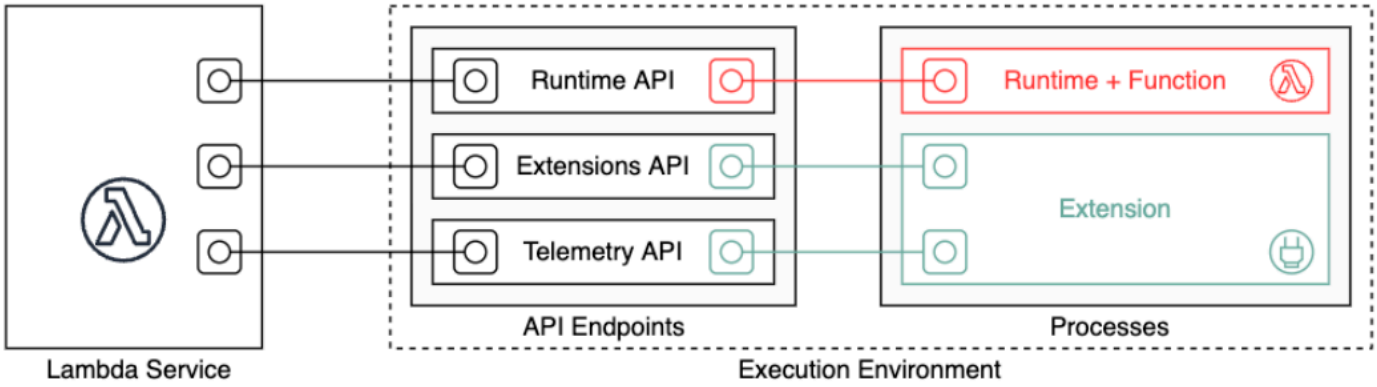
- 202 – Akzeptiert
- 400 – Ungültige Anfrage
- 403 – Verboten
- 500 – Container-Fehler. Nicht wiederherstellbarer Zustand. Die Erweiterung sollte umgehend beendet werden.

Lambda-Telemetrie-API

Über die Telemetry API können Ihre Erweiterungen Telemetriedaten direkt von Lambda empfangen. Während der Initialisierung und des Aufrufs von Funktionen erfasst Lambda automatisch Telemetriedaten wie Protokolle, Plattform-Metriken und Plattform-Ablaufverfolgungen. Über die Telemetry API können Erweiterungen diese Telemetriedaten direkt von Lambda in nahezu Echtzeit abrufen.

Sie können die Telemetrie-Streams für Ihre Lambda-Erweiterungen direkt in der Lambda-Ausführungsumgebung abonnieren. Nach dem Abonnement sendet Lambda automatisch alle Telemetriedaten an Ihre Erweiterungen. Sie können diese Daten dann verarbeiten, filtern und an Ihr bevorzugtes Ziel senden, z. B. einen Amazon Simple Storage Service (Amazon S3)-Bucket oder einen Drittanbieter von Beobachtbarkeits-Tools.

Das folgende Diagramm zeigt, wie die Extension API und die Telemetry API Erweiterungen von der Ausführungsumgebung aus mit Lambda verbinden. Die Runtime API verbindet zudem die Laufzeit und Funktion mit Lambda.



> **Important**
>
> Die Lambda-Telemetrie-API ersetzt die Lambda-Protokoll-API. Die Protokoll-API bleibt zwar voll funktionsfähig, wir empfehlen jedoch, in Zukunft nur die Telemetrie-API zu verwenden. Sie können Ihre Erweiterung für einen Telemetrie-Stream entweder über die Telemetrie-API oder die Protokoll-API abonnieren. Nach dem Abonnieren mithilfe einer dieser APIs gibt jeder Versuch, über die andere API zu abonnieren, einen Fehler zurück.

Erweiterungen können die Telemetrie-API verwenden, um drei verschiedene Telemetrie-Streams zu abonnieren:

- Plattformtelemetrie – Protokolle, Metriken und Ablaufverfolgungen, die Ereignisse und Fehler im Zusammenhang mit dem Laufzeitlebenszyklus der Ausführungsumgebung, dem Erweiterungslebenszyklus und Funktionsaufrufen beschreiben.
- Funktionsprotokolle – Benutzerdefinierte Protokolle, die der Lambda-Funktionscode generiert.
- Erweiterungsprotokolle – Benutzerdefinierte Protokolle, die der Lambda-Erweiterungscode generiert.

> **Note**
>
> Lambda sendet Protokolle und Metriken an CloudWatchund Ablaufverfolgungen an X-Ray (wenn Sie die Nachverfolgung aktiviert haben), auch wenn eine Erweiterung Telemetrie-Streams abonniert.

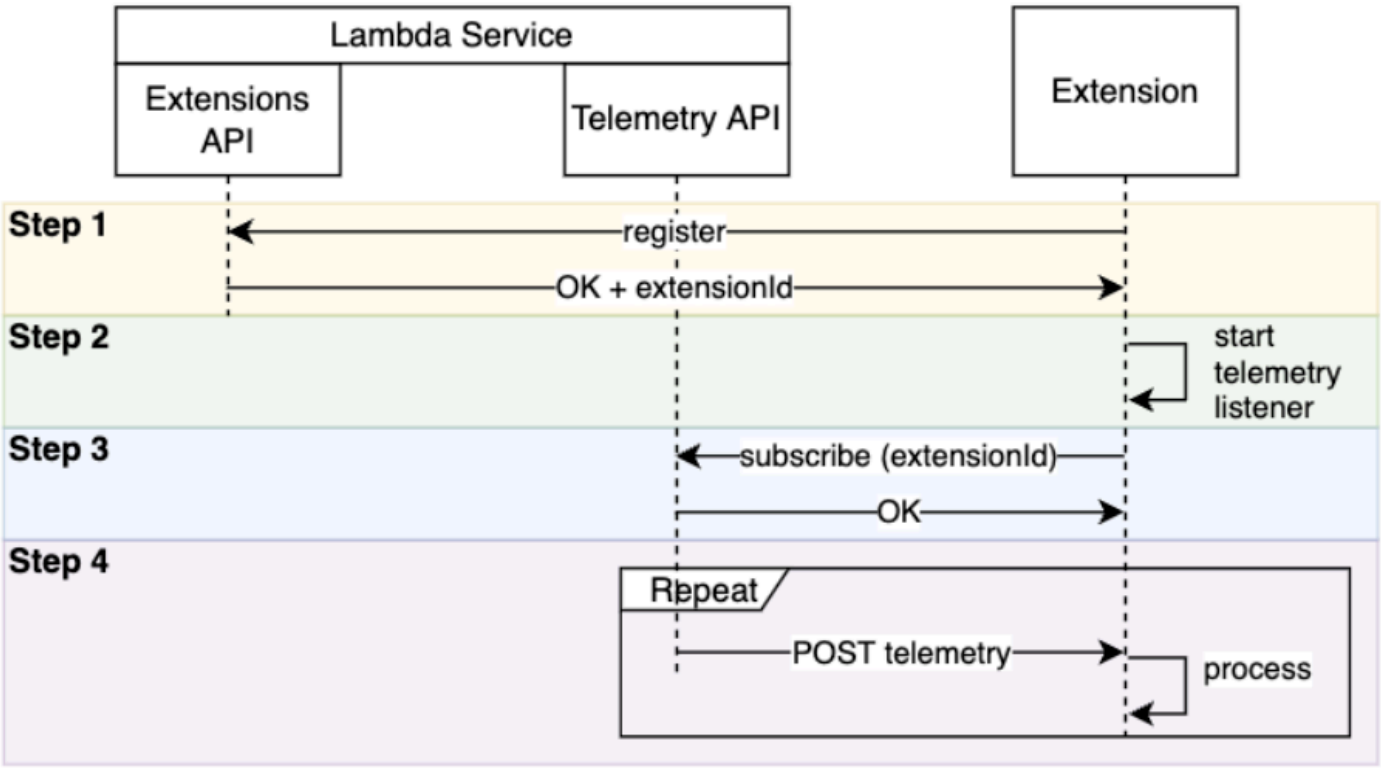
Sections

Erstellen von Erweiterungen mithilfe der Telemetrie-API

Lambda-Erweiterungen werden als unabhängige Prozesse in der Ausführungsumgebung ausgeführt. Erweiterungen können nach Abschluss des Funktionsaufrufs weiter ausgeführt werden. Da

Erweiterungen separate Prozesse sind, können Sie diese in einer anderen Sprache als dem Funktionscode schreiben. Es wird empfohlen, Erweiterungen mit einer kompilierten Sprache wie Golang oder Rust zu schreiben. Auf diese Weise ist die Erweiterung eine in sich geschlossene Binärdatei, die mit jeder unterstützten Laufzeitumgebung kompatibel sein kann.

Das folgende Diagramm zeigt einen vierstufigen Prozess zum Erstellen einer Erweiterung, die Telemetriedaten mithilfe der Telemetrie-API empfängt und verarbeitet.



Hier sind die einzelnen Schritte im Detail:

1. Registrieren Sie Ihre Erweiterung mithilfe von the section called “Erweiterungs-API”. Dadurch erhalten Sie einen `Lambda-Extension-Identifier`, den Sie in den folgenden Schritten benötigen. Weitere Informationen zum Registrieren einer Erweiterung finden Sie unter the section called “Registrieren Ihrer Erweiterung”.
2. Erstellen eines Telemetrie-Listeners. Dies kann ein einfacher HTTP- oder TCP-Server sein. Lambda verwendet den URI des Telemetrie-Listeners, um Telemetriedaten an Ihre Erweiterung zu senden. Weitere Informationen finden Sie unter the section called “Erstellen eines Telemetrie-Listeners”.
3. Verwenden Sie die Subscribe API in der Telemetry API, um die gewünschten Telemetrie-Streams für Ihre Erweiterung zu abonnieren. Für diesen Schritt benötigen Sie den URI Ihres

Telemetrie-Listeners. Weitere Informationen finden Sie unter the section called “Senden einer Abonnementanfrage an die Telemetrie-API”.

4. Rufen Sie Telemetriedaten von Lambda über den Telemetrie-Listener ab. Sie können diese Daten beliebig weiterverarbeiten, z. B. die Daten an Amazon S3 oder an einen externen Beobachtbarkeits-Service weiterleiten.

> **Note**
>
> Die Ausführungsumgebung einer Lambda-Funktion kann im Rahmen ihres Lebenszyklus mehrmals gestartet und angehalten werden. Im Allgemeinen wird Ihr Erweiterungscode während Funktionsaufrufen und auch bis zu 2 Sekunden während der Herunterfahrphase ausgeführt. Wir empfehlen, Telemetriedaten zu Batches zusammenzufassen, sobald sie bei Ihrem Listener eingehen. Verwenden Sie dann die Lebenszyklusereignisse `Invoke` und `Shutdown`, um jeden Batch an die gewünschten Ziele zu senden.

Registrieren Ihrer Erweiterung

Bevor Sie Telemetriedaten abonnieren können, müssen Sie Ihre Lambda-Erweiterung registrieren. Die Registrierung erfolgt während der Initialisierungsphase der Erweiterung. Das folgende Beispiel zeigt eine HTTP-Anfrage zur Registrierung einer Erweiterung.

```
POST http://${AWS_LAMBDA_RUNTIME_API}/2020-01-01/extension/register
 Lambda-Extension-Name: lambda_extension_name
{
    'events': [ 'INVOKE', 'SHUTDOWN']
}
```

Wenn die Anfrage erfolgreich ist, erhält der Subscriber eine Erfolgsantwort von HTTP 200. Der Antwort-Header enthält den `Lambda-Extension-Identifier`. Der Antworttext enthält weitere Eigenschaften der Funktion.

```
HTTP/1.1 200 OK
Lambda-Extension-Identifier: a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
{
    "functionName": "lambda_function",
    "functionVersion": "$LATEST",
    "handler": "lambda_handler",
```

```
    "accountId": "123456789012"
}
```

Weitere Informationen hierzu finden Sie unter the section called “Erweiterungs-API-Referenz”.

Erstellen eines Telemetrie-Listeners

Ihre Lambda-Erweiterung muss über einen Listener verfügen, der eingehende Anfragen der Telemetrie-API verarbeitet. Der folgende Code zeigt eine Beispielimplementierung eines Telemetrie-Listeners in Golang:

```
// Starts the server in a goroutine where the log events will be sent
func (s *TelemetryApiListener) Start() (string, error) {
 address := listenOnAddress()
 l.Info("[listener:Start] Starting on address", address)
 s.httpServer = &http.Server{Addr: address}
 http.HandleFunc("/", s.http_handler)
 go func() {
  err := s.httpServer.ListenAndServe()
  if err != http.ErrServerClosed {
   l.Error("[listener:goroutine] Unexpected stop on Http Server:", err)
   s.Shutdown()
  } else {
   l.Info("[listener:goroutine] Http Server closed:", err)
  }
 }()
 return fmt.Sprintf("http://%s/", address), nil
}

// http_handler handles the requests coming from the Telemetry API.
// Everytime Telemetry API sends log events, this function will read them from the
 response body
// and put into a synchronous queue to be dispatched later.
// Logging or printing besides the error cases below is not recommended if you have
 subscribed to
// receive extension logs. Otherwise, logging here will cause Telemetry API to send new
 logs for
// the printed lines which may create an infinite loop.
func (s *TelemetryApiListener) http_handler(w http.ResponseWriter, r *http.Request) {
 body, err := ioutil.ReadAll(r.Body)
 if err != nil {
  l.Error("[listener:http_handler] Error reading body:", err)
  return
```

```
 }

 // Parse and put the log messages into the queue
 var slice []interface{}
 _ = json.Unmarshal(body, &slice)

 for _, el := range slice {
  s.LogEventsQueue.Put(el)
 }

 l.Info("[listener:http_handler] logEvents received:", len(slice), " LogEventsQueue
 length:", s.LogEventsQueue.Len())
 slice = nil
}
```

Festlegen eines Zielprotokolls

Wenn Sie den Empfang von Telemetrie mithilfe der Telemetrie-API abonnieren, können Sie zusätzlich zur Ziel-URI ein Zielprotokoll angeben:

```
{
    "destination": {
        "protocol": "HTTP",
        "URI": "http://sandbox.localdomain:8080"
    }
}
```

Lambda akzeptiert zwei Protokolle für den Empfang von Telemetrie:

- HTTP (empfohlen) – Lambda übermittelt Telemetrie an einen lokalen HTTP-Endpunkt (`http://sandbox.localdomain:${PORT}/${PATH}`) als ein Array von Datensätzen im JSON-Format. Der Parameter `$PATH` ist optional. Lambda-unterstützt nur HTTP, nicht HTTPS. Lambda übermittelt Telemetrie über POST-Anfragen.
- TCP – Lambda übermittelt Telemtrie an einen TCP-Anschluss im Newline-delimited-JSON-(NDJSON)-Format.

> **Note**
>
> Wir empfehlen dringend, HTTP und nicht TCP zu verwenden. Mit TCP kann die Lambda-Plattform nicht bestätigen, dass es Telemetrie an die Anwendungsebene übermittelt. Wenn

Ihre Erweiterung abstürzt, verlieren Sie möglicherweise Telemetriedaten. Bei HTTP gibt es diese Einschränkung nicht.

Bevor Sie sich für den Empfang von Telemetriedaten registrieren, richten Sie den lokalen HTTP-Listener oder TCP-Port ein. Beachten Sie bei der Einrichtung Folgendes:

- Lambda sendet Telemetriedaten nur an Ziele, die sich innerhalb der Ausführungsumgebung befinden.
- Lambda wiederholt den Versuch, die Telemetriedaten (mit Backoff) zu senden, wenn es keinen Listener gibt oder wenn die POST-Anfrage zu einem Fehler führt. Wenn der Telemetrie-Listener abstürzt, erhält er nach dem Neustart der Ausführungsumgebung durch Lambda wieder Telemetriedaten.
- Lambda reserviert Port 9001. Es gibt keine weiteren Einschränkungen oder Empfehlungen für Portnummern.

Konfiguration der Speichernutzung und Pufferung

Der Speicherverbrauch in einer Ausführungsumgebung wächst linear mit der Anzahl der Abonnenten. Abonnements verbrauchen Speicherressourcen, da jedes einen neuen Speicherpuffer zum Speichern von Telemetriedaten öffnet. Die Pufferspeichernutzung wird zum Gesamtspeicherverbrauch in der Ausführungsumgebung gezählt.

Wenn Sie den Empfang von Telemetriedaten mithilfe der Telemetry API abonnieren, können Sie Telemetriedaten puffern und sie in Batches an Abonnenten übermitteln. Um die Speichernutzung zu optimieren, können Sie eine Pufferungskonfiguration angeben:

```
{
    "buffering": {
        "maxBytes": 256*1024,
        "maxItems": 1000,
        "timeoutMs": 100
    }
}
```

Pufferkonfigurations-Einstellungen

Parameter	Beschreibung	Standardwerte und Limits
`maxBytes`	Das maximale Telemetrievolumen (in Bytes), das im Speicher gepuffert werden soll.	Standard: 262 144 Mindestwert: 262 144 Höchstwert: 1 048 576
`maxItems`	Die maximale Anzahl von Ereignissen, die im Speicher gepuffert werden sollen.	Standard: 10 000 Mindestwert 1 000 Höchstwert: 10 000.
`timeoutMs`	Die maximale Zeit (in Millisekunden) zum Puffern eines Batches.	Standard: 1 000 Minimum: 25 Höchstwert: 30 000

Beachten Sie beim Einrichten der Pufferung die folgenden Punkte:

- Wenn einer der Eingabestreams geschlossen wird, leert Lambda die Protokolle. Dies kann beispielsweise passieren, wenn die Laufzeit abstürzt.
- Jeder Subscriber kann in seiner Abonnementanfrage eine andere Pufferungskonfiguration angeben.
- Rechnen Sie beim Bestimmen der Puffergröße für das Lesen der Daten mit eingehenden Nutzlasten in der Größenordnung von `2 * maxBytes + metadataBytes`, wobei `maxBytes` ein Bestandteil Ihrer Pufferungskonfiguration ist. Anhand der folgenden Metadaten können Sie `metadataBytes` abschätzen. Lambda hängt jedem Datensatz ähnliche Metadaten an:

```
{
   "time": "2022-08-20T12:31:32.123Z",
   "type": "function",
   "record": "Hello World"
}
```

- Wenn der Subscriber eingehende Telemetriedaten nicht schnell genug verarbeiten kann oder wenn Ihr Funktionscode ein sehr hohes Protokollvolumen erzeugt, löscht Lambda möglicherweise Datensätze, um die Speichernutzung zu begrenzen. In diesem Fall sendet Lambda ein `platform.logsDropped`-Ereignis.

Senden einer Abonnementanfrage an die Telemetrie-API

Lambda-Erweiterungen können den Empfang von Telemetriedaten abonnieren, indem sie eine Abonnementanfrage an die Telemetrie-API senden. Die Abonnementanfrage sollte Informationen über die Arten von Ereignissen enthalten, die die Erweiterung abonnieren soll. Darüber hinaus kann die Anfrage Informationen zum Lieferziel und eine Pufferkonfiguration enthalten.

Bevor Sie eine Abonnementanfrage senden, benötigen Sie eine Erweiterungs-ID (`Lambda-Extension-Identifier`). Wenn Sie Ihre Erweiterung in der Erweiterungs-API registrieren, erhalten Sie eine Erweiterungs-ID aus der API-Antwort.

Das Abonnement erfolgt während der Initialisierungsphase der Erweiterung. Das folgende Beispiel zeigt eine HTTP-Anfrage zum Abonnieren aller drei Telemetriestreams: Plattformtelemetrie, Funktionsprotokolle und Erweiterungsprotokolle.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
   "schemaVersion": "2022-12-13",
   "types": [
        "platform",
        "function",
        "extension"
   ],
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   },
   "destination": {
        "protocol": "HTTP",
        "URI": "http://sandbox.localdomain:8080"
   }
}
```

Ist die Anfrage erfolgreich, erhält der Subscriber eine HTTP 200-Erfolgsantwort.

```
HTTP/1.1 200 OK
"OK"
```

Eingehende Telemetrie-API-Nachrichten

Nach dem Abonnieren mit der Telemetry API beginnt eine Erweiterung automatisch, Telemetriedaten von Lambda über POST-Anfragen zu empfangen. Jeder POST-Anforderungstext enthält ein Array von `Event` Objekten. Jedes `Event` hat das folgende Schema:

```
{
   time: String,
   type: String,
   record: Object
}
```

- Die `time`-Eigenschaft definiert, wann die Lambda-Plattform das Ereignis generiert hat. Das ist nicht identisch mit dem Zeitpunkt, zu dem das Ereignis tatsächlich stattgefunden hat. Der Zeichenfolgenwert von `time` ist ein Zeitstempel im ISO 8601-Format.
- Die `type`-Eigenschaft definiert den Ereignistyp. Die folgende Tabelle beschreibt alle möglichen Werte.
- Die `record`-Eigenschaft definiert ein JSON-Objekt, das die Telemetriedaten enthält. Das Schema dieses JSON-Objekts hängt von dem `type` ab.

Die folgende Tabelle fasst alle `Event`-Objekttypen zusammen und enthält Links zur `Event`-Telemetrie-API-Schemareferenz für jeden Ereignistyp.

Telemetrie-API-Nachrichtentypen

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.initStart`	Die Funktionsinitialisierung wurde gestartet.	the section called “`platform.initStart`”-Schema

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.initRuntimeDone`	Die Funktionsinitialisierung ist abgeschlossen.	the section called “`platform.initRuntimeDone`”-Schema
Plattform-Ereignis	`platform.initReport`	Ein Bericht über die Funktionsinitialisierung.	the section called “`platform.initReport`”-Schema
Plattform-Ereignis	`platform.start`	Der Funktionsaufruf wurde gestartet.	the section called “`platform.start`”-Schema
Plattform-Ereignis	`platform.runtimeDone`	Die Laufzeit hat die Verarbeitung eines Ereignisses erfolgreich oder mit einem Fehler abgeschlossen.	the section called “`platform.runtimeDone`”-Schema
Plattform-Ereignis	`platform.report`	Ein Bericht über den Funktionsaufruf.	the section called “`platform.report`”-Schema
Plattform-Ereignis	`platform.restoreStart`	Die Laufzeitwiederherstellung wurde gestartet.	the section called “`platform.restoreStart`”-Schema
Plattform-Ereignis	`platform.restoreRuntimeDone`	Die Laufzeitwiederherstellung wurde abgeschlossen.	the section called “`platform.restoreRuntimeDone`”-Schema

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.restoreReport`	Bericht über die Laufzeitwiederherstellung.	the section called “`platform.restoreReport`”-Schema
Plattform-Ereignis	`platform.telemetrySubscription`	Die Erweiterung hat die Telemetrie-API abonniert.	the section called “`platform.telemetrySubscription`”-Schema
Plattform-Ereignis	`platform.logsDropped`	Lambda hat die Protokolleinträge gelöscht.	the section called “`platform.logsDropped`”-Schema
Funktionsprotokolle	`function`	Eine Protokollzeile aus dem Funktionscode.	the section called “`function`”-Schema
Erweiterungsprotokolle	`extension`	Eine Protokollzeile aus dem Erweiterungscode.	the section called “`extension`”-Schema

Referenz zur Lambda-Telemetrie-API

Verwenden Sie den Lambda-Telemetrie-API-Endpunkt, um Erweiterungen für Telemetrie-Streams zu abonnieren. Sie können den Telemtrie-API-Endpunkts aus der `AWS_LAMBDA_RUNTIME_API`-Umgebungsvariable abrufen. Um eine API-Anfrage zu senden, fügen Sie die API-Version (`2022-07-01/`) und `telemetry/` an. Beispielsweise:

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Die Definition der OpenAPI-Spezifikation (OAS) der Abonnementantwortversion `2022-12-13` finden Sie unter:

- HTTP – telemetry-api-http-schemaZIP
- TCP – telemetry-api-tcp-schemaZIP

API-Operationen

- Abonnieren

Abonnieren

Um einen Telemetrie-Stream zu abonnieren, kann eine Lambda-Erweiterung eine Abonnement-API-Anfrage senden.

- Pfad – `/telemetry`
- Methode – PUT
- Header
  - `Content-Type: application/json`
- Anfrage von Textparametern
  - schemaVersion
    - Erforderlich: Ja
    - Typ: Zeichenfolge
    - Gültige Werte: `"2022-12-13"` oder `"2022-07-01"`.
  - Ziel – Die Konfigurationseinstellungen, die das Ziel des Telemetrieereignisses und das Protokoll für die Ereignisübermittlung definieren.
    - Erforderlich: Ja

- Typ: Objekt

```
{
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080"
}
```

- Protokoll – Das Protokoll, das Lambda zum Senden von Telemetriedaten verwendet.
  - Erforderlich: Ja
  - Typ: Zeichenfolge
  - Gültige Werte: `"HTTP"|"TCP"`
- URI – Der URI, an den Telemetriedaten gesendet werden sollen.
  - Erforderlich: Ja
  - Typ: Zeichenfolge
- Weitere Informationen finden Sie unter the section called “Festlegen eines Zielprotokolls”.

- Typen – Die Telemetrietypen, die die Erweiterung abonnieren soll.
  - Erforderlich: Ja
  - Typ: Zeichenfolgen-Array
  - Zulässige Werte: `"platform"|"function"|"extension"`
- Pufferung – Die Konfigurationseinstellungen für die Ereignispufferung.
  - Erforderlich: Nein
  - Typ: Objekt

```
{
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   }
}
```

  - maxItems – Die maximale Anzahl der Ereignisse im Speicher, die gepuffert werden sollen.
    - Erforderlich: Nein
    - Typ: Ganzzahl
    - Standard: 1 000

    - Mindestwert 1 000
    - Höchstwert: 10 000.
- maxBytes – Das maximale Telemetrievolumen (in Bytes), das im Speicher gepuffert werden soll.
    - Erforderlich: Nein
    - Typ: Ganzzahl
    - Standard: 262 144
    - Mindestwert: 262 144
    - Höchstwert: 1 048 576
- timeoutMs – Die maximale Zeit (in Millisekunden) zum Puffern eines Batches.
    - Erforderlich: Nein
    - Typ: Ganzzahl
    - Standard: 1 000
    - Minimum: 25
    - Höchstwert: 30 000
- Weitere Informationen finden Sie unter the section called “Konfiguration der Speichernutzung und Pufferung”.

Beispiel für eine Abonnement-API-Anfrage

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry HTTP/1.1
{
   "schemaVersion": "2022-12-13",
   "types": [
        "platform",
        "function",
        "extension"
   ],
   "buffering": {
        "maxItems": 1000,
        "maxBytes": 256*1024,
        "timeoutMs": 100
   },
   "destination": {
        "protocol": "HTTP",
        "URI": "http://sandbox.localdomain:8080"
```

```
    }
}
```

Wenn die Abonnement-Anfrage erfolgreich war, erhält die Erweiterung eine Erfolgsbestätigung (HTTP 200):

```
HTTP/1.1 200 OK
"OK"
```

Wenn die Abonnement-Anfrage fehlschlägt, erhält die Erweiterung eine Fehlerantwort. Beispielsweise:

```
HTTP/1.1 400 OK
{
    "errorType": "ValidationError",
    "errorMessage": "URI port is not provided; types should not be empty"
}
```

Hier sind einige zusätzliche Antwortcodes, die die Erweiterung empfangen kann:

- 200 – Anfrage erfolgreich abgeschlossen
- 202 – Anfrage wurde akzeptiert. Antwort auf die Abonnement-Anfrage in einer lokalen Testumgebung
- 400 – Ungültige Anfrage
- 500 – Servicefehler

Referenz zum **`Event`**-Schema der Lambda-Telemetrie-API

Verwenden Sie den Lambda-Telemetrie-API-Endpunkt, um Erweiterungen für Telemetrie-Streams zu abonnieren. Sie können den Telemtrie-API-Endpunkts aus der `AWS_LAMBDA_RUNTIME_API`-Umgebungsvariable abrufen. Um eine API-Anfrage zu senden, fügen Sie die API-Version (`2022-07-01/`) und `telemetry/` an. Beispielsweise:

```
http://${AWS_LAMBDA_RUNTIME_API}/2022-07-01/telemetry/
```

Die Definition der OpenAPI-Spezifikation (OAS) der Abonnementantwortversion `2022-12-13` finden Sie unter:

- HTTP — telemetry-api-http-schema.zip
- TCP — .zip telemetry-api-tcp-schema

Die folgende Tabelle enthält eine Zusammenfassung aller `Event`-Objekttypen, die die Telemetrie-API unterstützt.

Telemetrie-API-Nachrichtentypen

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.initStart`	Die Funktionsinitialisierung wurde gestartet.	the section called “`platform.initStart`”-Schema
Plattform-Ereignis	`platform.initRuntimeDone`	Die Funktionsinitialisierung ist abgeschlossen.	the section called “`platform.initRuntimeDone`”-Schema
Plattform-Ereignis	`platform.initReport`	Ein Bericht über die Funktionsinitialisierung.	the section called “`platform.initReport`”-Schema

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.start`	Der Funktionsaufruf wurde gestartet.	the section called “`platform.start`”-Schema
Plattform-Ereignis	`platform.runtimeDone`	Die Laufzeit hat die Verarbeitung eines Ereignisses erfolgreich oder mit einem Fehler abgeschlossen.	the section called “`platform.runtimeDone`”-Schema
Plattform-Ereignis	`platform.report`	Ein Bericht über den Funktionsaufruf.	the section called “`platform.report`”-Schema
Plattform-Ereignis	`platform.restoreStart`	Die Laufzeitwiederherstellung wurde gestartet.	the section called “`platform.restoreStart`”-Schema
Plattform-Ereignis	`platform.restoreRuntimeDone`	Die Laufzeitwiederherstellung wurde abgeschlossen.	the section called “`platform.restoreRuntimeDone`”-Schema
Plattform-Ereignis	`platform.restoreReport`	Bericht über die Laufzeitwiederherstellung.	the section called “`platform.restoreReport`”-Schema

Kategorie	Ereignistyp	Beschreibung	Schema der Ereignisaufzeichnung
Plattform-Ereignis	`platform.telemetrySubscription`	Die Erweiterung hat die Telemetrie-API abonniert.	the section called “`platform.telemetrySubscription`”-Schema
Plattform-Ereignis	`platform.logsDropped`	Lambda hat die Protokolleinträge gelöscht.	the section called “`platform.logsDropped`”-Schema
Funktionsprotokolle	`function`	Eine Protokollzeile aus dem Funktionscode.	the section called “`function`”-Schema
Erweiterungsprotokolle	`extension`	Eine Protokollzeile aus dem Erweiterungscode.	the section called “`extension`”-Schema

Inhalt

Telemetrie-API **`Event`**-Objekttypen

Dieser Abschnitt beschreibt die Arten der `Event`-Objekte, die die Lambda-Telemetrie-API unterstützt. In den Ereignisbeschreibungen weist ein Fragezeichen (?) darauf hin, dass das Attribut möglicherweise nicht in diesem Objekt vorhanden ist.

`platform.initStart`

Ein `platform.initStart`-Ereignis zeigt an, dass die Initialisierungsphase der Funktion begonnen hat. Ein `platform.initStart` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.initStart
- record: PlatformInitStart
```

Dieses `PlatformInitStart`-Objekt hat die folgenden Attribute:

- functionName – `String`

- functionVersion – `String`
- initializationType – the section called “InitType”-Objekt
- instanceId? – `String`
- instanceMaxMemory? – `Integer`
- phase – the section called “InitPhase”-Objekt
- runtimeVersion? – `String`
- runtimeVersionArn? – `String`

Es folgt ein Beispiel für `Event` des Typs `platform.initStart`:

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.initStart",
    "record": {
        "initializationType": "on-demand",
        "phase": "init",
        "runtimeVersion": "nodejs-14.v3",
        "runtimeVersionArn": "arn",
        "functionName": "myFunction",
        "functionVersion": "$LATEST",
        "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
        "instanceMaxMemory": 256
    }
}
```

`platform.initRuntimeDone`

Ein `platform.initRuntimeDone`-Ereignis zeigt an, dass die Initialisierungsphase der Funktion abgeschlossen wurde. Ein `platform.initRuntimeDone` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.initRuntimeDone
- record: PlatformInitRuntimeDone
```

Dieses `PlatformInitRuntimeDone`-Objekt hat die folgenden Attribute:

- initializationType – the section called “InitType”-Objekt
- phase – the section called “InitPhase”-Objekt

- status – the section called “Status”-Objekt
- spans? – Liste von the section called “Span”-Objekten

Es folgt ein Beispiel für `Event` des Typs `platform.initRuntimeDone`:

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.initRuntimeDone",
    "record": {
        "initializationType": "on-demand"
        "status": "success",
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-06-02T12:02:33.913Z",
                "durationMs": 70.5
            }
        ]
    }
}
```

`platform.initReport`

Ein `platform.initReport`-Ereignis enthält einen Gesamtbericht über die Initialisierungsphase der Funktion. Ein `platform.initReport` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.initReport
- record: PlatformInitReport
```

Dieses `PlatformInitReport`-Objekt hat die folgenden Attribute:

- errorType? – Zeichenfolge
- initializationType – the section called “InitType”-Objekt
- phase – the section called “InitPhase”-Objekt
- metrics – the section called “InitReportMetrics”-Objekt
- spans? – Liste von the section called “Span”-Objekten
- status – the section called “Status”-Objekt

Es folgt ein Beispiel für `Event` des Typs `platform.initReport`:

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.initReport",
    "record": {
        "initializationType": "on-demand",
        "status": "success",
        "phase": "init",
        "metrics": {
            "durationMs": 125.33
        },
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-06-02T12:02:33.913Z",
                "durationMs": 90.1
            }
        ]
    }
}
```

`platform.start`

Ein `platform.start`-Ereignis zeigt an, dass die Funktionsaufrufphase begonnen hat. Ein `platform.start` `Event` Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.start
- record: PlatformStart
```

Dieses `PlatformStart`-Objekt hat die folgenden Attribute:

- requestId – `String`
- version? – `String`
- tracing? – the section called “TraceContext”

Es folgt ein Beispiel für `Event` des Typs `platform.start`:

```
{
```

```
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.start",
    "record": {
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
        "version": "$LATEST",
        "tracing": {
            "spanId": "54565fb41ac79632",
            "type": "X-Amzn-Trace-Id",
            "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
        }
    }
}
```

`platform.runtimeDone`

Ein `platform.runtimeDone`-Ereignis zeigt an, dass die Funktionsaufrufphase abgeschlossen ist. Ein `platform.runtimeDone` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.runtimeDone
- record: PlatformRuntimeDone
```

Dieses `PlatformRuntimeDone`-Objekt hat die folgenden Attribute:

- errorType? – `String`
- metrics? – the section called “RuntimeDoneMetrics” Objekt
- requestId – `String`
- status – the section called “Status”-Objekt
- spans? – Liste von the section called “Span”-Objekten
- tracing? – the section called “TraceContext”-Objekt

Es folgt ein Beispiel für `Event` des Typs `platform.runtimeDone`:

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.runtimeDone",
    "record": {
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
```

```
        "status": "success",
        "tracing": {
            "spanId": "54565fb41ac79632",
            "type": "X-Amzn-Trace-Id",
            "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
        },
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 80.0
            }
        ],
        "metrics": {
            "durationMs": 140.0,
            "producedBytes": 16
        }
    }
}
```

`platform.report`

Ein `platform.report`-Ereignis enthält einen Gesamtbericht über die Initialisierungsphase der Funktion. Ein `platform.report` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.report
- record: PlatformReport
```

Dieses `PlatformReport`-Objekt hat die folgenden Attribute:

- metrics – the section called “ReportMetrics”-Objekt
- requestId – `String`
- spans? – Liste von the section called “Span”-Objekten
- Status – the section called “Status”-Objekt
- Nachverfolgung? – the section called “TraceContext”-Objekt

Es folgt ein Beispiel für `Event` des Typs `platform.report`:

```
{
    "time": "2022-10-12T00:01:15.000Z",
    "type": "platform.report",
    "record": {
        "metrics": {
            "billedDurationMs": 694,
            "durationMs": 693.92,
            "initDurationMs": 397.68,
            "maxMemoryUsedMB": 84,
            "memorySizeMB": 128
        },
        "requestId": "6d68ca91-49c9-448d-89b8-7ca3e6dc66aa",
    }
}
```

`platform.restoreStart`

Ein `platform.restoreStart`-Ereignis zeigt an, dass ein Ereignis zur Wiederherstellung der Funktionsumgebung gestartet wurde. Bei einem Wiederherstellungsereignis einer Umgebung erstellt Lambda die Umgebung aus einem im Cache gespeicherten Snapshot, anstatt diese von Grund auf neu zu initialisieren. Weitere Informationen finden Sie unter Lambda SnapStart. Ein `platform.restoreStart` `Event` Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.restoreStart
- record: PlatformRestoreStart
```

Dieses `PlatformRestoreStart`-Objekt hat die folgenden Attribute:

- functionName – `String`
- functionVersion – `String`
- instanceId? – `String`
- instanceMaxMemory? – `String`
- runtimeVersion? – `String`
- runtimeVersionArn? – `String`

Es folgt ein Beispiel für `Event` des Typs `platform.restoreStart`:

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreStart",
    "record": {
        "runtimeVersion": "nodejs-14.v3",
        "runtimeVersionArn": "arn",
        "functionName": "myFunction",
        "functionVersion": "$LATEST",
        "instanceId": "82561ce0-53dd-47d1-90e0-c8f5e063e62e",
        "instanceMaxMemory": 256
    }
}
```

`platform.restoreRuntimeDone`

Ein `platform.restoreRuntimeDone`-Ereignis weist darauf hin, dass ein Wiederherstellungsereignis der Funktionsumgebung abgeschlossen wurde. Bei einem Wiederherstellungsereignis einer Umgebung erstellt Lambda die Umgebung aus einem im Cache gespeicherten Snapshot, anstatt diese von Grund auf neu zu initialisieren. Weitere Informationen finden Sie unter Lambda SnapStart. Ein `platform.restoreRuntimeDone` `Event` Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.restoreRuntimeDone
- record: PlatformRestoreRuntimeDone
```

Dieses `PlatformRestoreRuntimeDone`-Objekt hat die folgenden Attribute:

- errorType? – `String`
- spans? – Liste von `the section called “Span”`-Objekten
- status – `the section called “Status”`-Objekt

Es folgt ein Beispiel für `Event` des Typs `platform.restoreRuntimeDone`:

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreRuntimeDone",
    "record": {
        "status": "success",
```

```
        "spans": [
            {
                "name": "someTimeSpan",
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 80.0
            }
        ]
    }
}
```

`platform.restoreReport`

Ein `platform.restoreReport`-Ereignis enthält einen Gesamtbericht über ein Ereignis zur Funktionswiederherstellung. Ein `platform.restoreReport` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.restoreReport
- record: PlatformRestoreReport
```

Dieses `PlatformRestoreReport`-Objekt hat die folgenden Attribute:

- errorType? – Zeichenfolge
- metrics? – the section called “RestoreReportMetrics” Objekt
- spans? – Liste von the section called “Span”-Objekten
- status – the section called “Status”-Objekt

Es folgt ein Beispiel für `Event` des Typs `platform.restoreReport`:

```
{
    "time": "2022-10-12T00:00:15.064Z",
    "type": "platform.restoreReport",
    "record": {
        "status": "success",
        "metrics": {
            "durationMs": 15.19
        },
        "spans": [
            {
                "name": "someTimeSpan",
```

```
                "start": "2022-08-02T12:01:23:521Z",
                "durationMs": 30.0
            }
        ]
    }
}
```

platform.extension

Ein `extension`-Ereignis enthält Protokolle aus dem Erweiterungscode. Ein `extension` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = extension
- record: {}
```

Dieses `PlatformExtension`-Objekt hat die folgenden Attribute:

- events – Liste von `String`
- name – `String`
- status – `String`

Es folgt ein Beispiel für `Event` des Typs `platform.extension`:

```
{
    "time": "2022-10-12T00:02:15.000Z",
    "type": "platform.extension",
    "record": {
        "events": [ "INVOKE", "SHUTDOWN" ],
        "name": "my-telemetry-extension",
        "state": "Ready"
    }
}
```

platform.telemetrySubscription

Ein `platform.telemetrySubscription`-Ereignis enthält Informationen zu einem Erweiterungsabonnement. Ein `platform.telemetrySubscription` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.telemetrySubscription
- record: PlatformTelemetrySubscription
```

Dieses `PlatformTelemetrySubscription`-Objekt hat die folgenden Attribute:

- name – `String`
- status – `String`
- types – Liste von `String`

Es folgt ein Beispiel für `Event` des Typs `platform.telemetrySubscription`:

```
{
    "time": "2022-10-12T00:02:35.000Z",
    "type": "platform.telemetrySubscription",
    "record": {
        "name": "my-telemetry-extension",
        "state": "Subscribed",
        "types": [ "platform", "function" ]
    }
}
```

`platform.logsDropped`

Ein `platform.logsDropped`-Ereignis enthält Informationen über gelöschte Ereignisse. Lambda gibt das `platform.logsDropped` Ereignis aus, wenn eine Funktion Logs mit einer zu hohen Rate ausgibt, als dass Lambda sie verarbeiten könnte. Wenn Lambda Protokolle nicht mit der Geschwindigkeit an CloudWatch oder an die Erweiterung senden kann, die die Telemetrie-API abonniert hat, werden Protokolle gelöscht, um zu verhindern, dass die Ausführung der Funktion verlangsamt wird. Ein `platform.logsDropped` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = platform.logsDropped
- record: PlatformLogsDropped
```

Dieses `PlatformLogsDropped`-Objekt hat die folgenden Attribute:

- droppedBytes – `Integer`
- droppedRecords – `Integer`
- reason – `String`

Es folgt ein Beispiel für `Event` des Typs `platform.logsDropped`:

```
{
    "time": "2022-10-12T00:02:35.000Z",
    "type": "platform.logsDropped",
    "record": {
        "droppedBytes": 12345,
        "droppedRecords": 123,
        "reason": "Some logs were dropped because the downstream consumer is slower
 than the logs production rate"
    }
}
```

`function`

Ein `function`-Ereignis enthält Protokolle aus dem Funktionscode. Ein `function` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = function
- record: {}
```

Das Format des Felds `record` hängt davon ab, ob die Protokolle Ihrer Funktion im Klartext- oder JSON-Format formatiert sind. Weitere Informationen zu den Konfigurationsoptionen für das Protokollformat finden Sie unter the section called “Konfiguration der JSON- und Klartext-Protokollformate”.

Im Folgenden finden Sie ein Beispiel für `Event` vom Typ `function`, bei dem das Protokollformat Klartext ist:

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "function",
    "record": "[INFO] Hello world, I am a function!"
```

```
}
```

Im Folgenden finden Sie ein Beispiel für `Event` vom Typ `function`, bei dem das Protokollformat JSON ist:

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "function",
    "record": {
        "timestamp": "2022-10-12T00:03:50.000Z",
        "level": "INFO",
        "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
        "message": "Hello world, I am a function!"
    }
}
```

> **Note**
>
> Wenn die von Ihnen verwendete Schemaversion älter als die `2022-12-13`-Version ist, wird `"record"` immer als Zeichenfolge gerendert, auch wenn das Protokollierungsformat Ihrer Funktion als JSON konfiguriert ist.

`extension`

Ein `extension`-Ereignis enthält Protokolle aus dem Erweiterungscode. Ein `extension` `Event`-Objekt hat die folgende Form:

```
Event: Object
- time: String
- type: String = extension
- record: {}
```

Das Format des Felds `record` hängt davon ab, ob die Protokolle Ihrer Funktion im Klartext- oder JSON-Format formatiert sind. Weitere Informationen zu den Konfigurationsoptionen für das Protokollformat finden Sie unter the section called “Konfiguration der JSON- und Klartext-Protokollformate”.

Im Folgenden finden Sie ein Beispiel für `Event` vom Typ `extension`, bei dem das Protokollformat Klartext ist:

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "extension",
    "record": "[INFO] Hello world, I am an extension!"
}
```

Im Folgenden finden Sie ein Beispiel für `Event` vom Typ `extension`, bei dem das Protokollformat JSON ist:

```
{
    "time": "2022-10-12T00:03:50.000Z",
    "type": "extension",
    "record": {
       "timestamp": "2022-10-12T00:03:50.000Z",
       "level": "INFO",
       "requestId": "79b4f56e-95b1-4643-9700-2807f4e68189",
       "message": "Hello world, I am an extension!"
    }
}
```

> **Note**
>
> Wenn die von Ihnen verwendete Schemaversion älter als die `2022-12-13`-Version ist, wird `"record"` immer als Zeichenfolge gerendert, auch wenn das Protokollierungsformat Ihrer Funktion als JSON konfiguriert ist.

Freigegebene Objekttypen

Dieser Abschnitt beschreibt die Arten von freigegebenen Objekten, die die Lambda-Telemetrie-API unterstützt.

`InitPhase`

Eine Zeichenfolgenaufzählung, die die Phase beschreibt, in der der Initialisierungsschritt auftritt. In den meisten Fällen führt Lambda den Funktionsinitialisierungscode während der `init`-Phase aus. In einigen Fehlerfällen kann Lambda jedoch den Funktionsinitialisierungscode während der `invoke`-Phase erneut ausführen. (Dies wird als suppressed init bezeichnet.)

- Typ: – `String`

- Gültige Werte – `init|invoke|snap-start`

`InitReportMetrics`

Ein Objekt, das Metriken zu einer Initialisierungsphase enthält.

- Typ: – `Object`

Ein `InitReportMetrics`-Objekt hat die folgende Form:

```
InitReportMetrics: Object
- durationMs: Double
```

Es folgt ein Beispiel für ein `InitReportMetrics`-Objekt:

```
{
    "durationMs": 247.88
}
```

`InitType`

Eine Zeichenfolgenaufzählung, die beschreibt, wie Lambda die Umgebung initialisiert hat.

- Typ: – `String`
- Gültige Werte – `on-demand|provisioned-concurrency`

`ReportMetrics`

Ein Objekt, das Details zu einer abgeschlossenen Phase enthält.

- Typ: – `Object`

Ein `ReportMetrics`-Objekt hat die folgende Form:

```
ReportMetrics: Object
- billedDurationMs: Integer
- durationMs: Double
- initDurationMs?: Double
- maxMemoryUsedMB: Integer
```

```
- memorySizeMB: Integer
- restoreDurationMs?: Double
```

Es folgt ein Beispiel für ein `ReportMetrics`-Objekt:

```
{
    "billedDurationMs": 694,
    "durationMs": 693.92,
    "initDurationMs": 397.68,
    "maxMemoryUsedMB": 84,
    "memorySizeMB": 128
}
```

`RestoreReportMetrics`

Ein Objekt, das Metriken über eine abgeschlossene Wiederherstellungsphase enthält.

- Typ: – `Object`

Ein `RestoreReportMetrics`-Objekt hat die folgende Form:

```
RestoreReportMetrics: Object
- durationMs: Double
```

Es folgt ein Beispiel für ein `RestoreReportMetrics`-Objekt:

```
{
    "durationMs": 15.19
}
```

`RuntimeDoneMetrics`

Ein Objekt, das Metriken über eine Aufrufphase enthält.

- Typ: – `Object`

Ein `RuntimeDoneMetrics`-Objekt hat die folgende Form:

```
RuntimeDoneMetrics: Object
- durationMs: Double
```

```
- producedBytes?: Integer
```

Es folgt ein Beispiel für ein `RuntimeDoneMetrics`-Objekt:

```
{
    "durationMs": 200.0,
    "producedBytes": 15
}
```

`Span`

Ein Objekt, das Details einem Span enthält. Ein Span stellt eine Arbeitseinheit oder einen Vorgang in einer Ablaufverfolgung dar. Weitere Informationen zu Spans finden Sie unter Span auf der Tracing-API-Seite der Docs-Website. OpenTelemetry

Lambda unterstützt die folgenden zwei Bereiche für das `platform.RuntimeDone`-Ereignis:

- Der `responseLatency`-Span beschreibt, wie lange es gedauert hat, bis Ihre Lambda-Funktion mit dem Senden der Antwort begonnen hat.
- Der `responseDuration`-Spanbeschreibt, wie lange es gedauert hat, bis Ihre Lambda-Funktion das Senden der Antwort abgeschlossen hat.
- Die `runtimeOverhead`-Spanne beschreibt, wie lange es gedauert hat, bis die Lambda-Laufzeit signalisiert hat, dass sie für die Verarbeitung des nächsten Funktionsaufrufs bereit ist. Dies ist die Zeit, die die Laufzeit benötigt hat, um die nächste Aufruf-API aufzurufen, um das nächste Ereignis nach der Rückgabe Ihrer Funktionsantwort zu erhalten.

Es folgt ein Beispiel für ein Objekt des `responseLatency`-Spans:

```
{
        "name": "responseLatency",
        "start": "2022-08-02T12:01:23.521Z",
        "durationMs": 23.02
      }
```

`Status`

Ein Objekt, das den Status einer Initialisierungs- oder Aufrufphase beschreibt. Wenn der Status entweder `failure` oder `error` ist, dann enthält das `Status`-Objekt auch ein `errorType`-Feld, das den Fehler beschreibt.

- Typ: – `Object`
- Gültige Statuswerte – `success|failure|error|timeout`

`TraceContext`

Ein Objekt, das die Eigenschaften einer Ablaufverfolgung beschreibt.

- Typ: – `Object`

Ein `TraceContext`-Objekt hat die folgende Form:

```
TraceContext: Object
- spanId?: String
- type: TracingType enum
- value: String
```

Es folgt ein Beispiel für ein `TraceContext`-Objekt:

```
{
    "spanId": "073a49012f3c312e",
    "type": "X-Amzn-Trace-Id",
    "value":
 "Root=1-62e900b2-710d76f009d6e7785905449a;Parent=0efbd19962d95b05;Sampled=1"
}
```

`TracingType`

Eine Zeichenfolgenaufzählung, die den Ablaufverfolgungstyp in einem the section called “`TraceContext`”-Objekt beschreibt.

- Typ: – `String`
- Gültige Werte – `X-Amzn-Trace-Id`

Konvertieren von Lambda-Telemetrie-API-**`Event`**Objekten in OpenTelemetry Spans

Das AWS Lambda Telemetrie-API-Schema ist semantisch kompatibel mit OpenTelemetry (OTel). Das bedeutet, dass Sie Ihre AWS Lambda Telemetrie-API-`Event`Objekte in OpenTelemetry (OTel)-Spans konvertieren können. Beim Konvertieren sollten Sie kein einzelnes `Event`-Objekt einem einzelnen OTel Span zuordnen. Stattdessen sollten Sie alle drei Ereignisse, die sich auf eine Lebenszyklusphase beziehen, in einem einzigen OTel-Span darstellen. Die `start`, `runtimeDone`, und `runtimeReport`-Ereignisse repräsentieren beispielsweise einen einzelnen Funktionsaufruf. Stellen Sie alle drei Ereignisse als einen einzigen OTel-Span dar.

Sie können Ihre Ereignisse mithilfe von Span-Ereignissen oder untergeordneten (verschachtelten) Spans konvertieren. Die Tabellen auf dieser Seite beschreiben die Zuordnungen zwischen Telemetrie-API-Schemaeigenschaften und OTel-Span-Eigenschaften für beide Ansätze. Weitere Informationen zu OTel-Spans finden Sie unter Span auf der Seite Ablaufverfolgungs-API der OpenTelemetry Docs-Website.

Sections

Zuordnung zu OTel Spans mit Span-Ereignissen

In den folgenden Tabellen stellt e das Ereignis dar, das von der Telemetrie-Quelle stammt.

Zuordnung der **`*Start`**-Ereignisse

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Name`	Ihre Erweiterung generiert diesen Wert basierend auf dem `type`-Feld.
`Span.StartTime`	Verwenden Sie `e.time`.
`Span.EndTime`	Nicht zutreffend, da das Ereignis noch nicht abgeschlossen ist.
`Span.Kind`	Setzen Sie diesen Wert auf `Server`.

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Status`	Setzen Sie diesen Wert auf `Unset`.
`Span.TraceId`	Analysieren Sie den AWS X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `TraceId`-Wert.
`Span.ParentId`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Parent`-Wert.
`Span.SpanId`	Verwenden Sie `e.tracing.spanId` , falls verfügbar. Generieren Sie andernfalls eine neue `SpanId`.
`Span.SpanContext.TraceState`	Nicht zutreffend für einen X-Ray-Ablaufverfol gungskontext.
`Span.SpanContext.TraceFlags`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Sampled`-Wert.
`Span.Attributes`	Ihre Erweiterung kann hier beliebige benutzerd efinierte Werte hinzufügen.

Zuordnung der **`*RuntimeDone`**-Ereignisse

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Name`	Ihre Erweiterung generiert den Wert basierend auf dem `type`-Feld.
`Span.StartTime`	Verwenden Sie `e.time` aus dem übereinst immenden `*Start`-Ereignis. Als alternative Vorgehensweise verwenden Sie `e.time - e.metrics.durationMs` .

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.EndTime`	Nicht zutreffend, da das Ereignis noch nicht abgeschlossen ist.
`Span.Kind`	Setzen Sie diesen Wert auf `Server`.
`Span.Status`	Wenn `e.status` nicht gleich `success` ist, dann Wert auf `Error` festlegen. Ansonsten auf `Ok` festlegen.
`Span.Events[]`	Verwenden Sie `e.spans[]` .
`Span.Events[i].Name`	Verwenden Sie `e.spans[i].name` .
`Span.Events[i].Time`	Verwenden Sie `e.spans[i].start` .
`Span.TraceId`	Analysieren Sie den AWS X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `TraceId`-Wert.
`Span.ParentId`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Parent`-Wert.
`Span.SpanId`	Verwenden Sie dieselbe `SpanId` aus dem `*Start`-Ereignis. Falls nicht verfügbar, verwenden Sie `e.tracing.spanId` oder generieren Sie eine neue `SpanId`.
`Span.SpanContext.TraceState`	Nicht zutreffend für einen X-Ray-Ablaufverfol gungskontext.
`Span.SpanContext.TraceFlags`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Sampled`-Wert.
`Span.Attributes`	Ihre Erweiterung kann hier beliebige benutzerd efinierte Werte hinzufügen.

Zuordnung der **`*Report`**-Ereignisse

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Name`	Ihre Erweiterung generiert den Wert basierend auf dem `type`-Feld.
`Span.StartTime`	Verwenden Sie `e.time` aus dem übereinstimmenden `*Start`-Ereignis. Als alternative Vorgehensweise verwenden Sie `e.time - e.metrics.durationMs` .
`Span.EndTime`	Verwenden Sie `e.time`.
`Span.Kind`	Setzen Sie diesen Wert auf `Server`.
`Span.Status`	Verwenden Sie den gleichen Wert wie das `*RuntimeDone` -Ereignis.
`Span.TraceId`	Analysieren Sie den AWS X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `TraceId`-Wert.
`Span.ParentId`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Parent`-Wert.
`Span.SpanId`	Verwenden Sie dieselbe `SpanId` aus dem `*Start`-Ereignis. Falls nicht verfügbar, verwenden Sie `e.tracing.spanId` oder generieren Sie eine neue `SpanId`.
`Span.SpanContext.TraceState`	Nicht zutreffend für einen X-Ray-Ablaufverfolgungskontext.
`Span.SpanContext.TraceFlags`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Sampled`-Wert.

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Attributes`	Ihre Erweiterung kann hier beliebige benutzerdefinierte Werte hinzufügen.

Zuordnung zu OTel-Spans mit untergeordneten Spans

Die folgende Tabelle beschreibt, wie Lambda-Telemetrie-API-Ereignisse in OTel-Spans mit untergeordneten (verschachtelten) Spans für `*RuntimeDone`-Spans konvertiert werden. Informationen zu `*Start`- und `*Report`-Zuordnungen finden Sie in den Tabellen in the section called “Zuordnung zu OTel Spans mit Span-Ereignissen”, da diese für untergeordnete Spans identisch sind. In dieser Tabelle stellt `e` das Ereignis dar, das von der Telemetrie-Quelle stammt.

Zuordnung der **`*RuntimeDone`**-Ereignisse

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.Name`	Ihre Erweiterung generiert den Wert basierend auf dem `type`-Feld.
`Span.StartTime`	Verwenden Sie `e.time` aus dem übereinstimmenden `*Start`-Ereignis. Als alternative Vorgehensweise verwenden Sie `e.time - e.metrics.durationMs` .
`Span.EndTime`	Nicht zutreffend, da das Ereignis noch nicht abgeschlossen ist.
`Span.Kind`	Setzen Sie diesen Wert auf `Server`.
`Span.Status`	Wenn `e.status` nicht gleich `success` ist, dann Wert auf `Error` festlegen. Ansonsten auf `0k` festlegen.
`Span.TraceId`	Analysieren Sie den AWS X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `TraceId`-Wert.

OpenTelemetry	Schema der Lambda-Telemetrie-API
`Span.ParentId`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Parent`-Wert.
`Span.SpanId`	Verwenden Sie dieselbe `SpanId` aus dem `*Start`-Ereignis. Falls nicht verfügbar, verwenden Sie `e.tracing.spanId` oder generieren Sie eine neue `SpanId`.
`Span.SpanContext.TraceState`	Nicht zutreffend für einen X-Ray-Ablaufverfol gungskontext.
`Span.SpanContext.TraceFlags`	Analysieren Sie den X-Ray-Header, der in `e.tracing.value` gefunden wurde, und verwenden Sie dann den `Sampled`-Wert.
`Span.Attributes`	Ihre Erweiterung kann hier beliebige benutzerd efinierte Werte hinzufügen.
`ChildSpan[i].Name`	Verwenden Sie `e.spans[i].name` .
`ChildSpan[i].StartTime`	Verwenden Sie `e.spans[i].start` .
`ChildSpan[i].EndTime`	Verwenden Sie `e.spans[i].start + e.spans[i].durations` .
`ChildSpan[i].Kind`	Wie bei übergeordnetem `Span.Kind` .
`ChildSpan[i].Status`	Wie bei übergeordnetem `Span.Status` .
`ChildSpan[i].TraceId`	Wie bei übergeordnetem `Span.TraceId` .
`ChildSpan[i].ParentId`	Verwenden Sie die übergeordnete `Span.Span Id` .
`ChildSpan[i].SpanId`	Generieren Sie eine neue `SpanId`.

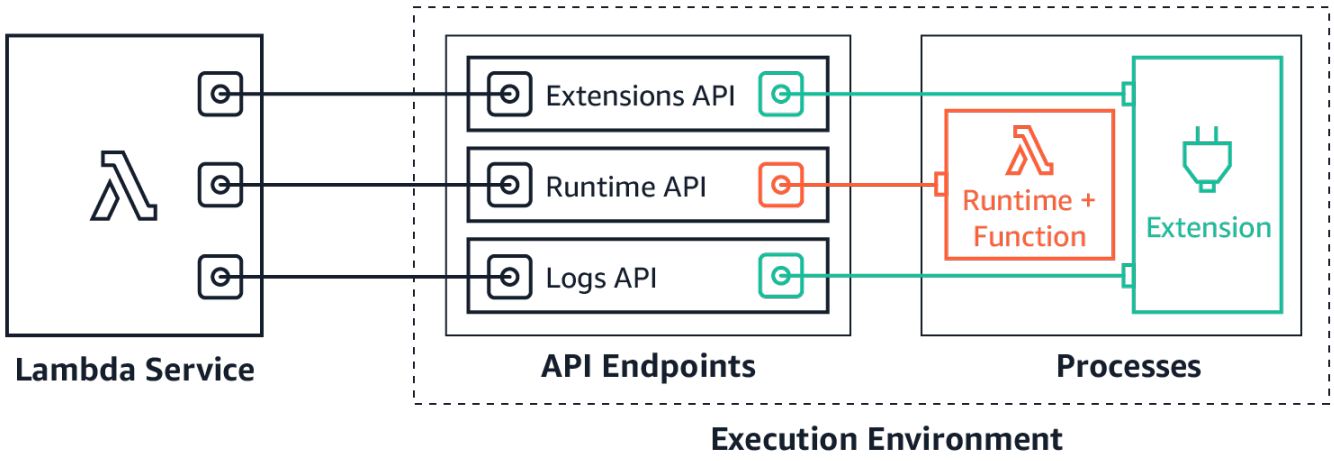
OpenTelemetry	Schema der Lambda-Telemetrie-API
`ChildSpan[i].SpanContext.TraceState`	Nicht zutreffend für einen X-Ray-Ablaufverfolgungskontext.
`ChildSpan[i].SpanContext.TraceFlags`	Wie bei übergeordnetem `Span.SpanContext.TraceFlags` .

API für Lambda-Protokolle

> **Important**
>
> Die Lambda-Telemetrie-API ersetzt die Lambda-Protokoll-API. Die Protokoll-API bleibt zwar voll funktionsfähig, wir empfehlen jedoch, in Zukunft nur die Telemetrie-API zu verwenden. Sie können Ihre Erweiterung für einen Telemetrie-Stream entweder über die Telemetrie-API oder die Protokoll-API abonnieren. Nach dem Abonnieren mithilfe einer dieser APIs gibt jeder Versuch, über die andere API zu abonnieren, einen Fehler zurück.

Lambda erfasst automatisch Laufzeitprotokolle und streamt sie an Amazon CloudWatch. Dieser Protokolldatenstream enthält die Protokolle, die Ihr Funktionscode und Ihre Erweiterungen generieren, sowie die Protokolle, die Lambda im Rahmen des Funktionsaufrufens generiert.

Lambda-Erweiterungen können die Lambda-Laufzeitprotokoll-API verwenden, um Protokollstreams direkt aus der Lambda-Ausführungsumgebung zu abonnieren. Lambda streamt die Protokolle zur Erweiterung und die Erweiterung kann die Protokolle dann an ein beliebiges bevorzugtes Ziel verarbeiten, filtern und senden.



Die Logs API ermöglicht es Erweiterungen, drei verschiedene Protokollstreams zu abonnieren:

- Funktionsprotokolle, die die Lambda-Funktion generiert und in `stdout` oder `stderr` schreibt.
- Erweiterungsprotokolle, die der Erweiterungscode generiert.
- Lambda-Plattformprotokolle, die Ereignisse und Fehler im Zusammenhang mit Aufrufen und Erweiterungen aufzeichnen.

> **Note**
>
> Lambda sendet alle Protokolle an CloudWatch, auch wenn eine Erweiterung einen oder mehrere der Protokollstreams abonniert.

Themen

Abonnieren des Empfangs von Protokollen

Eine Lambda-Erweiterung kann den Empfang von Protokollen abonnieren, indem sie eine Abonnementanfrage an die Protokoll-API sendet.

Um den Empfang von Protokollen zu abonnieren, benötigen Sie die Erweiterungskennung (`Lambda-Extension-Identifier`). Registrieren Sie zunächst die Erweiterung , um die Erweiterungskennung zu erhalten. Abonnieren Sie dann während der Initialisierung die Logs API. Lambda verarbeitet nach Abschluss der Initialisierungsphase keine Abonnementanfragen.

> **Note**
>
> Das Logs API-Abonnement ist idempotent. Doppelte Abonnementanfragen führen nicht zu doppelten Abonnements.

Speicherauslastung

Die Speichernutzung steigt linear, wenn die Anzahl der Abonnenten zunimmt. Abonnements verbrauchen Speicherressourcen, da jedes Abonnement einen neuen Speicherpuffer zum

Speichern der Protokolle öffnet. Um die Speicherauslastung zu optimieren, können Sie die Pufferungskonfigurationanpassen. Die Pufferspeichernutzung wird zum Gesamtspeicherverbrauch in der Ausführungsumgebung gezählt.

Ziel-Protokolle

Sie können eines der folgenden Protokolle auswählen, um die Logs zu erhalten:

1. HTTP (empfohlen) – Lambda stellt Protokolle als Array von Datensätzen im JSON-Format an einen lokalen HTTP-Endpunkt (`http://sandbox.localdomain:${PORT}/${PATH}`) bereit. Der Parameter `$PATH` ist optional. Beachten Sie, dass nur HTTP unterstützt wird, nicht HTTPS. Sie können wählen, ob Sie Logs über PUT oder POST erhalten möchten.
2. TCP – Lambda stellt Protokolle an einen TCP-Port im Newline-delimited-JSON-(NDJSON)-Format bereit.

Wir empfehlen, HTTP statt TCP zu verwenden. Mit TCP kann die Lambda-Plattform nicht bestätigen, wenn es Protokolle an die Anwendungsebene übermittelt. Daher können Sie Protokolle verlieren, wenn Ihre Erweiterung abstürzt. Bei HTTP gilt diese Einschränkung nicht.

Wir empfehlen außerdem, den lokalen HTTP-Listener oder den TCP-Port einzurichten, bevor Sie sich für den Empfang von Protokollen anmelden. Beachten Sie bei der Einrichtung Folgendes:

- Lambda sendet Protokolle nur an Ziele, die sich innerhalb der Ausführungsumgebung befinden.
- Lambda wiederholt den Versuch, die Protokolle (mit Backoff) zu senden, wenn es keinen Listener gibt oder wenn die POST- oder PUT-Anfrage zu einem Fehler führt. Wenn der Protokollabonnent abstürzt, erhält er nach dem Neustart der Ausführungsumgebung durch Lambda weiterhin Protokolle.
- Lambda reserviert Port 9001. Es gibt keine weiteren Einschränkungen oder Empfehlungen für Portnummern.

Pufferung der Konfiguration

Lambda kann Protokolle puffern und an den Abonnenten liefern. Sie können dieses Verhalten in der Abonnementanfrage konfigurieren, indem Sie die folgenden optionalen Felder angeben. Beachten Sie, dass Lambda den Standardwert für jedes Feld verwenden wird, das Sie nicht angeben.

- timeoutMs – Die maximale Zeit (in Millisekunden) zum Puffern eines Batches. Standard: 1 000. Minimum: 25. Höchstwert: 30 000.

- maxBytes – Die maximale Größe (in Byte) der Protokolle, die im Speicher gepuffert werden sollen. Standard: 262 144. Mindestwert: 262 144. Höchstwert: 1 048 576.
- maxItems – Die maximale Anzahl der Ereignisse im Speicher, die gepuffert werden sollen. Standard: 10 000. Mindestwert 1 000. Höchstwert: 10 000.

Beachten Sie bei der Pufferung die folgenden Punkte:

- Lambda bereinigt die Protokolle, wenn einer der Eingabestreams geschlossen wird, z. B. wenn die Laufzeit abstürzt.
- Jeder Abonnent kann in seiner Abonnementanfrage eine andere Pufferungskonfiguration angeben.
- Berücksichtigen Sie die Puffergröße, die Sie zum Lesen der Daten benötigen. Gehen Sie davon aus, dass die Nutzlasten so groß wie `2*maxBytes+metadata` sein werden, wo `maxBytes` in der Abonnementanfrage konfiguriert ist. Lambda fügt beispielsweise jedem Datensatz die folgenden Metadaten-Bytes hinzu:

  ```
  {
  "time": "2020-08-20T12:31:32.123Z",
  "type": "function",
  "record": "Hello World"
  }
  ```

- Wenn der Abonnent eingehende Protokolle nicht schnell genug verarbeiten kann, wird Lambda Protokolle möglicherweise löschen, um die Speicherauslastung begrenzt zu halten. Um die Anzahl der gelöschten Datensätze anzugeben, schickt Lambda ein `platform.logsDropped`-Protokoll.

Beispielabonnement

Das folgende Beispiel zeigt eine Anfrage zum Abonnieren der Plattform- und Funktionsprotokolle.

```
PUT http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs HTTP/1.1
{ "schemaVersion": "2020-08-15",
  "types": [
      "platform",
      "function"
    ],
  "buffering": {
      "maxItems": 1000,
      "maxBytes": 262144,
      "timeoutMs": 100
```

```
    },
  "destination": {
    "protocol": "HTTP",
    "URI": "http://sandbox.localdomain:8080/lambda_logs"
  }
}
```

Wenn die Anfrage erfolgreich ist, erhält der Abonnent eine Erfolgsantwort von HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Beispielcode für Logs API

Beispielcode zum Senden von Protokollen an ein benutzerdefiniertes Ziel finden Sie unter Verwenden von AWS Lambda-Erweiterungen zum Senden von Protokollen an benutzerdefinierte Ziele im AWS-Compute-Blog.

Codebeispiele für Python und Go, die zeigen, wie Sie eine grundlegende Lambda-Erweiterung entwickeln und die Logs-API abonnieren, finden Sie unter AWS Lambda Erweiterungen im AWS - Beispiel- GitHub Repository. Für weitere Informationen zum Erstellen einer Lambda-Erweiterung siehe the section called “Erweiterungs-API”.

Logs API-Referenz

Sie können den Wert des API-Endpunkts aus der `AWS_LAMBDA_RUNTIME_API`-Umgebungsvariablen abrufen. Um eine API-Anfrage zu senden, verwenden Sie das Präfix `2020-08-15/` vor dem API-Pfad. Beispielsweise:

```
http://${AWS_LAMBDA_RUNTIME_API}/2020-08-15/logs
```

Die OpenAPI-Spezifikation für die Logs-API-Version 2020-08-15 ist hier verfügbar: logs-api-request.zip

Abonnieren

Um einen oder mehrere der in der Lambda-Ausführungsumgebung verfügbaren Protokollstreams zu abonnieren, senden Erweiterungen eine Abonnement-API-Anforderung.

Pfad – `/logs`

Methode – PUT

Body-Parameter

`destination` – Siehe the section called “Ziel-Protokolle”. Erforderlich: ja Typ: Strings.

`buffering` – Siehe the section called “Pufferung der Konfiguration”. Erforderlich: Nein Typ: Strings.

`types` – Ein Array der zu empfangenden Protokollentypen. Erforderlich: ja Typ: Zeichenfolge-Array Gültige Werte: „platform“, „function“, „extension“.

`schemaVersion` – Erforderlich: Nein. Standardwert: „2020-08-15“. Stellen Sie „2021-03-18“ ein, damit die Erweiterung `platform.runtimeDone`-Meldungen empfangen kann.

Antwortparameter

Die OpenAPI-Spezifikationen für die Abonnementantworten, Version 2020-08-15, stehen für HTTP- und TCP-Protokolle zur Verfügung:

- HTTP: logs-api-http-responseZIP
- TCP: logs-api-tcp-responseZIP

Antwortcodes

- 200 – Anfrage erfolgreich abgeschlossen
- 202 – Anfrage wurde akzeptiert. Antwort auf eine Abonnementanfrage während lokaler Tests.
- 4XX – Ungültige Anfrage
- 500 – Servicefehler

Wenn die Anfrage erfolgreich ist, erhält der Abonnent eine Erfolgsantwort von HTTP 200.

```
HTTP/1.1 200 OK
"OK"
```

Schlägt die Anfrage fehl, erhält der Abonnent eine Fehlerantwort. Zum Beispiel:

```
HTTP/1.1 400 OK
{
    "errorType": "Logs.ValidationError",
```

```
    "errorMessage": URI port is not provided; types should not be empty"
}
```

Protokollmeldungen

Die Logs API ermöglicht es Erweiterungen, drei verschiedene Protokollstreams zu abonnieren:

- Funktion – Protokolle, die die Lambda-Funktion generiert und in `stdout` oder `stderr` schreibt.
- Erweiterung – Protokolle, die der Erweiterungscode generiert.
- Plattform – Protokolle, die von der Laufzeitplattform generiert werden und die Ereignisse und Fehler im Zusammenhang mit Aufrufen und Erweiterungen aufzeichnen.

Themen

Funktionsprotokolle

Die Lambda-Funktion und interne Erweiterungen generieren Funktionsprotokolle und schreiben sie in `stdout` oder `stderr`.

Das folgende Beispiel zeigt das Format einer Funktionsprotokollmeldung. {„time“: „2020-08-20T12:31:32.123Z“, „type“: „function“, „record“: „ERROR encountered. Stack trace:\n\my-function (line 10)\n" }

Erweiterungsprotokolle

Erweiterungen können Erweiterungsprotokolle generieren. Das Protokollformat ist das gleiche wie bei einem Funktionsprotokoll.

Plattformprotokolle

Lambda generiert Protokollmeldungen für Plattformereignisse wie `platform.start`, `platform.end` und `platform.fault`.

Optional können Sie die Version 2021-03-18 des Logs API-Schemas abonnieren, welche die `platform.runtimeDone`-Protokollmeldungen enthält.

Beispiel für Plattformprotokollmeldungen

Das folgende Beispiel zeigt die Plattformstart- und Plattformendprotokolle. Diese Protokolle zeigen die Startzeit des Aufrufs und die Endzeit des Aufrufs für den Aufruf an, den die RequestID angibt.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.start",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
}
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.end",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56"}
}
```

Die platform.initRuntimeDone-Protokollmeldung zeigt den Status der `Runtime init` Unterphase an, die Teil der Init-Lebenszyklusphase ist. Wenn `Runtime init` erfolgreich ist, sendet die Laufzeit eine `/next`-Laufzeit-API-Anfrage (für die `on-demand`- und `provisioned-concurrency`-Initialisierungstypen) oder `restore/next` (für den `snap-start`-Initialisierungstyp). Das folgende Beispiel zeigt eine erfolgreiche platform.initRuntimeDone-Protokollmeldung für den `-snap-start`Initialisierungstyp.

```
{
  "time":"2022-07-17T18:41:57.083Z",
  "type":"platform.initRuntimeDone",
  "record":{
      "initializationType":"snap-start",
      "status":"success"
  }
}
```

Die platform.initReport-Protokollnachricht zeigt, wie lange die `Init`-Phase gedauert hat und wie viele Millisekunden Ihnen während dieser Phase in Rechnung gestellt wurden. Wenn der Initialisierungstyp `provisioned-concurrency` lautet, sendet Lambda diese Nachricht während des Aufrufs. Wenn der Initialisierungstyp `snap-start` lautet, sendet Lambda diese Nachricht nach der Wiederherstellung des Snapshots. Das folgende Beispiel zeigt eine platform.initReport-Protokollnachricht für den `snap-start`-Initialisierungstyp.

```
{
```

```
  "time":"2022-07-17T18:41:57.083Z",
  "type":"platform.initReport",
  "record":{
      "initializationType":"snap-start",
      "metrics":{
          "durationMs":731.79,
          "billedDurationMs":732
          }
  }
}
```

Das Berichtsprotokoll der Plattform enthält Metriken über den Aufruf, den die RequestID angibt. Das `initDurationMs`-Feld ist nur dann im Protokoll enthalten, wenn der Aufruf einen Kaltstart enthielt. Wenn die AWS X-Ray-Ablaufverfolgung aktiv ist, enthält das Protokoll X-Ray-Metadaten. Das folgende Beispiel zeigt ein Plattformberichtsprotokoll für einen Aufruf, der einen Kaltstart enthielt.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.report",
    "record": {"requestId": "6f7f0961f83442118a7af6fe80b88d56",
        "metrics": {"durationMs": 101.51,
            "billedDurationMs": 300,
            "memorySizeMB": 512,
            "maxMemoryUsedMB": 33,
            "initDurationMs": 116.67
        }
    }
}
```

Das Plattformfehlerprotokoll erfasst Fehler bei der Laufzeit oder der Ausführungsumgebung. Das folgende Beispiel zeigt eine Fehlerprotokollmeldung der Plattform.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.fault",
    "record": "RequestId: d783b35e-a91d-4251-af17-035953428a2c Process exited before
 completing request"
}
```

Lambda generiert ein Plattformerweiterungsprotokoll, wenn sich eine Erweiterung bei der Erweiterungs-API registriert. Das folgende Beispiel zeigt eine Plattformerweiterungsmeldung.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.extension",
    "record": {"name": "Foo.bar",
        "state": "Ready",
        "events": ["INVOKE", "SHUTDOWN"]
     }
}
```

Lambda generiert ein Plattformprotokoll-Abonnementprotokoll, wenn eine Erweiterung die Protokoll-API abonniert. Das folgende Beispiel zeigt eine Protokoll-Abonnementmeldung.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.logsSubscription",
    "record": {"name": "Foo.bar",
        "state": "Subscribed",
        "types": ["function", "platform"],
    }
}
```

Lambda generiert ein vom Plattformprotokoll abgelegtes Protokoll, wenn eine Erweiterung nicht in der Lage ist, die Anzahl der Protokolle zu verarbeiten, die sie empfängt. Das folgende Beispiel zeigt eine `platform.logsDropped`-Protokollmeldung.

```
{
    "time": "2020-08-20T12:31:32.123Z",
    "type": "platform.logsDropped",
    "record": {"reason": "Consumer seems to have fallen behind as it has not
 acknowledged receipt of logs.",
        "droppedRecords": 123,
        "droppedBytes" 12345
    }
}
```

Die platform.restoreStart-Protokollnachricht zeigt den Zeitpunkt an, zu dem die `Restore`-Phase begonnen hat (nur `snap-start`-Initialisierungstyp). Beispiel:

```
{
  "time":"2022-07-17T18:43:44.782Z",
```

```
  "type":"platform.restoreStart",
  "record":{}
}
```

Die platform.restoreReport-Protokollnachricht zeigt, wie lange die `Restore`-Phase gedauert hat und wie viele Millisekunden Ihnen während dieser Phase in Rechnung gestellt wurden (nur `snap-start`-Initialisierungstyp). Beispiel:

```
{
  "time":"2022-07-17T18:43:45.936Z",
  "type":"platform.restoreReport",
  "record":{
      "metrics":{
          "durationMs":70.87,
          "billedDurationMs":13
      }
  }
}
```

Plattform **`runtimeDone`**-Meldungen

Wenn Sie die Schemaversion in der Abonnementanforderung auf „2021-03-18“ setzen, schickt Lambda eine `platform.runtimeDone`-Meldung, nachdem der Funktionsaufruf entweder erfolgreich oder mit einem Fehler abgeschlossen wurde. Die Erweiterung kann diese Meldung verwenden, um die gesamte Telemetrie-Sammlung für diesen Funktionsaufruf anzuhalten.

Die OpenAPI-Spezifikation für den Protokollereignistyp in der Schemaversion 2021-03-18 ist hier verfügbar: schema-2021-03-18.zip

Lambda generiert die `platform.runtimeDone`-Protokollmeldung, wenn die Laufzeitumgebung eine `Next`- oder `Error`-Laufzeit-API-Anforderung sendet. Das `platform.runtimeDone`-Protokoll informiert die Verbraucher über die Protokoll-API, dass der Funktionsaufruf abgeschlossen ist. Erweiterungen können diese Informationen verwenden, um zu entscheiden, wann die gesamte während dieses Aufrufs gesammelte Telemetrie gesendet werden soll.

Beispiele

Lambda sendet die `platform.runtimeDone`-Meldung, nachdem die Laufzeit die NEXT-Anfrage sendet, wenn der Funktionsaufruf abgeschlossen wird. Die folgenden Beispiele zeigen Meldungen für jeden der Statuswerte: Erfolg, Misserfolg und Timeout.

Example Beispiel Erfolgsmeldung

```
{
    "time": "2021-02-04T20:00:05.123Z",
    "type": "platform.runtimeDone",
    "record": {
       "requestId":"6f7f0961f83442118a7af6fe80b88",
       "status": "success"
    }
}
```

Example Beispiel Misserfolgsmeldung

```
{
   "time": "2021-02-04T20:00:05.123Z",
   "type": "platform.runtimeDone",
   "record": {
      "requestId":"6f7f0961f83442118a7af6fe80b88",
      "status": "failure"
   }
}
```

Example Beispiel Timeout-Meldung

```
{
   "time": "2021-02-04T20:00:05.123Z",
   "type": "platform.runtimeDone",
   "record": {
      "requestId":"6f7f0961f83442118a7af6fe80b88",
      "status": "timeout"
  }
}
```

Example Beispiel für platform.restoreRuntimeDone message (**`snap-start`**nur -Initialisierungstyp)

Die platform.restoreRuntimeDone-Protokollmeldung zeigt, ob die -`Restore`Phase erfolgreich war oder nicht. Lambda sendet diese Nachricht, wenn die Laufzeit eine `restore/next`-Laufzeit-API-Anfrage sendet. Es gibt drei mögliche Status: erfolgreich, fehlgeschlagen und Timeout. Das folgende Beispiel zeigt eine erfolgreiche platform.restoreRuntimeDone-Protokollmeldung.

```
{
```

```
  "time":"2022-07-17T18:43:45.936Z",
  "type":"platform.restoreRuntimeDone",
  "record":{
      "status":"success"
  }
}
```

Beheben von Problemen in Lambda

Die folgenden Themen enthalten Ratschläge zur Fehlerbehebung bei Fehlern und Problemen, die bei der Verwendung der Lambda-API, -Konsole oder -Tools auftreten können. Wenn Sie auf ein Problem stoßen, das hier nicht aufgeführt ist, können Sie die Schaltfläche Feedback auf dieser Seite verwenden, um es zu melden.

Weitere Tipps zur Fehlerbehebung und Antworten auf häufig gestellte Supportfragen finden Sie im AWS - Wissenscenter.

Weitere Informationen zum Debuggen und zur Problembehandlung für Lambda-Anwendungen finden Sie bei Serverless Land unter Debugging.

Themen

Beheben von Bereitstellungsproblemen in Lambda

Wenn Sie Ihre Funktion aktualisieren, stellt Lambda die Änderung durch Starten der neuen Instances der Funktion mit aktualisiertem Code oder aktualisierten Einstellungen bereit. Bereitstellungsfehler verhindern die Verwendung der neuen Version und können auf Probleme mit Bereitstellungspaket, Code, Berechtigungen oder Tools zurückzuführen sein.

Wenn Sie Updates für Ihre Funktion direkt mit der Lambda-API oder mit einem Client wie dem bereitstellen AWS CLI, können Sie Fehler von Lambda direkt in der Ausgabe sehen. Wenn Sie Dienste wie AWS CloudFormation, oder verwenden AWS CodeDeploy AWS CodePipeline, suchen Sie in den Protokollen oder im Eventstream für diesen Dienst nach der Antwort von Lambda.

Die folgenden Themen enthalten Ratschläge zur Fehlerbehebung bei Fehlern und Problemen, die bei der Verwendung der Lambda-API, -Konsole oder -Tools auftreten können. Wenn Sie auf ein Problem stoßen, das hier nicht aufgeführt ist, können Sie die Schaltfläche Feedback auf dieser Seite verwenden, um es zu melden.

Weitere Tipps zur Fehlerbehebung und Antworten auf häufig gestellte Supportfragen finden Sie im AWS - Wissenscenter.

Weitere Informationen zum Debuggen und zur Problembehandlung für Lambda-Anwendungen finden Sie bei Serverless Land unter Debugging.

Themen

Allgemein: Berechtigung wird verweigert/Kann solche Datei nicht laden

Fehler: EACCES: Berechtigung verweigert. Öffnen Sie '/var/task/index.js'

Fehler: kann eine derartige Datei nicht laden – Funktion

Fehler: [Fehler 13] Berechtigung verweigert: '/var/task/function.py'

Die Lambda-Laufzeit benötigt die Berechtigung zum Lesen der Dateien in Ihrem Bereitstellungspaket. In der oktalen Schreibweise von Linux-Berechtigungen benötigt Lambda 644 Berechtigungen für nicht ausführbare Dateien (rw-r--r--) und 755 Berechtigungen () für Verzeichnisse und ausführbare Dateien. rwxr-xr-x

Verwenden Sie unter Linux und MacOS den `chmod`-Befehl, um Dateiberechtigungen für Dateien und Verzeichnisse in Ihrem Bereitstellungspaket zu ändern. Führen Sie beispielsweise den folgenden Befehl aus, um einer ausführbaren Datei die richtigen Berechtigungen zu gewähren.

```
chmod 755 <filepath>
```

Informationen zum Ändern von Dateiberechtigungen in Windows finden Sie unter Festlegen, Anzeigen, Ändern oder Entfernen von Berechtigungen für ein Objekt in der Microsoft-Windows-Dokumentation.

Allgemein: Beim Aufrufen von UpdateFunctionCode

Fehler: Beim Aufrufen der UpdateFunctionCode Operation ist ein Fehler aufgetreten (RequestEntityTooLargeException)

Wenn Sie ein Bereitstellungspaket oder ein Ebenenarchiv direkt in Lambda hochladen, ist die Größe der ZIP-Datei auf 50 MB begrenzt. Um eine größere Datei hochzuladen, speichern Sie sie in Amazon S3 und verwenden Sie die S3Bucket- und S3Key--Parameter.

> **Note**
>
> Wenn Sie eine Datei direkt mit dem AWS CLI AWS SDK oder auf andere Weise hochladen, wird die binäre ZIP-Datei in ein Base64-Format konvertiert, wodurch sich ihre Größe um etwa 30% erhöht. Um dies und die Größe anderer Parameter in der Anforderung zu ermöglichen, ist die tatsächliche von Lambda angewendete Größenbeschränkung der Anforderung größer. Aus diesem Grund ist der Grenzwert von 50 MB ein ungefährer Wert.

Amazon S3: Fehlercode PermanentRedirect.

Fehler: Während ist ein Fehler aufgetreten GetObject. S3-Fehlercode: PermanentRedirect. S3-Fehlermeldung: Der Bucket befindet sich in dieser Region: us-east-2. Verwenden Sie diese Region, um die Anfrage zu wiederholen

Wenn Sie das Bereitstellungspaket einer Funktion aus einem Amazon-S3-Bucket hochladen, muss sich der Bucket in derselben Region wie die Funktion befinden. Dieses Problem kann auftreten, wenn Sie ein Amazon S3 S3-Objekt in einem Aufruf angeben oder die Befehle package und deploy in der AWS CLI oder AWS SAM CLI verwenden. UpdateFunctionCode Erstellen Sie einen Bucket mit Bereitstellungsartefakt für jede Region, in der Sie Anwendungen entwickeln.

Allgemein: Kann nicht gefunden werden, kann nicht geladen werden, Klasse nicht gefunden, keine solche Datei oder kein Verzeichnis

Fehler: Modul 'function' kann nicht gefunden werden

Fehler: kann eine derartige Datei nicht laden – Funktion

Fehler: Modul 'function' kann nicht importiert werden

Fehler: Klasse nicht gefunden: function.Handler

Fehler: fork/exec /var/task/function: keine solche Datei oder kein solches Verzeichnis

Fehler: Der Typ 'Function.Handler' kann nicht aus der Assembly 'Function' geladen werden.'

Der Name der Datei oder Klasse in der Handler-Konfiguration Ihrer Funktion stimmt nicht mit Ihrem Code überein. Weitere Informationen finden Sie im folgenden Abschnitt.

Allgemein: Undefinierter Methodenhandler

Fehler: index.handler ist nicht definiert oder wurde nicht exportiert

Fehler: Handler 'handler' fehlt für Modul 'function'

Fehler: undefinierter Methoden−`Handler' für #<:0x000055b76ccebf98> LambdaHandler

Fehler: Keine öffentliche Methode namens handleRequest mit der entsprechenden Methodensignatur für Klasse function.Handler gefunden

Fehler: Die Methode 'handleRequest' konnte nicht im Typ 'Function.Handler' der Assembly 'Function' gefunden werden

Der Name der Handler-Methode in der Handler-Konfiguration Ihrer Funktion stimmt nicht mit Ihrem Code überein. Jede Laufzeit definiert eine Namenskonvention für Handler wie *`Dateiname`*.*`Methodenname`*. Der Handler ist die Methode im Code Ihrer Funktion, die von der Laufzeit ausführt wird, wenn Ihre Funktion aufgerufen wird.

Lambda stellt für einige Sprachen eine Bibliothek mit einer Schnittstelle bereit, die erwartet, dass eine Handler-Methode einen bestimmten Namen hat. Weitere Informationen zur Handlerbenennung für jede Sprache finden Sie in den folgenden Themen.

- Erstellen von Lambda-Funktionen mit Node.js
- Erstellen von Lambda-Funktionen mit Python
- Erstellen von Lambda-Funktionen mit Ruby

- Erstellen von Lambda-Funktionen mit Java
- Erstellen von Lambda-Funktionen mit Go
- Erstellen von Lambda-Funktionen mit C#
- Aufbau von Lambda-Funktionen mit PowerShell

Lambda: Ebenenkonvertierung ist fehlgeschlagen.

Fehler: Lambda-Ebenenkonvertierung ist fehlgeschlagen. Hinweise zur Lösung dieses Problems finden Sie auf der Seite „Beheben von Bereitstellungsproblemen in Lambda“ im Lambda-Benutzerhandbuch.

Wenn Sie eine Lambda-Funktion mit einer Ebene konfigurieren, führt Lambda die Ebene mit Ihrem Funktionscode zusammen. Wenn dieser Prozess nicht abgeschlossen wird, gibt Lambda diesen Fehler zurück. Führen Sie in diesem Fall die folgenden Schritte aus:

- Löschen Sie alle ungenutzten Dateien von Ihrer Ebene.
- Löschen Sie alle symbolischen Links in Ihrer Ebene.
- Benennen Sie alle Dateien um, die denselben Namen wie ein Verzeichnis in einer der Ebenen Ihrer Funktion haben.

Lambda: oder InvalidParameterValueException RequestEntityTooLargeException

FehlerInvalidParameterValueException: Lambda konnte Ihre Umgebungsvariablen nicht konfigurieren, da die von Ihnen angegebenen Umgebungsvariablen das Limit von 4 KB überschritten haben. Gemessene Zeichenfolge: {"A1":" USFEY5 7ATNx5BSM... cyPiPn

Fehler:RequestEntityTooLargeException: Die Anfrage muss für den Vorgang kleiner als 5120 Byte sein UpdateFunctionConfiguration

Die maximale Größe des Variablenobjekts, das in der Konfiguration der Funktion gespeichert ist, darf 4096 Bytes nicht überschreiten. Dazu gehören Schlüsselnamen, Werte, Anführungszeichen, Kommas und Klammern. Die Gesamtgröße des HTTP-Anforderungstexts ist ebenfalls begrenzt.

```
{
    "FunctionName": "my-function",
```

```
    "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-function",
    "Runtime": "nodejs20.x",
    "Role": "arn:aws:iam::123456789012:role/lambda-role",
    "Environment": {
        "Variables": {
            "BUCKET": "DOC-EXAMPLE-BUCKET",
            "KEY": "file.txt"
        }
    },
    ...
}
```

In diesem Beispiel umfasst das Objekt 39 Zeichen und benötigt 39 Bytes, wenn es als Zeichenfolge gespeichert wird (ohne Leerzeichen `{"BUCKET":"DOC-EXAMPLE-BUCKET","KEY":"file.txt"}`. Standard-ASCII-Zeichen in Umgebungsvariablenwerten verwenden jeweils ein Byte. Erweiterte ASCII- und Unicode-Zeichen können zwischen 2 und 4 Bytes pro Zeichen verwenden.

Lambda: InvalidParameterValueException

FehlerInvalidParameterValueException: Lambda konnte Ihre Umgebungsvariablen nicht konfigurieren, da die von Ihnen angegebenen Umgebungsvariablen reservierte Schlüssel enthalten, deren Änderung derzeit nicht unterstützt wird.

Lambda reserviert einige Umgebungsvariablenschlüssel zur internen Verwendung. Beispielsweise wird `AWS_REGION` von der Laufzeit verwendet, um die aktuelle Region zu bestimmen, und kann nicht außer Kraft gesetzt werden. Andere Variablen, wie z. B. `PATH`, werden von der Laufzeit verwendet, können aber in Ihrer Funktionskonfiguration erweitert werden. Eine vollständige Liste finden Sie unter Definierte Laufzeitumgebungsvariablen.

Lambda: Kontingente für Gleichzeitigkeit und Speicher

Fehler: Die ConcurrentExecutions für die Funktion angegebene Funktion senkt den Wert des Kontos UnreservedConcurrentExecution unter den Mindestwert

Fehler: Der Wert MemorySize " hat die Einschränkung nicht erfüllt: Das Element muss einen Wert haben, der kleiner oder gleich 3008 ist

Diese Fehler treten auf, wenn Sie für Ihr Konto die Kontingente für Gleichzeitigkeit oder Speicher überschreiten. Bei neuen AWS Konten wurden Parallelität und Speicherkontingente reduziert. Um

Fehler im Zusammenhang mit der Gleichzeitigkeit zu beheben, können Sie eine Kontingenterhöhung beantragen. Sie können keine Erhöhung des Speicherkontingents beantragen.

- Parallelität: Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie versuchen, eine Funktion mit reservierter oder bereitgestellter Parallelität zu erstellen, oder wenn Ihre funktionsspezifische Parallelitätsanforderung (PutFunctionConcurrency) das Parallelitätskontingent Ihres Kontos überschreitet.
- Speicher: Fehler treten auf, wenn die der Funktion zugewiesene Speichermenge das Speicherkontingent Ihres Kontos übersteigt.

Beheben von Aufruf-Problemen in Lambda

Wenn Sie eine Lambda-Funktion aufrufen, validiert Lambda die Anforderung und überprüft die Skalierungskapazität, bevor es das Ereignis an Ihre Funktion oder bei asynchronem Aufruf an die Ereigniswarteschlange sendet. Aufruffehler können durch Probleme mit Anforderungsparametern, Ereignisstruktur, Funktionseinstellungen, Benutzerberechtigungen, Ressourcenberechtigungen oder Grenzwerten verursacht werden.

Wenn Sie Ihre Funktion direkt aufrufen, sehen Sie Aufruffehler in der Antwort von Lambda. Wenn Sie Ihre Funktion asynchron mit einer Ereignisquellen-Zuweisung oder über einen anderen Service aufrufen, finden Sie möglicherweise Fehler in Protokollen, eine Warteschlange für unzustellbare Nachrichten oder ein Ziel für fehlerhafte Ereignisse. Die Optionen für die Fehlerbehandlung und das Wiederholungsverhalten variieren je nachdem, wie Sie Ihre Funktion aufrufen, und nach der Art des Fehlers.

Eine Liste der Fehlertypen, die der `Invoke`-Vorgang zurückgeben kann, finden Sie unter Aufrufen.

IAM: lambda:InvokeFunction not authorized

Fehler: Benutzer: arn:aws:iam::123456789012:user/developer ist nicht autorisiert, Folgendes auszuführen: lambda:InvokeFunction on-Ressource: my-function

Ihr Benutzer oder die Rolle, die Sie annehmen, muss über die Berechtigung zum Aufrufen einer Funktion verfügen. Diese Anforderung gilt auch für Lambda-Funktionen und andere Datenverarbeitungsressourcen, die Funktionen aufrufen. Fügen Sie Ihrem AWSLambdaRole Benutzer die AWS verwaltete Richtlinie oder eine benutzerdefinierte Richtlinie hinzu, die die `lambda:InvokeFunction` Aktion für die Zielfunktion zulässt.

> **Note**
>
> Der Name der IAM-Aktion (`lambda:InvokeFunction`) bezieht sich auf den `Invoke`-Lambda-API-Vorgang.

Weitere Informationen finden Sie unter Verwaltung von Berechtigungen in AWS Lambda.

Lambda: Gültiges Bootstrap konnte nicht gefunden werden (LaufzeitInvalidEntrypoint).

Fehler: Kein gültiger Bootstrap gefunden: [/var/task/bootstrap /opt/bootstrap]

Dieser Fehler tritt normalerweise auf, wenn das Stammverzeichnis Ihres Bereitstellungspakets keine ausführbare Datei mit dem Namen `bootstrap` enthält. Wenn Sie beispielsweise eine `provided.al2023`-Funktion über eine ZIP-Datei bereitstellen, muss sich die `bootstrap`-Datei im Stammverzeichnis der ZIP-Datei befinden, nicht in einem Verzeichnis.

Lambda: Der Vorgang kann nicht ausgeführt werden ResourceConflictException

Fehler: ResourceConflictException: Der Vorgang kann derzeit nicht ausgeführt werden. Die Funktion befindet sich derzeit in folgendem Zustand: Ausstehend

Wenn Sie zum Zeitpunkt der Erstellung eine Funktion mit einer Virtual Private Cloud (VPC) verbinden, wechselt die Funktion in einen `Pending`-Zustand, während Lambda Elastic-Network-Schnittstellen erstellt. Während dieser Zeit können Sie Ihre Funktion nicht aufrufen oder ändern. Wenn Sie Ihre Funktion nach der Erstellung mit einer VPC verbinden, können Sie sie aufrufen, während das Update aussteht, aber Sie können den Code oder die Konfiguration nicht ändern.

Weitere Informationen finden Sie unter Lambda-Funktionszustände.

Lambda: Funktion bleibt im Status Pending

Fehler: Eine Funktion bleibt mehrere Minuten im *`Pending`*-Zustand.

Wenn eine Funktion länger als sechs Minuten im `Pending`-Zustand ist, rufen Sie eine der folgenden API-Operationen auf, um die Blockierung aufzuheben.

- UpdateFunctionCode

- UpdateFunctionConfiguration
- PublishVersion

Lambda bricht den ausstehenden Vorgang ab und versetzt die Funktion in den `Failed`-Zustand. Sie können dann versuchen, eine weitere Aktualisierung durchzuführen.

Lambda: Eine Funktion verwendet alle Parallelität

Problem: Eine Funktion verwendet die gesamte verfügbare Gleichzeitigkeit, wodurch andere Funktionen gedrosselt werden.

Um die verfügbare Gleichzeitigkeit Ihres AWS Kontos in einer - AWS Region in Pools aufzuteilen, verwenden Sie die reservierte Gleichzeitigkeit . Durch reservierte Gleichzeitigkeit wird sichergestellt, dass eine Funktion immer auf ihre zugewiesene Gleichzeitigkeit skalieren kann und nicht über die zugewiesene Gleichzeitigkeit hinaus skaliert wird.

Allgemein: Funktion kann nicht mit anderen Konten oder Diensten aufgerufen werden

Problem: Sie können Ihre Funktion direkt aufrufen. Sie wird jedoch nicht ausgeführt, wenn sie von einem anderen Service oder Konto aufgerufen wird.

Sie erteilen anderen Services und Konten die Berechtigung zum Aufrufen einer Funktion in der ressourcenbasierten Richtlinieder Funktion. Wenn sich der Aufrufer in einem anderen Konto befindet, benötigt dieser Benutzer auch die Berechtigung zum Aufrufen von Funktionen.

Allgemein: Funktionsaufruf bleibt im Looping

Problem: Die Funktion wird kontinuierlich in einer Schleife aufgerufen.

Dies tritt in der Regel auf, wenn Ihre Funktion Ressourcen in demselben AWS Service verwaltet, der sie auslöst. Beispielsweise ist es möglich, eine Funktion zu erstellen, die ein Objekt in einem Bucket von Amazon Simple Storage Service (Amazon S3) speichert, der mit einer Benachrichtigung konfiguriert ist, die die Funktion erneut aufruft. Um die Ausführung der Funktion zu beenden, reduzieren Sie die verfügbare Gleichzeitigkeit auf Null, wodurch alle zukünftigen Aufrufe gedrosselt werden. Identifizieren Sie dann den Codepfad oder Konfigurationsfehler, der den rekursiven Aufruf verursacht hat. Lambda erkennt und stoppt automatisch rekursive Schleifen für einige AWS Services und SDKs. Weitere Informationen finden Sie unter the section called “Erkennung rekursiver Schleifen”.

Lambda: Alias-Routing mit bereitgestellter Parallelität

Problem: Bereitgestellte Parallelitäts-Überlauf-Aufrufe während des Alias-Routings.

Lambda verwendet ein einfaches probabilistisches Modell, um den Datenverkehr zwischen den beiden Funktionsversionen zu verteilen. Bei niedrigem Datenverkehr sehen Sie möglicherweise eine hohe Abweichung zwischen dem konfigurierten und dem tatsächlichen Prozentsatz des Datenverkehrs für jede Version. Wenn Ihre Funktion bereitgestellte Parallelität verwendet, können Sie Überlaufaufrufe durch Konfigurieren einer höheren Anzahl von bereitgestellten Parallelitätsinstances während des aktiven Alias-Routings vermeiden.

Lambda: Kaltstarts mit bereitgestellter Parallelität

Problem: Sie erleben Kaltstarts nach dem Aktivieren der bereitgestellten Parallelität.

Wenn die Anzahl der gleichzeitigen Ausführungen einer Funktion kleiner oder gleich der konfigurierten Ebene der bereitgestellten Parallelität ist, sollte es keine Kaltstarts geben. Um Ihnen zu helfen zu bestätigen, ob die bereitgestellte Parallelität normal funktioniert, gehen Sie wie folgt vor:

- Überprüfen Sie, ob die bereitgestellte Parallelität auf der Funktionsversion oder dem Alias aktiviert ist.

  > **Note**
  >
  > Die bereitgestellte Gleichzeitigkeit kann in der unveröffentlichten Version der Funktion nicht konfiguriert werden.

- Stellen Sie sicher, dass Ihre Auslöser die richtige Funktionsversion oder den richtigen Alias aufrufen. Wenn Sie zum Beispiel Amazon API Gateway verwenden, überprüfen Sie, dass Amazon API die Funktionsversion oder den Alias mit bereitgestellter Parallelität aufruft, nicht $LATEST. Um zu bestätigen, dass die bereitgestellte Gleichzeitigkeit verwendet wird, können Sie die ProvisionedConcurrencyInvocations Amazon- CloudWatch Metrik überprüfen. Ein Wert ungleich Null gibt an, dass die Funktion Aufrufe in initialisierten Ausführungsumgebungen verarbeitet.
- Stellen Sie fest, ob Ihre Funktionsgleichzeitigkeit die konfigurierte Ebene der bereitgestellten Gleichzeitigkeit überschreitet, indem Sie die ProvisionedConcurrencySpilloverInvocations CloudWatch Metrik überprüfen. Ein Wert ungleich Null gibt an, dass die gesamte bereitgestellte Parallelität verwendet wird und einige Aufrufe mit einem Kaltstart stattgefunden haben.
- Überprüfen Sie Ihre Aufrufhäufigkeit (Anfragen pro Sekunde) Funktionen mit bereitgestellter Parallelität haben eine maximale Rate von 10 Anfragen pro Sekunde pro bereitgestellte Parallelität.

Beispielsweise kann eine Funktion, die mit 100 bereitgestellter Parallelität konfiguriert ist, 1.000 Anfragen pro Sekunde bearbeiten. Wenn die Aufrufrate 1.000 Anfragen pro Sekunde übersteigt, kann es zu Kaltstarts kommen.

Lambda: Kaltstarts mit neuen Versionen

Problem: Sie erleben Kaltstarts, wenn Sie neue Versionen Ihrer Funktion bereitstellen.

Wenn Sie einen Funktionsalias aktualisieren, verschiebt Lambda die bereitgestellte Parallelität basierend auf den für den Alias konfigurierten Gewichtungen automatisch auf die neue Version.

Fehler: KMS DisabledException: Lambda konnte die Umgebungsvariablen nicht entschlüsseln, da der verwendete KMS-Schlüssel deaktiviert ist. Bitte überprüfen Sie die KMS-Schlüsseleinstellungen der Funktion.

Dieser Fehler kann auftreten, wenn Ihr AWS Key Management Service (AWS KMS)-Schlüssel deaktiviert ist oder wenn die Erteilung, die Lambda die Verwendung des Schlüssels erlaubt, widerrufen wird. Wenn die Gewährung fehlt, konfigurieren Sie die Funktion so, dass sie einen anderen Schlüssel verwendet. Weisen Sie dann den benutzerdefinierten Schlüssel neu zu, um die Erteilung neu zu erstellen.

EFS: Die Funktion konnte das EFS-Dateisystem nicht mounten

Fehler: EFSMountFailureException : Die Funktion konnte das EFS-Dateisystem nicht mit dem Zugriffspunkt arn:aws:elasticfilesystem:us-east-2:123456789012:access-point/fsap-015cxmplb72b405fd mounten.

Die Mounting-Anforderung der Funktion an das Dateisystem wurde abgelehnt. Überprüfen Sie die Berechtigungen der Funktion und bestätigen Sie, dass das Dateisystem und der Zugriffspunkt vorhanden und einsatzbereit sind.

EFS: Die Funktion konnte keine Verbindung zum EFS-Dateisystem herstellen

Fehler: EFSMountConnectivityException : Die Funktion konnte keine Verbindung zum Amazon-EFS-Dateisystem mit dem Zugriffspunkt arn:aws:elasticfilesystem:us-east- 2:123456789012:access-point/fsap-015cxmplb72b405fd herstellen. Überprüfen Sie die Netzwerkkonfiguration und versuchen Sie es erneut.

Die Funktion konnte keine Verbindung zum Dateisystem der Funktion mit dem NFS-Protokoll (TCP-Port 2049) herstellen. Überprüfen Sie die Sicherheitsgruppe und die Routingkonfiguration für die Subnetze der VPC.

Wenn Sie diese Fehler erhalten, nachdem Sie die VPC-Konfigurationseinstellungen Ihrer Funktion aktualisiert haben, versuchen Sie, das Mounting und das erneute Mounting des Dateisystems aufzuheben.

EFS: Die Funktion konnte das EFS-Dateisystem aufgrund eines Timeouts nicht mounten

Fehler: EFSMountTimeoutException : Die Funktion konnte das EFS-Dateisystem mit dem Zugriffspunkt {arn:aws:elasticfilesystem:us-east- 2:123456789012:access-point/fsap-015cxmplb72b405fd} aufgrund einer Mounting-Zeitüberschreitung nicht mounten.

Die Funktion konnte eine Verbindung mit dem Dateisystem der Funktion herstellen, aber bei der Mounting-Operation trat eine Zeitüberschreitung auf. Versuchen Sie es nach kurzer Zeit erneut und erwägen Sie, die Nebenläufigkeit der Funktion zu begrenzen, um die Belastung des Dateisystems zu reduzieren.

Lambda: Lambda hat einen IO-Prozess erkannt, der zu lange dauerte

EFSIOException: Diese Funktions-Instance wurde angehalten, da Lambda einen I/O-Prozess erkannt hat, der zu lange gedauert hat.

Bei einem vorherigen Aufruf trat eine Zeitüberschreitung auf und Lambda konnte den Funktions-Handler nicht beenden. Dieses Problem kann auftreten, wenn ein angehängtes Dateisystem keine Burst-Credits hat und der Basisdurchsatz nicht ausreicht. Um den Durchsatz zu erhöhen, können Sie die Größe des Dateisystems erhöhen oder den bereitgestellten Durchsatz verwenden. Weitere Informationen finden Sie unter Durchsatz.

Beheben von Ausführungsproblemen in Lambda

Wenn die Lambda-Laufzeitumgebung Ihren Funktionscode ausführt, wird das Ereignis möglicherweise auf einer Instance der Funktion verarbeitet, auf der schon länger Ereignisse verarbeitet werden, oder muss möglicherweise eine neue Instance initialisiert werden. Fehler können während der Funktionsinitialisierung, wenn Ihr Handler-Code das Ereignis verarbeitet oder wenn Ihre Funktion eine Antwort zurückgibt (oder nicht zurückgibt), auftreten.

Funktionsausführungsfehler können durch Probleme mit Code, Funktionskonfiguration, nachgeschalteten Ressourcen oder Berechtigungen verursacht werden. Wenn Sie Ihre Funktion direkt aufrufen, sehen Sie Funktionsfehler in der Antwort von Lambda. Wenn Sie Ihre Funktion asynchron mit einer Ereignisquellen-Zuweisung oder über einen anderen Service aufrufen, finden Sie möglicherweise Fehler in Protokollen, eine Warteschlange für unzustellbare Nachrichten oder ein Ziel bei Ausfall. Die Optionen für die Fehlerbehandlung und das Wiederholungsverhalten variieren je nachdem, wie Sie Ihre Funktion aufrufen, und nach der Art des Fehlers.

Wenn Ihr Funktionscode oder die Lambda-Laufzeit einen Fehler zurückgibt, ist der Statuscode in der Antwort von Lambda „200 OK“. Das Vorhandensein eines Fehlers in der Antwort wird durch einen Header namens `X-Amz-Function-Error` angezeigt. Statuscodes der Serien 400 und 500 sind für Aufruffehler reserviert.

Lambda: Die Ausführung dauert zu lange

Problem: Die Ausführung der Funktion dauert zu lange.

Wenn die Ausführung Ihres Codes in Lambda viel länger dauert als auf Ihrem lokalen Computer, kann er durch den der Funktion zur Verfügung stehenden Speicher oder die Rechenleistung eingeschränkt sein. Konfigurieren Sie die Funktion mit zusätzlichem Arbeitsspeicher, um sowohl Arbeitsspeicher als auch CPU zu erhöhen.

Lambda: Protokolle oder Ablaufverfolgungen erscheinen nicht

Problem: Protokolle werden nicht in CloudWatch Logs angezeigt.

Problem: Spuren erscheinen nicht in AWS X-Ray.

Ihre Funktion benötigt die Erlaubnis, CloudWatch Logs und X-Ray aufzurufen. Aktualisieren Sie die Ausführungsrolle, um ihr die Berechtigung zu erteilen. Fügen Sie die folgenden verwalteten Richtlinien hinzu, um Protokolle und Ablaufverfolgung zu aktivieren.

- AWSLambdaBasicExecutionRole
- AWSXRayDaemonWriteAccess

Wenn Sie Ihrer Funktion Berechtigungen hinzufügen, führen Sie auch eine einfache Aktualisierung des Codes oder der Konfiguration durch. Dies zwingt ausgeführte Instances Ihrer Funktion, die veraltete Anmeldeinformationen haben, anzuhalten und ersetzt zu werden.

> **Note**
>
> Es kann 5 bis 10 Minuten dauern, bis Protokolle nach einem Funktionsaufruf angezeigt werden.

Lambda: Nicht alle Protokolle meiner Funktion werden angezeigt

Problem: Funktionsprotokolle fehlen in den CloudWatch Protokollen, obwohl meine Berechtigungen korrekt sind

Wenn Ihr System die Kontingentgrenzen für CloudWatch Logs AWS-Konto erreicht, wird die Funktionsprotokollierung CloudWatch gedrosselt. In diesem Fall werden einige der von Ihren Funktionen ausgegebenen Protokolle möglicherweise nicht in CloudWatch den Protokollen angezeigt.

Wenn Ihre Funktion Logs mit einer zu hohen Rate ausgibt, als dass Lambda sie verarbeiten könnte, kann dies auch dazu führen, dass Protokollausgaben nicht in CloudWatch Logs erscheinen. Wenn Lambda Protokolle nicht mit der Geschwindigkeit senden kann, CloudWatch an die Ihre Funktion sie generiert, werden Protokolle gelöscht, um zu verhindern, dass die Ausführung Ihrer Funktion verlangsamt wird.

Wenn Ihre Funktion für die Verwendung von Protokollen im JSON-Format konfiguriert ist, versucht Lambda, beim Löschen von Protokollen ein `logsDropped`Ereignis an CloudWatch Logs zu senden. Wenn jedoch die Protokollierung Ihrer Funktion CloudWatch gedrosselt wird, erreicht dieses Ereignis möglicherweise nicht CloudWatch Logs, sodass Sie nicht immer einen Datensatz sehen, wenn Lambda Logs löscht.

Gehen Sie wie folgt vor, um zu überprüfen, ob Ihr System die Kontingentgrenzen für CloudWatch Logs erreicht AWS-Konto hat:

1. Öffnen Sie die Service Quotas-Konsole.
2. Wählen Sie im Navigationsbereich AWS -Services.
3. Suchen Sie in der AWS Serviceliste nach Amazon CloudWatch Logs.
4. Wählen Sie in der Liste mit den Service Quotas die Kontingente `CreateLogGroup throttle limit in transactions per second`, `CreateLogStream throttle limit in transactions per second` und `PutLogEvents throttle limit in transactions per second` aus, um die Auslastung anzuzeigen.

Sie können auch CloudWatch Alarme einrichten, die Sie benachrichtigen, wenn Ihre Kontoauslastung ein von Ihnen für diese Kontingente festgelegtes Limit überschreitet. Weitere Informationen finden Sie unter Einen CloudWatch Alarm auf der Grundlage eines statischen Schwellenwerts erstellen.

Wenn die standardmäßigen Kontingentgrenzen für CloudWatch Logs für Ihren Anwendungsfall nicht ausreichen, können Sie eine Erhöhung des Kontingents beantragen.

Lambda: Die Funktion kehrt zurück, bevor die Ausführung beendet ist

Problem: (Node.js) Rückgabe der Funktion erfolgt, bevor Code ausgeführt wird

Viele Bibliotheken, einschließlich des AWS SDK, arbeiten asynchron. Wenn Sie einen Netzwerkaufruf tätigen oder einen anderen Vorgang ausführen, für den auf eine Antwort gewartet werden muss, geben Bibliotheken ein Objekt zurück, das als Zusage bezeichnet wird und mit dem der Status der Operation im Hintergrund nachverfolgt wird.

Um zu warten, bis die Zusage in eine Antwort aufgelöst wird, verwenden Sie das Schlüsselwort `await`. Dadurch wird verhindert, dass der Handler-Code ausgeführt wird, bis die Zusage in ein Objekt aufgelöst wird, das die Antwort enthält. Wenn Sie die Daten aus der Antwort in Ihrem Code nicht verwenden müssen, können Sie die Zusage direkt an die Laufzeit zurückgeben.

Einige Bibliotheken geben keine Zusagen zurück, können aber in Code verpackt werden, der dies tut. Weitere Informationen finden Sie unter Definieren Sie den Lambda-Funktionshandler in Node.js.

AWS SDK: Versionen und Updates

Problem: Das in der Runtime enthaltene AWS SDK ist nicht die neueste Version

Problem: Das in der Runtime enthaltene AWS SDK wird automatisch aktualisiert

Die Laufzeiten für Skriptsprachen beinhalten das AWS SDK und werden regelmäßig auf die neueste Version aktualisiert. Die aktuelle Version einer jeden Laufzeit ist auf der Seite der Laufzeiten aufgeführt. Um eine neuere Version des AWS SDK zu verwenden oder Ihre Funktionen an eine bestimmte Version zu binden, können Sie die Bibliothek mit Ihrem Funktionscode bündeln oder eine Lambda-Schicht erstellen. Weitere Informationen zum Erstellen eines Bereitstellungspakets mit Abhängigkeiten finden Sie in den folgenden Themen:

Node.js

- Bereitstellen von Node.js Lambda-Funktionen mit ZIP-Dateiarchiven

Python

- Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen

Ruby

- Arbeiten mit ZIP-Dateiarchiven für Ruby-Lambda-Funktionen

Java

- Bereitstellen von Java-Lambda-Funktionen mit ZIP- oder JAR-Dateiarchiven

Go

- Bereitstellen von Lambda-Go-Funktionen mit ZIP-Dateiarchiven

C#

- Erstellen und Bereitstellen von C#-Lambda-Funktionen mit ZIP-Dateiarchiven

PowerShell

- Bereitstellen von PowerShell Lambda-Funktionen mit ZIP-Dateiarchiven

Python: Bibliotheken werden falsch geladen

Problem: (Python) Einige Bibliotheken werden nicht korrekt aus dem Bereitstellungspaket geladen

Bibliotheken mit Erweiterungsmodulen, die in C oder C ++ geschrieben sind, müssen in einer Umgebung mit derselben Prozessorarchitektur wie Lambda (Amazon Linux) kompiliert werden. Weitere Informationen finden Sie unter Arbeiten mit ZIP-Dateiarchiven und Python-Lambda-Funktionen.

Beheben von Netzwerkproblemen in Lambda

Standardmäßig führt Lambda Ihre Funktionen in einer internen Virtual Private Cloud (VPC) mit Konnektivität zu AWS -Services und dem Internet aus. Um auf lokale Netzwerkressourcen zuzugreifen, können Sie Ihre Funktion so konfigurieren, dass sie sich mit einer VPC in Ihrem Konto verbindet. Wenn Sie diese Funktion verwenden, verwalten Sie den Internetzugriff und die Netzwerkkonnektivität der Funktion mit Ressourcen von Amazon Virtual Private Cloud (Amazon VPC).

Netzwerkverbindungsfehler können auf Probleme mit der Routing-Konfiguration Ihrer VPC, den Sicherheitsgruppenregeln, AWS Identity and Access Management (IAM) -Rollenberechtigungen

oder der Network Address Translation (NAT) oder auf die Verfügbarkeit von Ressourcen wie IP-Adressen oder Netzwerkschnittstellen zurückzuführen sein. Je nach Problem wird möglicherweise ein bestimmter Fehler oder Timeout angezeigt, wenn eine Anfrage ihr Ziel nicht erreichen kann.

VPC: Funktion verliert Internetzugriff oder läuft ab

Problem: Ihre Lambda-Funktion verliert Internetzugriff nach der Verbindung mit einer VPC.

Fehler: Fehler: Verbindung ETIMEDOUT 176.32.98.189:443

Fehler: Fehler: Zeitüberschreitung der Aufgabe nach 10,00 Sekunden

FehlerReadTimeoutError: Timeout beim Lesen. (Timeout beim Lesen = 15)

Wenn Sie eine Funktion mit einer VPC verbinden, werden alle ausgehenden Anforderungen über die VPC geleitet. Um eine Verbindung zum Internet herzustellen, konfigurieren Sie Ihre VPC so, dass ausgehender Datenverkehr aus dem Subnetz der Funktion an ein NAT-Gateway in einem öffentlichen Subnetz gesendet wird. Weitere Informationen und VPC-Beispielkonfigurationen finden Sie unter the section called “Internetzugang für VPC-Funktionen”.

Wenn einige Ihrer TCP-Verbindungen eine Zeitüberschreitung haben, kann dies auf die Paketfragmentierung zurückzuführen sein. Lambda-Funktionen können eingehende fragmentierte TCP-Anfragen nicht verarbeiten, da Lambda keine IP-Fragmentierung für TCP oder ICMP unterstützt.

VPC: Die Funktion benötigt Zugriff auf AWS Dienste, ohne das Internet zu nutzen

Problem: Ihre Lambda-Funktion benötigt Zugriff auf AWS Dienste, ohne das Internet zu nutzen.

Verwenden Sie VPC-Endpunkte, um eine Funktion mit AWS Diensten aus einem privaten Subnetz ohne Internetzugang zu verbinden.

VPC: Grenzwert für Elastic-Network-Schnittstellen erreicht

Fehler: ENILimitReachedException: Das elastic network interface Network-Schnittstellenlimit wurde für die VPC der Funktion erreicht.

Wenn Sie eine Funktion mit einer Lambda-VPC verbinden, erstellt Lambda für jede Kombination aus Subnetz und Sicherheitsgruppe, die der Funktion zugeordnet ist, eine Elastic-Network-Schnittstelle.

Das Standard-Servicekontingent beträgt 250 Netzwerkschnittstellen pro VPC. Zum Anfordern einer Erhöhung für ein Kontingent können Sie die Service-Quotas-Konsole verwenden.

EC2: Elastische Netzwerkschnittstelle mit dem Typ „Lambda“

Fehlercode: Client. OperationNotPermitted

Fehlermeldung: Die Sicherheitsgruppe kann für diesen Schnittstellentyp nicht geändert werden

Sie erhalten diesen Fehler, wenn Sie versuchen, eine Elastic-Network-Schnittstelle (ENI) zu ändern, das von Lambda verwaltet wird. Das `ModifyNetworkInterfaceAttribute` ist nicht in der Lambda-API für Aktualisierungsvorgänge auf elastischen Netzwerkschnittstellen enthalten, die von Lambda erstellt wurden.

AWS Lambda Anwendungen

Eine AWS Lambda Anwendung ist eine Kombination aus Lambda-Funktionen, Ereignisquellen und anderen Ressourcen, die zusammenarbeiten, um Aufgaben auszuführen. Sie können andere Tools verwenden AWS CloudFormation , um die Komponenten Ihrer Anwendung in einem einzigen Paket zusammenzufassen, das als eine Ressource bereitgestellt und verwaltet werden kann. Anwendungen machen Ihre Lambda-Projekte portabel und ermöglichen Ihnen die Integration mit zusätzlichen Entwicklertools wie AWS CodePipeline AWS CodeBuild, und der AWS Serverless Application Model Befehlszeilenschnittstelle (AWS SAM CLI).

AWS Serverless Application Repository stellt eine Sammlung von Lambda-Anwendungen zur Verfügung, die Sie in Ihrem Konto mit nur wenigen Klicks bereitstellen können. Das Repository enthält sowohl ready-to-use Anwendungen als auch Beispiele, die Sie als Ausgangspunkt für Ihre eigenen Projekte verwenden können. Sie können auch eigenen Projekte für die Aufnahme übermitteln.

Mit AWS CloudFormation können Sie eine Vorlage erstellen, die die Ressourcen Ihrer Anwendung definiert und Ihnen die Verwaltung der Anwendung als Stack ermöglicht. Sie können Ressourcen Ihrem Anwendungs-Stack hinzufügen oder ändern und profitieren dabei von mehr Sicherheit. Wenn ein Teil eines Updates fehlschlägt, AWS CloudFormation wird automatisch zur vorherigen Konfiguration zurückgesetzt. Mithilfe von AWS CloudFormation Parametern können Sie aus derselben Vorlage mehrere Umgebungen für Ihre Anwendung erstellen. AWS SAMerweitert AWS CloudFormation mit einer vereinfachten Syntax, die sich auf die Entwicklung von Lambda-Anwendungen konzentriert.

Die AWS CLI und AWS SAM -CLI sind Befehlszeilentools zum Verwalten von Lambda-Anwendungs-Stacks. Zusätzlich zu Befehlen für die Verwaltung von Anwendungsstapeln mit der AWS CloudFormation API AWS CLI unterstützt sie Befehle auf höherer Ebene, die Aufgaben wie das Hochladen von Bereitstellungspaketen und das Aktualisieren von Vorlagen vereinfachen. Die AWS SAM CLI bietet zusätzliche Funktionen, darunter die Validierung von Vorlagen, lokales Testen und die Integration in CI/CD-Systeme.

Wenn Sie eine Anwendung erstellen, können Sie ihr Git-Repository entweder mit CodeCommit oder mit einer AWS CodeStar Verbindung zu erstellen GitHub. CodeCommit ermöglicht es Ihnen, die IAM-Konsole zur Verwaltung von SSH-Schlüsseln und HTTP-Anmeldeinformationen für Ihre Benutzer zu verwenden. CodeConnections ermöglicht es Ihnen, eine Verbindung zu Ihrem GitHub Konto herzustellen. Weitere Informationen zu Verbindungen finden Sie unter Was sind Verbindungen? im Benutzerhandbuch zur Entwickler-Tools-Konsole.

Weitere Informationen zum Entwerfen von Lambda-Anwendungen finden Sie bei Serverless Land unter Application design.

Themen

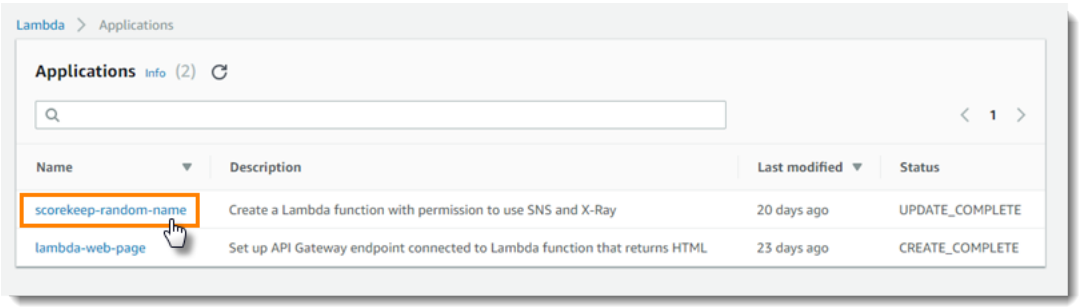
- Verwalten von Anwendungen in der AWS Lambda-Konsole
- Erstellen Sie fortlaufende Bereitstellungen für Lambda-Funktionen
- Verwendung von Lambda mit Kubernetes

Verwalten von Anwendungen in der AWS Lambda-Konsole

Die AWS Lambda-Konsole unterstützt Sie bei der Überwachung und Verwaltung Ihrer Lambda-Anwendungen. Das Menü Anwendungen führt AWS CloudFormation-Stacks mit Lambda-Funktionen auf. Das Menü enthält Stacks, die Sie in AWS CloudFormation über die AWS CloudFormation-Konsole, AWS Serverless Application Repository, die AWS CLI oder die AWS SAM-CLI starten.

So zeigen Sie eine Lambda-Anwendung an

1. Öffnen Sie die Seite Anwendungen der Lambda-Konsole.
2. Wählen Sie eine Anwendung aus.



Die Übersicht enthält die folgenden Informationen zu Ihrer Anwendung.

- AWS CloudFormation-Vorlage oder SAM-Vorlage – Die Vorlage, die Ihre Anwendung definiert.
- Ressourcen – Die AWS-Ressourcen, die von der Vorlage Ihrer Anwendung definiert werden. Zum Verwalten der Lambda-Funktionen Ihrer Anwendung wählen Sie einen Funktionsnamen in der Liste aus.

Überwachen von Anwendungen

Auf der Registerkarte Überwachung wird ein Amazon CloudWatch -Dashboard mit aggregierten Metriken für die Ressourcen in Ihrer Anwendung angezeigt.

So überwachen Sie eine Lambda-Anwendung

1. Öffnen Sie die Seite Anwendungen der Lambda-Konsole.
2. Wählen Sie Monitoring.

Standardmäßig zeigt die Lambda-Konsole ein grundlegendes Dashboard an. Sie können diese Seite anpassen, indem Sie benutzerdefinierte Dashboards in Ihrer Anwendungsvorlage definieren. Wenn Ihre Vorlage ein oder mehrere Dashboards enthält, zeigt die Seite Ihre Dashboards anstelle des Standard-Dashboards an. Sie mit dem Dropdown-Menü oben rechts auf der Seite zwischen Dashboards wechseln.

Benutzerdefinierte Überwachungs-Dashboards

Passen Sie Ihre Anwendungsüberwachungsseite an, indem Sie Ihrer Anwendungsvorlage ein oder mehrere Amazon- CloudWatch Dashboards mit dem AWS::CloudWatch::Dashboard Ressourcentyp hinzufügen. Das folgende Beispiel erstellt ein Dashboard mit einem einzigen Widget, das die Anzahl der Aufrufe einer Funktion mit dem Namen grafisch darstell `my-function`.

Example Dashboard-Funktionsvorlage

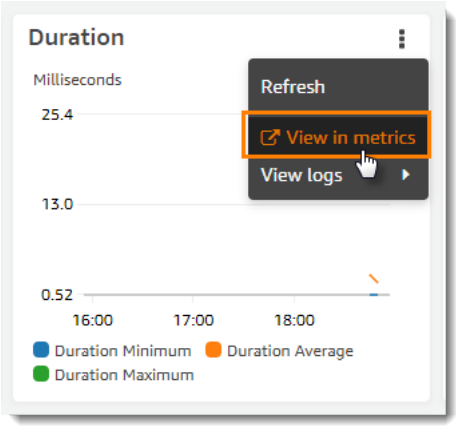
```
Resources:
  MyDashboard:
    Type: AWS::CloudWatch::Dashboard
    Properties:
      DashboardName: my-dashboard
      DashboardBody: |
        {
            "widgets": [
                {
                    "type": "metric",
                    "width": 12,
                    "height": 6,
                    "properties": {
                        "metrics": [
                            [
                                "AWS/Lambda",
                                "Invocations",
                                "FunctionName",
                                "my-function",
                                {
                                    "stat": "Sum",
                                    "label": "MyFunction"
                                }
                            ],
                            [
                                {
                                    "expression": "SUM(METRICS())",
```

```
                                "label": "Total Invocations"
                            }
                        ]
                    ],
                    "region": "us-east-1",
                    "title": "Invocations",
                    "view": "timeSeries",
                    "stacked": false
                }
            }
        ]
    }
```

Sie können die Definition für eines der Widgets im Standardüberwachsungs-Dashboard der CloudWatch-Konsole überwachen.

So zeigen Sie eine Widget-Definition an

1. Öffnen Sie die Seite Anwendungen der Lambda-Konsole.
2. Wählen Sie eine Anwendung mit dem Standard-Dashboard.
3. Wählen Sie Monitoring.
4. Wählen Sie für ein Widget View in metrics (In Metriken anzeigen) aus dem Dropdown-Menü aus.



5. Wählen Sie Source aus.

Weitere Informationen zum Erstellen von CloudWatch Dashboards und Widgets finden Sie unter Dashboard-Textstruktur und Syntax in der Amazon CloudWatch -API-Referenz .

Erstellen Sie fortlaufende Bereitstellungen für Lambda-Funktionen

Verwenden Sie fortlaufende Bereitstellungen, um die Risiken zu kontrollieren, die mit der Einführung neuer Versionen Ihrer Lambda-Funktion verbunden sind. In einer fortlaufenden Bereitstellung stellt das System automatisch die neue Version der Funktion bereit und sendet schrittweise eine zunehmende Menge an Datenverkehr an die neue Version. Der Datenverkehr und die Erhöhungsrate sind Parameter, die Sie konfigurieren können.

Sie konfigurieren eine fortlaufende Bereitstellung mithilfe AWS CodeDeploy von und. AWS SAM CodeDeploy ist ein Service, der Anwendungsbereitstellungen auf Amazon-Computerplattformen wie Amazon EC2 und automatisiert. AWS LambdaWeitere Informationen finden Sie unter Was ist? CodeDeploy . Durch CodeDeploy die Bereitstellung Ihrer Lambda-Funktion können Sie den Status der Bereitstellung auf einfache Weise überwachen und ein Rollback einleiten, falls Sie Probleme feststellen.

AWS SAM ist ein Open-Source-Framework für die Erstellung serverloser Anwendungen. Sie erstellen eine AWS SAM Vorlage (im YAML-Format), um die Konfiguration der Komponenten anzugeben, die für die fortlaufende Bereitstellung erforderlich sind. AWS SAM verwendet die Vorlage, um die Komponenten zu erstellen und zu konfigurieren. Weitere Informationen finden Sie unter Was ist AWS SAM?

AWS SAM Führt in einer fortlaufenden Bereitstellung die folgenden Aufgaben aus:

- Es konfiguriert Ihre Lambda-Funktion und erstellt einen Alias.

  Die Alias-Weiterleitungskonfiguration ist die zugrunde liegende Funktion, die die fortlaufende Bereitstellung implementiert.
- Es erstellt eine CodeDeploy Anwendungs- und Bereitstellungsgruppe.

  Die Bereitstellungsgruppe verwaltet die fortlaufende Bereitstellung und das Rollback (falls erforderlich).
- Sie erkennt, wenn Sie eine neue Version Ihrer Lambda-Funktion erstellen.
- Es wird ausgelöst CodeDeploy , um die Bereitstellung der neuen Version zu starten.

Beispiel für eine AWS SAM Lambda-Vorlage

Das folgende Beispiel zeigt eine AWS SAM -Vorlage für eine einfache fortlaufende Bereitstellung.

```
AWSTemplateFormatVersion : '2010-09-09'
Transform: AWS::Serverless-2016-10-31
Description: A sample SAM template for deploying Lambda functions.

Resources:
# Details about the myDateTimeFunction Lambda function
  myDateTimeFunction:
    Type: AWS::Serverless::Function
    Properties:
      Handler: myDateTimeFunction.handler
      Runtime: nodejs18.x
# Creates an alias named "live" for the function, and automatically publishes when you
 update the function.
      AutoPublishAlias: live
      DeploymentPreference:
# Specifies the deployment configuration
          Type: Linear10PercentEvery2Minutes
```

Diese Vorlage definiert eine Lambda-Funktion mit der Bezeichnung `myDateTimeFunction` und den folgenden Eigenschaften.

AutoPublishAlias

Die `AutoPublishAlias`-Eigenschaft erstellt einen Alias mit der Bezeichnung `live`. Darüber hinaus erkennt das AWS SAM -Framework automatisch, wenn Sie neuen Code für die Funktion speichern. Das Framework veröffentlicht dann eine neue Funktionsversion und aktualisiert den `live`-Alias so, dass er auf die neue Version verweist.

DeploymentPreference

Die `DeploymentPreference` Eigenschaft bestimmt die Geschwindigkeit, mit der die CodeDeploy Anwendung den Datenverkehr von der ursprünglichen Version der Lambda-Funktion auf die neue Version verlagert. Der Wert `Linear10PercentEvery2Minutes` verschiebt alle zwei Minuten weitere zehn Prozent des Datenverkehrs zur neuen Version.

Eine Liste der vordefinierten Bereitstellungskonfigurationen finden Sie unter Bereitstellungskonfigurationen.

Ein ausführliches Tutorial zur Verwendung CodeDeploy mit Lambda-Funktionen finden Sie unter Bereitstellen einer aktualisierten Lambda-Funktion mit. CodeDeploy

Verwendung von Lambda mit Kubernetes

Sie können Lambda-Funktionen mit der Kubernetes-API mithilfe von AWS-Controllern für Kubernetes (ACK) oder Crossplane bereitstellen und verwalten.

AWS-Controller für Kubernetes (ACK)

Sie können ACK zum Bereitstellen und Verwalten von AWS-Ressourcen über die Kubernetes-API verwenden. Über ACK AWS bietet benutzerdefinierte Open-Source-Controller für AWS Services wie Lambda, Amazon Elastic Container Registry (Amazon ECR), Amazon Simple Storage Service (Amazon S3) und Amazon SageMaker. Jeder unterstützte AWS-Service verfügt über einen eigenen benutzerdefinierten Controller. Installieren Sie in Ihrem Kubernetes-Cluster einen Controller für jeden AWS-Service, den Sie verwenden möchten. Erstellen Sie anschließend eine benutzerdefinierte Ressourcendefinition (Custom Resource Definition, CRD), um die AWS-Ressourcen zu definieren.

Wir empfehlen die Verwendung von Helm 3.8 oder höher, um ACK-Controller zu installieren. Jeder ACK-Controller verfügt über ein eigenes Helm-Chart, das den Controller, CRDs und Kubernetes RBAC-Regeln installiert. Weitere Informationen finden Sie unter Installieren eines ACK-Controllers in der ACK-Dokumentation.

Nachdem Sie die benutzerdefinierte ACK-Ressource erstellt haben, können Sie sie wie jedes andere integrierte Kubernetes-Objekt verwenden. Beispielsweise können Sie Lambda-Funktionen mit Ihren bevorzugten Kubernetes-Toolchains, einschließlich kubectl, bereitstellen und verwalten.

Hier sind einige Beispielanwendungsfälle für die Bereitstellung von Lambda-Funktionen über ACK:

- Ihr Unternehmen verwendet rollenbasierte Zugriffssteuerung (RBAC) und IAM-Rollen für Service-Konten, um Berechtigungsgrenzen zu erstellen. Mit ACK können Sie dieses Sicherheitsmodell für Lambda wiederverwenden, ohne neue Benutzer und Richtlinien erstellen zu müssen.
- Ihre Organisation verfügt über einen DevOps Prozess zur Bereitstellung von Ressourcen in einem Amazon Elastic Kubernetes Service (Amazon EKS)-Cluster mithilfe von Kubernetes-Manifesten. Mit ACK können Sie ein Manifest verwenden, um Lambda-Funktionen bereitzustellen, ohne eine separate Infrastruktur in Form von Code-Vorlagen zu erstellen.

Weitere Informationen zur Verwendung von ACK finden Sie im Lambda-Tutorial in der ACK-Dokumentation.

Crossplane

Crossplane ist ein Open-Source-Projekt der Cloud Native Computing Foundation (CNCF), das Kubernetes zur Verwaltung von Cloud-Infrastrukturressourcen verwendet. Mit Crossplane können Entwickler Infrastruktur anfordern, ohne deren Komplexität verstehen zu müssen. Plattformteams behalten die Kontrolle über die Bereitstellung und Verwaltung der Infrastruktur.

Mit Crossplane können Sie Lambda-Funktionen mit Ihren bevorzugten Kubernetes-Toolchains wie kubectl und jeder CI/CD-Pipeline bereitstellen und verwalten, die Manifeste für Kubernetes bereitstellen kann. Hier sind einige Beispielanwendungsfälle für die Bereitstellung von Lambda-Funktionen über Crossplane:

- Ihr Unternehmen möchte Compliance durchsetzen, indem es sicherstellt, dass Lambda-Funktionen über die richtigen Tags verfügen. Plattformteams können Crossplane Compositions verwenden, um diese Richtlinie durch API-Abstraktionen zu definieren. Entwickler können diese Abstraktionen dann verwenden, um Lambda-Funktionen mit Tags bereitzustellen.
- Ihr Projekt verwendet GitOps mit Kubernetes. In diesem Modell gleicht Kubernetes kontinuierlich das Git-Repository (gewünschter Status) mit den im Cluster ausgeführten Ressourcen (aktueller Status) ab. Wenn es Unterschiede gibt, nimmt der GitOps Prozess automatisch Änderungen am Cluster vor. Sie können GitOps mit Kubernetes verwenden, um Lambda-Funktionen über Crossplane bereitzustellen und zu verwalten, indem Sie vertraute Kubernetes-Tools und -Konzepte wie CRDs und Controller verwenden. https://kubernetes.io/docs/concepts/architecture/controller/

Weitere Informationen zur Verwendung von Crossplane mit Lambda finden Sie hier:

- AWS-Blueprints für Crossplane: Dieses Repository enthält Beispiele für die Verwendung von Crossplane zum Bereitstellen von AWS-Ressourcen, einschließlich Lambda-Funktionen.

  > **Note**
  >
  > AWS-Blueprints für Crossplane befinden sich in der aktiven Entwicklung und sollten nicht in der Produktion verwendet werden.

- Bereitstellung von Lambda mit Amazon EKS und Crossplane: Dieses Video demonstriert ein fortgeschrittenes Beispiel für das Bereitstellen einer Serverless AWS-Architektur mit Crossplane, wobei das Design sowohl aus der Entwickler- als auch aus der Plattformperspektive untersucht wird.

Lambda-Beispielanwendungen

Das GitHub Repository für dieses Handbuch enthält Beispielanwendungen, die die Verwendung verschiedener Sprachen und AWS Dienste demonstrieren. Jede Beispielanwendung enthält Skripts für die einfache Bereitstellung und Bereinigung, eine AWS SAM Vorlage und unterstützende Ressourcen.

Node.js

Lambda-Beispielanwendungen in Node.js

- blank-nodejs — Eine Funktion von Node.js, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK zeigt. AWS
- nodejs-apig – Eine Funktion mit einem öffentlichen API-Endpunkt, die ein Ereignis aus API Gateway verarbeitet und eine HTTP-Antwort zurückgibt.
- efs-nodejs – Eine Funktion, die ein Amazon-EFS-Dateisystem in einer Amazon VPC nutzt. Dieses Beispiel umfasst eine VPC, ein Dateisystem, Bindungsbereitstellung-Ziele und einen Zugriffspunkt, der für die Verwendung mit Lambda konfiguriert ist.

Python

Lambda-Beispielanwendungen in Python

- blank-python — Eine Python-Funktion, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK zeigt. AWS

Ruby

Lambda-Beispielanwendungen in Ruby

- blank-ruby — Eine Ruby-Funktion, die die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem SDK zeigt. AWS
- Ruby-Codebeispiele für AWS Lambda — In Ruby geschriebene Codebeispiele, die zeigen, wie man mit AWS Lambda interagiert.

Java

Lambda-Beispielanwendungen in Java

- java17-examples – Eine Java-Funktion, die demonstriert, wie ein Java-Datensatz verwendet wird, um ein Eingabeereignis-Datenobjekt darzustellen.
- Java-Basis – Eine Sammlung minimaler Java-Funktionen mit Einheitentests und variabler Protokollierungskonfiguration.
- Java-Ereignisse – Eine Sammlung von Java-Funktionen, die Grundcode für den Umgang mit Ereignissen aus verschiedenen Services wie Amazon API Gateway, Amazon SQS und Amazon Kinesis enthalten. Diese Funktionen verwenden die neueste Version der aws-lambda-java-events-Bibliothek (3.0.0 und neuer). Für diese Beispiele ist das AWS SDK nicht als Abhängigkeit erforderlich.
- s3-java – Eine Java-Funktion die Benachrichtigungsereignisse aus Amazon S3 verarbeitet und die Java Class Library (JCL) verwendet, um Miniaturansichten aus hochgeladenen Image-Dateien zu erstellen.
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion – Eine Java-Funktion, die eine Amazon-DynamoDB-Tabelle durchsucht, die Mitarbeiterinformationen enthält. Anschließend verwendet es Amazon Simple Notification Service, um eine Textnachricht an Mitarbeiter zu senden, die ihr Betriebsjubiläum feiern. In diesem Beispiel wird API Gateway verwendet, um die Funktion aufzurufen.

Ausführen beliebter Java-Frameworks auf Lambda

- spring-cloud-function-samples — Ein Beispiel aus Spring, das zeigt, wie das Spring Cloud Function-Framework zur Erstellung von Lambda-Funktionen verwendet wird. AWS
- Serverlose Spring Boot-Anwendungsdemo — Ein Beispiel, das zeigt, wie eine typische Spring Boot-Anwendung in einer verwalteten Java-Laufzeit mit und ohne SnapStart oder als natives GraalVM-Image mit einer benutzerdefinierten Laufzeit eingerichtet wird.
- Serverlose Micronaut-Anwendungsdemo — Ein Beispiel, das zeigt, wie Micronaut in einer verwalteten Java-Laufzeit mit und ohne oder als natives SnapStart GraalVM-Image mit einer benutzerdefinierten Laufzeit verwendet wird. Erfahren Sie mehr in den Micronaut/Lambda-Leitfäden.
- Serverlose Quarkus-Anwendungsdemo — Ein Beispiel, das zeigt, wie Quarkus in einer verwalteten Java-Laufzeit mit und ohne oder als natives GraalVM-Image mit einer SnapStart

benutzerdefinierten Laufzeit verwendet werden kann. Weitere Informationen finden Sie im Quarkus/Lambda-Leitfaden und im Quarkus/-Leitfaden. SnapStart

Go

Lambda stellt die folgenden Beispielanwendungen für die Go-Laufzeit bereit:

Lambda-Beispielanwendungen in Go

- go-al2: Eine Hello World-Funktion, die die öffentliche IP-Adresse zurückgibt. Diese App verwendet die benutzerdefinierte Laufzeit `provided.al2`.
- blank-go — Eine Go-Funktion, die die Verwendung der Go-Bibliotheken, der Protokollierung, der Umgebungsvariablen und des SDK von Lambda zeigt. AWS Diese App verwendet die Laufzeit `go1.x`.

C#

Lambda-Beispielanwendungen in C#

- blank-csharp AWS X-Ray Eine C #-Funktion, welche die Verwendung der Lambda-NET-Bibliotheken, Protokollierung, Umgebungsvariablen, -Nachverfolgung, Einheitentests und des AWS SDK aufzeigt.
- blank-csharp-with-layer – Eine C#-Funktion, die die .NET-CLI verwendet, um eine Ebene zu erstellen, die die Abhängigkeiten der Funktion bündelt.
- ec2-spot – Eine Funktion, die Spot-Instance-Anforderungen in Amazon EC2 verwaltet.

PowerShell

Lambda bietet die folgenden Beispielanwendungen für PowerShell:

- blank-powershell — Eine PowerShell Funktion, die die Verwendung von Logging, Umgebungsvariablen und dem SDK veranschaulicht. AWS

Um eine Beispielanwendung bereitzustellen, befolgen Sie die Anweisungen in der README-Datei. Um mehr über die Architektur und Anwendungsfälle einer Anwendung zu erfahren, lesen Sie die Themen in diesem Kapitel.

Themen

- Leere Funktionsmusteranwendung für AWS Lambda

Leere Funktionsmusteranwendung für AWS Lambda

Die leere Funktionsbeispielanwendung ist eine Starteranwendung, die geläufige Operationen in Lambda mit einer Funktion veranschaulicht, die die Lambda-API aufruft. Es zeigt die Verwendung von Logging, Umgebungsvariablen, AWS X-Ray Tracing, Layern, Unit-Tests und dem AWS SDK. Erkunden Sie diese Anwendung, um mehr über das Erstellen von Lambda-Funktionen in Ihrer Programmiersprache zu erfahren, oder verwenden Sie sie als Ausgangspunkt für Ihre eigenen Projekte.

Varianten dieser Beispielanwendung stehen für folgende Sprachen zur Verfügung:

Varianten

- Node.js – blank-nodejs.
- Python – blank-python.
- Ruby – blank-ruby.
- Java – blank-java.
- Go – blank-go.
- C# – blank-csharp.
- PowerShell — leere Powershell.

In den Beispielen in diesem Thema wird auf Code aus der Node.js-Version eingegangen, die Details gelten jedoch im Allgemeinen für alle Varianten.

Mit dem und können Sie das Beispiel in wenigen Minuten bereitstellen. AWS CLI AWS CloudFormation Befolgen Sie die Anweisungen in der README-Datei zum Herunterladen, Konfigurieren und Bereitstellen in Ihrem Konto.

Abschnitte

Architektur- und Handler-Code

Die Beispielanwendung besteht aus Funktionscode, einer AWS CloudFormation Vorlage und unterstützenden Ressourcen. Wenn Sie das Beispiel bereitstellen, verwenden Sie die folgenden AWS Dienste:

- AWS Lambda — Führt Funktionscode aus, sendet CloudWatch Protokolle an Logs und sendet Trace-Daten an X-Ray. Die Funktion ruft auch die Lambda-API auf, um Details über die Kontingente und die Nutzung des Kontos in der aktuellen Region zu erhalten.
- AWS X-Ray – sammelt Nachverfolgungsdaten, indiziert Ablaufverfolgungen für die Suche und generiert eine Service-Übersicht.
- Amazon CloudWatch — Speichert Protokolle und Metriken.
- AWS Identity and Access Management (IAM) — Erteilt die Erlaubnis.
- Amazon Simple Storage Service (Amazon S3) – Speichert das Bereitstellungspaket der Funktion während der Bereitstellung.
- AWS CloudFormation – Erstellt Anwendungsressourcen und stellt Funktionscode bereit.

Für jeden Service fallen Standardgebühren an. Weitere Informationen finden Sie unter AWS - Preise.

Der Funktionscode zeigt einen grundlegenden Workflow für die Verarbeitung eines Ereignisses. Der Handler nimmt ein Amazon-Simple-Queue-Service (Amazon SQS)-Ereignis als Eingabe und iteriert die darin enthaltenen Datensätze, wobei der Inhalt jeder Nachricht protokolliert wird. Er protokolliert den Inhalt des Ereignisses, das Kontextobjekt und Umgebungsvariablen. Dann ruft es mit dem AWS SDK auf und leitet die Antwort an die Lambda-Laufzeit zurück.

Example blank-nodejs/function/index.js – Handler-Code

```
// Handler
exports.handler = async function(event, context) {
    event.Records.forEach(record => {
        console.log(record.body);
    });

    console.log('## ENVIRONMENT VARIABLES: ' + serialize(process.env));
    console.log('## CONTEXT: ' + serialize(context));
    console.log('## EVENT: ' + serialize(event));

    return getAccountSettings();
```

```
};

// Use SDK client
var getAccountSettings = function() {
    return lambda.send(new GetAccountSettingsCommand());
};

var serialize = function(object) {
    return JSON.stringify(object, null, 2);
};
```

Die Beispielanwendung enthält keine Amazon-SQS-Warteschlange zum Senden von Ereignissen, sondern verwendet ein Ereignis von Amazon SQS (event.json) um zu veranschaulichen, wie Ereignisse verarbeitet werden. Informationen zum Hinzufügen einer Amazon-SQS-Warteschlange zu Ihrer Anwendung finden Sie unter Verwenden von Lambda mit Amazon SQS.

Automatisierung der Bereitstellung mit AWS CloudFormation und dem AWS CLI

Die Ressourcen der Beispielanwendung werden in einer AWS CloudFormation Vorlage definiert und zusammen mit dem bereitgestellt AWS CLI. Das Projekt umfasst einfache Shell-Skripte, die das Einrichten, Bereitstellen, Aufrufen und Abreißen der Anwendung automatisieren.

Die Anwendungsvorlage verwendet einen Ressourcentyp AWS Serverless Application Model (AWS SAM), um das Modell zu definieren. AWS SAM vereinfacht die Erstellung von Vorlagen für serverlose Anwendungen, indem die Definition von Ausführungsrollen, APIs und anderen Ressourcen automatisiert wird.

Die Vorlage definiert die Ressourcen im Anwendungs-Stack. Dazu gehören die Funktion, ihre Ausführungsrolle und eine Lambda-Ebene, die die Bibliotheksabhängigkeiten der Funktion bereitstellt. Der Stack enthält weder den Bucket, den er während der Bereitstellung AWS CLI verwendet, noch die CloudWatch Protokollgruppe Logs.

Example blank-nodejs/template.yml – Serverless-Ressourcen

```
AWSTemplateFormatVersion: '2010-09-09'
Transform: 'AWS::Serverless-2016-10-31'
Description: An AWS Lambda application that calls the Lambda API.
Resources:
  function:
```

```
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs20.x
      CodeUri: function/.
      Description: Call the AWS Lambda API
      Timeout: 10
      # Function's execution role
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
      Tracing: Active
      Layers:
        - !Ref libs
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-nodejs-lib
      Description: Dependencies for the blank sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - nodejs20.x
```

Wenn Sie die Anwendung bereitstellen, AWS CloudFormation wendet die AWS SAM Transformation auf die Vorlage an, um eine AWS CloudFormation Vorlage mit Standardtypen wie `AWS::Lambda::Function` und zu generieren`AWS::IAM::Role`.

Example Verarbeitete Vorlage

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "An AWS Lambda application that calls the Lambda API.",
  "Resources": {
    "function": {
      "Type": "AWS::Lambda::Function",
      "Properties": {
        "Layers": [
          {
            "Ref": "libs32xmpl61b2"
          }
        ],
        "TracingConfig": {
```

```
          "Mode": "Active"
        },
        "Code": {
          "S3Bucket": "lambda-artifacts-6b000xmpl1e9bf2a",
          "S3Key": "3d3axmpl473d249d039d2d7a37512db3"
        },
        "Description": "Call the AWS Lambda API",
        "Tags": [
          {
            "Value": "SAM",
            "Key": "lambda:createdBy"
          }
        ],
```

In diesem Beispiel gibt die Eigenschaft `Code` ein Objekt in einem Amazon-S3-Bucket an. Dies entspricht dem lokalen Pfad in der Eigenschaft `CodeUri` in der Projektvorlage:

```
      CodeUri: function/.
```

Um die Projektdateien zu Amazon S3 hochzuladen, verwendet das Bereitstellungsskript Befehle in der AWS CLI. Der Befehl `cloudformation package` verarbeitet die Vorlage vorab, lädt Artefakte hoch und ersetzt lokale Pfade durch Amazon-S3-Objektpositionen. Der `cloudformation deploy` Befehl stellt die verarbeitete Vorlage mit einem AWS CloudFormation Änderungssatz bereit.

Example blank-nodejs/3-deploy.sh – Verpacken und Bereitstellen

```
#!/bin/bash
set -eo pipefail
ARTIFACT_BUCKET=$(cat bucket-name.txt)
aws cloudformation package --template-file template.yml --s3-bucket $ARTIFACT_BUCKET --
output-template-file out.yml
aws cloudformation deploy --template-file out.yml --stack-name blank-nodejs --
capabilities CAPABILITY_NAMED_IAM
```

Wenn Sie dieses Skript zum ersten Mal ausführen, erstellt es einen AWS CloudFormation Stapel mit dem Namen`blank-nodejs`. Wenn Sie Änderungen am Funktionscode oder der Vorlage vornehmen, können Sie sie bzw. ihn erneut ausführen, um den Stack zu aktualisieren.

Das Bereinigungsskript (blank-nodejs/5-cleanup.sh) löscht den Stack und löscht optional den Bereitstellungs-Bucket und die Funktionsprotokolle.

Instrumentierung mit dem AWS X-Ray

Die Beispielfunktion wird mit für die Ablaufverfolgung konfiguriert AWS X-Ray. Wenn der Ablaufverfolgungsmodus aktiviert ist, zeichnet Lambda-Zeit-Informationen für eine Teilmenge von Aufrufen auf und sendet sie an X-Ray. X-Ray verarbeitet die Daten, um ein Service-Mapping zu generieren, die einen Client-Knoten und zwei Service-Knoten zeigt.

Der erste Serviceknoten (`AWS::Lambda`) stellt den Lambda-Service dar, der die Aufrufanforderung validiert und sie an die Funktion sendet. Der zweite Knoten, `AWS::Lambda::Function`, stellt die Funktion selbst dar.

Um zusätzliche Details aufzuzeichnen, verwendet die Beispielfunktion das X-Ray-SDK. Mit minimalen Änderungen am Funktionscode zeichnet das X-Ray-SDK Details zu Aufrufen von AWS Diensten auf, die mit dem AWS SDK getätigt wurden.

Example blank-nodejs/function/index.js – Instrumentierung

```
const AWSXRay = require('aws-xray-sdk-core');
const { LambdaClient, GetAccountSettingsCommand } = require('@aws-sdk/client-lambda');

// Create client outside of handler to reuse
const lambda = AWSXRay.captureAWSv3Client(new LambdaClient());
```

Durch die Instrumentierung des AWS SDK-Clients wird der Service Map ein zusätzlicher Knoten und mehr Details in den Traces hinzugefügt. In diesem Beispiel zeigt die Service-Übersicht die Beispielfunktion, mit der die Lambda-API aufgerufen wird, um Details zur Speicherung und Parallelität in der aktuellen Region zu erhalten.

Die Ablaufverfolgung zeigt Timing-Details für den Aufruf mit Teilsegmenten für Funktionsinitialisierung, Aufruf und Overhead. Das Aufruf-Untersegment hat ein Untersegment für den AWS SDK-Aufruf zur API-Operation. `GetAccountSettings`

Sie können das X-Ray SDK und andere Bibliotheken in das Bereitstellungspaket Ihrer Funktion aufnehmen oder separat in einer Lambda-Ebene bereitstellen. Für Node.js, Ruby und Python beinhaltet die Lambda-Laufzeit das AWS SDK in der Ausführungsumgebung.

Abhängigkeitsverwaltung mit Ebenen

Sie können Bibliotheken lokal installieren und in das Bereitstellungspaket, das Sie zu Lambda hochladen, aufnehmen, aber dies hat seine Nachteile. Größere Dateigrößen verlangsamen

die Bereitstellung und können Sie daran hindern, Änderungen an Ihrem Funktionscode in der Lambda-Konsole zu testen. Um das Bereitstellungspaket klein zu halten und zu verhindern, dass Abhängigkeiten hochgeladen werden, die sich nicht geändert haben, erstellt die Beispiel-App eine Lambda-Ebene und ordnet sie der Funktion zu.

Example blank-nodejs/template.yml – Abhängigkeitsebene

```
Resources:
  function:
    Type: AWS::Serverless::Function
    Properties:
      Handler: index.handler
      Runtime: nodejs20.x
      CodeUri: function/.
      Description: Call the AWS Lambda API
      Timeout: 10
      # Function's execution role
      Policies:
        - AWSLambdaBasicExecutionRole
        - AWSLambda_ReadOnlyAccess
        - AWSXrayWriteOnlyAccess
      Tracing: Active
      Layers:
        - !Ref libs
  libs:
    Type: AWS::Serverless::LayerVersion
    Properties:
      LayerName: blank-nodejs-lib
      Description: Dependencies for the blank sample app.
      ContentUri: lib/.
      CompatibleRuntimes:
        - nodejs20.x
```

Das `2-build-layer.sh`-Skript installiert die Abhängigkeiten der Funktion mit npm und platziert sie in einem Ordner mit der für die Lambda-Laufzeit erforderlichen Struktur.

Example 2-build-layer.sh – Vorbereiten der Ebene

```
#!/bin/bash
set -eo pipefail
mkdir -p lib/nodejs
rm -rf node_modules lib/nodejs/node_modules
```

```
npm install --production
mv node_modules lib/nodejs/
```

Wenn Sie die Beispielanwendung zum ersten Mal bereitstellen, AWS CLI verpackt sie die Ebene getrennt vom Funktionscode und stellt beide bereit. Für nachfolgende Bereitstellungen wird das Ebenenarchiv nur hochgeladen, wenn sich der Inhalt des Ordners `lib` geändert hat.

Lambda mit einem AWS SDK verwenden

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eine API, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDK-Dokumentation	Codebeispiele
AWS SDK for C++	AWS SDK for C++ Code-Beispiele
AWS CLI	AWS CLI Code-Beispiele
AWS SDK for Go	AWS SDK for Go Code-Beispiele
AWS SDK for Java	AWS SDK for Java Code-Beispiele
AWS SDK for JavaScript	AWS SDK for JavaScript Code-Beispiele
AWS SDK for Kotlin	AWS SDK for Kotlin Code-Beispiele
AWS SDK for .NET	AWS SDK for .NET Code-Beispiele
AWS SDK for PHP	AWS SDK for PHP Code-Beispiele
AWS Tools for PowerShell	Tools für PowerShell Codebeispiele
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) Code-Beispiele
AWS SDK for Ruby	AWS SDK for Ruby Code-Beispiele
AWS SDK for Rust	AWS SDK for Rust Code-Beispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Code-Beispiele
AWS SDK for Swift	AWS SDK for Swift Code-Beispiele

Für Beispiele, die sich speziell auf Lambda beziehen, siehe Codebeispiele für Lambda mit SDKs AWS.

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Codebeispiele für Lambda mit SDKs AWS

Die folgenden Codebeispiele zeigen, wie Lambda mit einem AWS Software Development Kit (SDK) verwendet wird.

Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Während Aktionen Ihnen zeigen, wie Sie einzelne Servicefunktionen aufrufen, können Sie Aktionen im Kontext der zugehörigen Szenarien und serviceübergreifenden Beispiele sehen.

Szenarien sind Codebeispiele, die Ihnen zeigen, wie Sie eine bestimmte Aufgabe ausführen können, indem Sie mehrere Funktionen innerhalb desselben Services aufrufen.

Serviceübergreifende Beispiele sind Beispielanwendungen, die über mehrere AWS-Services hinweg arbeiten.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte

Hallo Lambda

Die folgenden Codebeispiele veranschaulichen, wie Sie mit der Verwendung von Lambda beginnen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
namespace LambdaActions;

using Amazon.Lambda;

public class HelloLambda
```

```
{
    static async Task Main(string[] args)
    {
        var lambdaClient = new AmazonLambdaClient();

        Console.WriteLine("Hello AWS Lambda");
        Console.WriteLine("Let's get started with AWS Lambda by listing your
 existing Lambda functions:");

        var response = await lambdaClient.ListFunctionsAsync();
        response.Functions.ForEach(function =>
        {

 Console.WriteLine($"{function.FunctionName}\t{function.Description}");
        });
    }
}
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Code für die C MakeLists .txt-CMake-Datei.

```
# Set the minimum required version of CMake for this project.
cmake_minimum_required(VERSION 3.13)

# Set the AWS service components used by this project.
set(SERVICE_COMPONENTS lambda)

# Set this project's name.
project("hello_lambda")
```

```
# Set the C++ standard to use to build this target.
# At least C++ 11 is required for the AWS SDK for C++.
set(CMAKE_CXX_STANDARD 11)

# Use the MSVC variable to determine if this is a Windows build.
set(WINDOWS_BUILD ${MSVC})

if (WINDOWS_BUILD) # Set the location where CMake can find the installed
 libraries for the AWS SDK.
    string(REPLACE ";" "/aws-cpp-sdk-all;" SYSTEM_MODULE_PATH
 "${CMAKE_SYSTEM_PREFIX_PATH}/aws-cpp-sdk-all")
    list(APPEND CMAKE_PREFIX_PATH ${SYSTEM_MODULE_PATH})
endif ()

# Find the AWS SDK for C++ package.
find_package(AWSSDK REQUIRED COMPONENTS ${SERVICE_COMPONENTS})

if (WINDOWS_BUILD AND AWSSDK_INSTALL_AS_SHARED_LIBS)
     # Copy relevant AWS SDK for C++ libraries into the current binary directory
 for running and debugging.

     # set(BIN_SUB_DIR "/Debug") # if you are building from the command line you
 may need to uncomment this
                                     # and set the proper subdirectory to the
 executables' location.

     AWSSDK_CPY_DYN_LIBS(SERVICE_COMPONENTS ""
 ${CMAKE_CURRENT_BINARY_DIR}${BIN_SUB_DIR})
endif ()

add_executable(${PROJECT_NAME}
        hello_lambda.cpp)

target_link_libraries(${PROJECT_NAME}
        ${AWSSDK_LINK_LIBRARIES})
```

Code für die Quelldatei „hello_lambda.cpp“.

```
#include <aws/core/Aws.h>
#include <aws/lambda/LambdaClient.h>
#include <aws/lambda/model/ListFunctionsRequest.h>
```

```
#include <iostream>

/*
 *  A "Hello Lambda" starter application which initializes an AWS Lambda (Lambda)
 client and lists the Lambda functions.
 *
 *  main function
 *
 *  Usage: 'hello_lambda'
 *
 */

int main(int argc, char **argv) {
    Aws::SDKOptions options;
    // Optionally change the log level for debugging.
//   options.loggingOptions.logLevel = Utils::Logging::LogLevel::Debug;
    Aws::InitAPI(options); // Should only be called once.
    int result = 0;
    {
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region (overrides config file).
        // clientConfig.region = "us-east-1";

        Aws::Lambda::LambdaClient lambdaClient(clientConfig);
        std::vector<Aws::String> functions;
        Aws::String marker; // Used for pagination.

        do {
            Aws::Lambda::Model::ListFunctionsRequest request;
            if (!marker.empty()) {
                request.SetMarker(marker);
            }

            Aws::Lambda::Model::ListFunctionsOutcome outcome =
 lambdaClient.ListFunctions(
                    request);

            if (outcome.IsSuccess()) {
                const Aws::Lambda::Model::ListFunctionsResult
 &listFunctionsResult = outcome.GetResult();
                std::cout << listFunctionsResult.GetFunctions().size()
                          << " lambda functions were retrieved." << std::endl;
```

```
                for (const Aws::Lambda::Model::FunctionConfiguration
 &functionConfiguration: listFunctionsResult.GetFunctions()) {
                    functions.push_back(functionConfiguration.GetFunctionName());
                    std::cout << functions.size() << "  "
                              << functionConfiguration.GetDescription() <<
 std::endl;
                    std::cout << "   "
                              <<
 Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                      functionConfiguration.GetRuntime()) << ": "
                              << functionConfiguration.GetHandler()
                              << std::endl;
                }
                marker = listFunctionsResult.GetNextMarker();
            } else {
                std::cerr << "Error with Lambda::ListFunctions. "
                          << outcome.GetError().GetMessage()
                          << std::endl;
                result = 1;
                break;
            }
        } while (!marker.empty());
    }


    Aws::ShutdownAPI(options); // Should only be called once.
    return result;
}
```

- Einzelheiten zur API finden Sie unter ListFunctions AWS SDK for C++API-Referenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/lambda"
)

// main uses the AWS SDK for Go (v2) to create an AWS Lambda client and list up
 to 10
// functions in your account.
// This example uses the default settings specified in your shared credentials
// and config files.
func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  fmt.Println("Couldn't load default configuration. Have you set up your AWS
 account?")
  fmt.Println(err)
  return
 }
 lambdaClient := lambda.NewFromConfig(sdkConfig)

 maxItems := 10
 fmt.Printf("Let's list up to %v functions for your account.\n", maxItems)
 result, err := lambdaClient.ListFunctions(context.TODO(),
 &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 if err != nil {
  fmt.Printf("Couldn't list functions for your account. Here's why: %v\n", err)
  return
 }
 if len(result.Functions) == 0 {
  fmt.Println("You don't have any functions!")
 } else {
  for _, function := range result.Functions {
   fmt.Printf("\t%v\n", *function.FunctionName)
  }
```

```
 }
}
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
package com.example.lambda;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.LambdaException;
import software.amazon.awssdk.services.lambda.model.ListFunctionsResponse;
import software.amazon.awssdk.services.lambda.model.FunctionConfiguration;
import java.util.List;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class ListLambdaFunctions {
    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
                .region(region)
                .build();
```

```
        listFunctions(awsLambda);
        awsLambda.close();
    }

    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
 config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import { LambdaClient, paginateListFunctions } from "@aws-sdk/client-lambda";

const client = new LambdaClient({});

export const helloLambda = async () => {
  const paginator = paginateListFunctions({ client }, {});
  const functions = [];

  for await (const page of paginator) {
```

```
    const funcNames = page.Functions.map((f) => f.FunctionName);
    functions.push(...funcNames);
  }

  console.log("Functions:");
  console.log(functions.join("\n"));
  return functions;
};
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for JavaScript API-Referenz.

Codebeispiele

- Aktionen für Lambda mithilfe von SDKs AWS
  - Verwendung CreateAlias mit einem AWS SDK oder CLI
  - Verwendung CreateFunction mit einem AWS SDK oder CLI
  - Verwendung DeleteAlias mit einem AWS SDK oder CLI
  - Verwendung DeleteFunction mit einem AWS SDK oder CLI
  - Verwendung DeleteFunctionConcurrency mit einem AWS SDK oder CLI
  - Verwendung DeleteProvisionedConcurrencyConfig mit einem AWS SDK oder CLI
  - Verwendung GetAccountSettings mit einem AWS SDK oder CLI
  - Verwendung GetAlias mit einem AWS SDK oder CLI
  - Verwendung GetFunction mit einem AWS SDK oder CLI
  - Verwendung GetFunctionConcurrency mit einem AWS SDK oder CLI
  - Verwendung GetFunctionConfiguration mit einem AWS SDK oder CLI
  - Verwendung GetPolicy mit einem AWS SDK oder CLI
  - Verwendung GetProvisionedConcurrencyConfig mit einem AWS SDK oder CLI
  - Verwendung Invoke mit einem AWS SDK oder CLI
  - Verwendung ListFunctions mit einem AWS SDK oder CLI
  - Verwendung ListProvisionedConcurrencyConfigs mit einem AWS SDK oder CLI
  - Verwendung ListTags mit einem AWS SDK oder CLI
  - Verwendung ListVersionsByFunction mit einem AWS SDK oder CLI
  - Verwendung PublishVersion mit einem AWS SDK oder CLI
  - Verwendung PutFunctionConcurrency mit einem AWS SDK oder CLI

- Eine Anwendung für Foto-Asset-Management erstellen, mit der Benutzer Fotos mithilfe von Labels verwalten können
- Erstellen einer Websocket-Chat-Anwendung mit API Gateway
- Erstellen einer Anwendung, die Kundenfeedback analysiert und Audio generiert
- Aufrufen einer Lambda-Funktion von einem Browser aus
- Transformieren Sie Daten für Ihre Anwendung mit S3 Object Lambda
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion
- Verwenden von Step Functions, um Lambda-Funktionen aufzurufen
- Verwendung geplanter Ereignisse zum Aufrufen einer Lambda-Funktion

Aktionen für Lambda mithilfe von SDKs AWS

Die folgenden Codebeispiele zeigen, wie einzelne Lambda-Aktionen mit AWS SDKs ausgeführt werden. Diese Auszüge rufen die Lambda-API auf und sind Codeauszüge aus größeren Programmen, die im Kontext ausgeführt werden müssen. Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen des Codes finden.

Die folgenden Beispiele enthalten nur die am häufigsten verwendeten Aktionen. Eine vollständige Liste finden Sie in der AWS Lambda -API-Referenz.

Beispiele

- Verwendung CreateAlias mit einem AWS SDK oder CLI
- Verwendung CreateFunction mit einem AWS SDK oder CLI
- Verwendung DeleteAlias mit einem AWS SDK oder CLI
- Verwendung DeleteFunction mit einem AWS SDK oder CLI
- Verwendung DeleteFunctionConcurrency mit einem AWS SDK oder CLI
- Verwendung DeleteProvisionedConcurrencyConfig mit einem AWS SDK oder CLI
- Verwendung GetAccountSettings mit einem AWS SDK oder CLI
- Verwendung GetAlias mit einem AWS SDK oder CLI
- Verwendung GetFunction mit einem AWS SDK oder CLI
- Verwendung GetFunctionConcurrency mit einem AWS SDK oder CLI
- Verwendung GetFunctionConfiguration mit einem AWS SDK oder CLI
- Verwendung GetPolicy mit einem AWS SDK oder CLI

- Verwendung GetProvisionedConcurrencyConfig mit einem AWS SDK oder CLI
- Verwendung Invoke mit einem AWS SDK oder CLI
- Verwendung ListFunctions mit einem AWS SDK oder CLI
- Verwendung ListProvisionedConcurrencyConfigs mit einem AWS SDK oder CLI
- Verwendung ListTags mit einem AWS SDK oder CLI
- Verwendung ListVersionsByFunction mit einem AWS SDK oder CLI
- Verwendung PublishVersion mit einem AWS SDK oder CLI
- Verwendung PutFunctionConcurrency mit einem AWS SDK oder CLI
- Verwendung PutProvisionedConcurrencyConfig mit einem AWS SDK oder CLI
- Verwendung RemovePermission mit einem AWS SDK oder CLI
- Verwendung TagResource mit einem AWS SDK oder CLI
- Verwendung UntagResource mit einem AWS SDK oder CLI
- Verwendung UpdateAlias mit einem AWS SDK oder CLI
- Verwendung UpdateFunctionCode mit einem AWS SDK oder CLI
- Verwendung UpdateFunctionConfiguration mit einem AWS SDK oder CLI

Verwendung **`CreateAlias`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateAlias`.

CLI

AWS CLI

Um einen Alias für eine Lambda-Funktion zu erstellen

Im folgenden `create-alias` Beispiel wird ein Alias mit dem Namen erstellt`LIVE`, der auf Version 1 der `my-function` Lambda-Funktion verweist.

```
aws lambda create-alias \
    --function-name my-function \
    --description "alias for live version of function" \
    --function-version 1 \
    --name LIVE
```

Ausgabe:

```
{
    "FunctionVersion": "1",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
    "Description": "alias for live version of function"
}
```

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz CreateAlias.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird ein neuer Lambda-Alias für die angegebene Version und Routing-Konfiguration erstellt, um den Prozentsatz der empfangenen Aufrufanforderungen anzugeben.

```
New-LMAlias -FunctionName "MylambdaFunction123" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6} -Description "Alias
 for version 4" -FunctionVersion 4 -Name "PowershellAlias"
```

- Einzelheiten zur API finden Sie unter CreateAlias AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`CreateFunction`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`CreateFunction`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <summary>
/// Creates a new Lambda function.
/// </summary>
/// <param name="functionName">The name of the function.</param>
/// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
/// bucket where the zip file containing the code is located.</param>
/// <param name="s3Key">The Amazon S3 key of the zip file.</param>
/// <param name="role">The Amazon Resource Name (ARN) of a role with the
/// appropriate Lambda permissions.</param>
/// <param name="handler">The name of the handler function.</param>
/// <returns>The Amazon Resource Name (ARN) of the newly created
/// Lambda function.</returns>
public async Task<string> CreateLambdaFunctionAsync(
    string functionName,
    string s3Bucket,
    string s3Key,
    string role,
    string handler)
{
    // Defines the location for the function code.
    // S3Bucket - The S3 bucket where the file containing
    //            the source code is stored.
    // S3Key    - The name of the file containing the code.
    var functionCode = new FunctionCode
    {
        S3Bucket = s3Bucket,
        S3Key = s3Key,
    };

    var createFunctionRequest = new CreateFunctionRequest
```

```
        {
            FunctionName = functionName,
            Description = "Created by the Lambda .NET API",
            Code = functionCode,
            Handler = handler,
            Runtime = Runtime.Dotnet6,
            Role = role,
        };

        var reponse = await
 _lambdaService.CreateFunctionAsync(createFunctionRequest);
        return reponse.FunctionArn;
    }
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
 (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::CreateFunctionRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetDescription(LAMBDA_DESCRIPTION); // Optional.
#if USE_CPP_LAMBDA_FUNCTION
        request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
        request.SetTimeout(15);
        request.SetMemorySize(128);
```

```
        // Assume the AWS Lambda function was built in Docker with same
 architecture
        // as this code.
#if  defined(__x86_64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
#elif defined(__aarch64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
#else
#error "Unimplemented architecture"
#endif // defined(architecture)
#else
        request.SetRuntime(Aws::Lambda::Model::Runtime::python3_8);
#endif
        request.SetRole(roleArn);
        request.SetHandler(LAMBDA_HANDLER_NAME);
        request.SetPublish(true);
        Aws::Lambda::Model::FunctionCode code;
        std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();

        code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
 buffer.str().c_str(),
                                               buffer.str().length()));
        request.SetCode(code);

        Aws::Lambda::Model::CreateFunctionOutcome outcome =
 client.CreateFunction(
```

```
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda function was successfully created. " <<
 seconds
                      << " seconds elapsed." << std::endl;
            break;
        }

        else {
            std::cerr << "Error with CreateFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            deleteIamRole(clientConfig);
            return false;
        }
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Eine Lambda-Funktion erstellen

Im folgenden Beispiel für `create-function` wird eine Lambda-Funktion mit dem Namen `my-function` erstellt.

```
aws lambda create-function \
    --function-name my-function \
    --runtime nodejs18.x \
    --zip-file fileb://my-function.zip \
    --handler my-function.handler \
    --role arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
tges6bf4
```

Inhalt von `my-function.zip`:

```
This file is a deployment package that contains your function code and any
 dependencies.
```

Ausgabe:

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "PFn4S+er27qk+UuZSTKEQfNKG/XNn7QJs90mJgq6oH8=",
    "FunctionName": "my-function",
    "CodeSize": 308,
    "RevisionId": "873282ed-4cd3-4dc8-a069-d0c647e470c6",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2023-10-14T22:26:11.234+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs18.x",
    "Description": ""
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie CreateFunctionin der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
```

```
}



// CreateFunction creates a new Lambda function from code contained in the
 zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
 until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(functionName string, handlerName
 string,
 iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.CreateFunction(context.TODO(),
 &lambda.CreateFunctionInput{
  Code:         &types.FunctionCode{ZipFile: zipPackage.Bytes()},
  FunctionName: aws.String(functionName),
  Role:         iamRoleArn,
  Handler:      aws.String(handlerName),
  Publish:      true,
  Runtime:      types.RuntimePython38,
 })
 if err != nil {
  var resConflict *types.ResourceConflictException
  if errors.As(err, &resConflict) {
   log.Printf("Function %v already exists.\n", functionName)
   state = types.StateActive
  } else {
   log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
  }
 } else {
  waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(context.TODO(),
 &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
```

```
  }
 }
 return state
}
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.services.lambda.model.CreateFunctionRequest;
import software.amazon.awssdk.services.lambda.model.FunctionCode;
import software.amazon.awssdk.services.lambda.model.CreateFunctionResponse;
import software.amazon.awssdk.services.lambda.model.GetFunctionRequest;
import software.amazon.awssdk.services.lambda.model.GetFunctionResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;
import software.amazon.awssdk.services.lambda.model.Runtime;
import software.amazon.awssdk.services.lambda.waiters.LambdaWaiter;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;

/**
 * This code example requires a ZIP or JAR that represents the code of the
 * Lambda function.
 * If you do not have a ZIP or JAR, please refer to the following document:
 *
 * https://github.com/aws-doc-sdk-examples/tree/master/javav2/usecases/
creating_workflows_stepfunctions
```

```
 *
 * Also, set up your development environment, including your credentials.
 *
 * For information, see this documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateFunction {
    public static void main(String[] args) {

        final String usage = """

                Usage:
                    <functionName> <filePath> <role> <handler>\s

                Where:
                    functionName - The name of the Lambda function.\s
                    filePath - The path to the ZIP or JAR where the code is
 located.\s
                    role - The role ARN that has Lambda permissions.\s
                    handler - The fully qualified method name (for example,
 example.Handler::handleRequest). \s
                """;

        if (args.length != 4) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        String filePath = args[1];
        String role = args[2];
        String handler = args[3];
        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
                .region(region)
                .build();

        createLambdaFunction(awsLambda, functionName, filePath, role, handler);
        awsLambda.close();
    }
```

```
    public static void createLambdaFunction(LambdaClient awsLambda,
            String functionName,
            String filePath,
            String role,
            String handler) {

        try {
            LambdaWaiter waiter = awsLambda.waiter();
            InputStream is = new FileInputStream(filePath);
            SdkBytes fileToUpload = SdkBytes.fromInputStream(is);

            FunctionCode code = FunctionCode.builder()
                    .zipFile(fileToUpload)
                    .build();

            CreateFunctionRequest functionRequest =
 CreateFunctionRequest.builder()
                    .functionName(functionName)
                    .description("Created by the Lambda Java API")
                    .code(code)
                    .handler(handler)
                    .runtime(Runtime.JAVA8)
                    .role(role)
                    .build();

            // Create a Lambda function using a waiter.
            CreateFunctionResponse functionResponse =
 awsLambda.createFunction(functionRequest);
            GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
                    .functionName(functionName)
                    .build();
            WaiterResponse<GetFunctionResponse> waiterResponse =
 waiter.waitUntilFunctionExists(getFunctionRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println("The function ARN is " +
 functionResponse.functionArn());

        } catch (LambdaException | FileNotFoundException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const createFunction = async (funcName, roleArn) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);

  const command = new CreateFunctionCommand({
    Code: { ZipFile: code },
    FunctionName: funcName,
    Role: roleArn,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun createNewFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String
): String? {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }

    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java8
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitUntilFunctionActive {
            functionName = myFunctionName
        }
        return functionResponse.functionArn
    }
}
```

- Einzelheiten zur API finden Sie CreateFunctionin der API-Referenz zum AWS SDK für Kotlin.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function createFunction($functionName, $role, $bucketName, $handler)
    {
        //This assumes the Lambda function is in an S3 bucket.
        return $this->customWaiter(function () use ($functionName, $role,
$bucketName, $handler) {
            return $this->lambdaClient->createFunction([
                'Code' => [
                    'S3Bucket' => $bucketName,
                    'S3Key' => $functionName,
                ],
                'FunctionName' => $functionName,
                'Role' => $role['Arn'],
                'Runtime' => 'python3.9',
                'Handler' => "$handler.lambda_handler",
            ]);
        });
    }
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for PHP API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird eine neue C#-Funktion (dotnetcore1.0 Runtime) mit dem Namen AWS Lambda erstellt, die die kompilierten Binärdateien für die Funktion aus einer ZIP-

Datei MyFunction im lokalen Dateisystem bereitstellt (relative oder absolute Pfade können verwendet werden). C#-Lambda-Funktionen spezifizieren den Handler für die Funktion mit der Bezeichnung AssemblyName: :Namespace. ClassName::. MethodName Sie sollten den Assemblynamen (ohne DLL-Suffix), den Namespace, den Klassennamen und den Methodennamen der Handler-Spezifikation entsprechend ersetzen. Für die neue Funktion werden die Umgebungsvariablen 'envvar1' und 'envvar2' aus den bereitgestellten Werten eingerichtet.

```
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -ZipFilename .\MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

Ausgabe:

```
CodeSha256       : /NgBMd...gq71I=
CodeSize         : 214784
DeadLetterConfig :
Description      : My C# Lambda Function
Environment      : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn      : arn:aws:lambda:us-west-2:123456789012:function:ToUpper
FunctionName     : MyFunction
Handler          : AssemblyName::Namespace.ClassName::MethodName
KMSKeyArn        :
LastModified     : 2016-12-29T23:50:14.207+0000
MemorySize       : 128
Role             : arn:aws:iam::123456789012:role/LambdaFullExecRole
Runtime          : dotnetcore1.0
Timeout          : 3
Version          : $LATEST
VpcConfig        :
```

Beispiel 2: Dieses Beispiel ähnelt dem vorherigen, außer dass die Funktionsbinärdateien zuerst in einen Amazon S3 S3-Bucket hochgeladen werden (der sich in derselben Region wie die beabsichtigte Lambda-Funktion befinden muss) und das resultierende S3-Objekt dann beim Erstellen der Funktion referenziert wird.

```
Write-S3Object -BucketName mybucket -Key MyFunctionBinaries.zip -File .
\MyFunctionBinaries.zip
Publish-LMFunction -Description "My C# Lambda Function" `
        -FunctionName MyFunction `
        -BucketName mybucket `
        -Key MyFunctionBinaries.zip `
        -Handler "AssemblyName::Namespace.ClassName::MethodName" `
        -Role "arn:aws:iam::123456789012:role/LambdaFullExecRole" `
        -Runtime dotnetcore1.0 `
        -Environment_Variable @{ "envvar1"="value";"envvar2"="value" }
```

- Einzelheiten zur API finden Sie unter CreateFunction AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def create_function(
        self, function_name, handler_name, iam_role, deployment_package
    ):
        """
        Deploys a Lambda function.

        :param function_name: The name of the Lambda function.
        :param handler_name: The fully qualified name of the handler function.
 This
                             must include the file name and the function name.
        :param iam_role: The IAM role to use for the function.
```

```
        :param deployment_package: The deployment package that contains the
function
                                   code in .zip format.
        :return: The Amazon Resource Name (ARN) of the newly created function.
        """
        try:
            response = self.lambda_client.create_function(
                FunctionName=function_name,
                Description="AWS Lambda doc example",
                Runtime="python3.8",
                Role=iam_role.arn,
                Handler=handler_name,
                Code={"ZipFile": deployment_package},
                Publish=True,
            )
            function_arn = response["FunctionArn"]
            waiter = self.lambda_client.get_waiter("function_active_v2")
            waiter.wait(FunctionName=function_name)
            logger.info(
                "Created function '%s' with ARN: '%s'.",
                function_name,
                response["FunctionArn"],
            )
        except ClientError:
            logger.error("Couldn't create function %s.", function_name)
            raise
        else:
            return function_arn
```

- Einzelheiten zur API finden Sie CreateFunctionin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Deploys a Lambda function.
  #
  # @param function_name: The name of the Lambda function.
  # @param handler_name: The fully qualified name of the handler function. This
  #                      must include the file name and the function name.
  # @param role_arn: The IAM role to use for the function.
  # @param deployment_package: The deployment package that contains the function
  #                            code in .zip format.
  # @return: The Amazon Resource Name (ARN) of the newly created function.
  def create_function(function_name, handler_name, role_arn, deployment_package)
    response = @lambda_client.create_function({
                                                role: role_arn.to_s,
                                                function_name: function_name,
                                                handler: handler_name,
                                                runtime: "ruby2.7",
                                                code: {
                                                  zip_file: deployment_package
                                                },
                                                environment: {
                                                  variables: {
                                                    "LOG_LEVEL" => "info"
                                                  }
                                                }
```

```
                                                    })
    @lambda_client.wait_until(:function_active_v2, { function_name:
function_name}) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
    response
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error creating #{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

- Einzelheiten zur API finden Sie CreateFunctionin der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /**
     * Create a function, uploading from a zip file.
     */
    pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
anyhow::Error> {
        let code = self.prepare_function(zip_file, None).await?;

        let key = code.s3_key().unwrap().to_string();

        let role = self.create_role().await.map_err(|e| anyhow!(e))?;

        info!("Created iam role, waiting 15s for it to become active");
        tokio::time::sleep(Duration::from_secs(15)).await;

        info!("Creating lambda function {}", self.lambda_name);
```

```
        let _ = self
            .lambda_client
            .create_function()
            .function_name(self.lambda_name.clone())
            .code(code)
            .role(role.arn())
            .runtime(aws_sdk_lambda::types::Runtime::Providedal2)
            .handler("_unused")
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        self.lambda_client
            .publish_version()
            .function_name(self.lambda_name.clone())
            .send()
            .await?;

        Ok(key)
    }

    /**
     * Upload function code from a path to a zip file.
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
```

```
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
            .s3_key(key)
            .build())
    }
```

- Einzelheiten zur API finden Sie CreateFunctionin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    TRY.
        lo_lmd->createfunction(
            iv_functionname = iv_function_name
            iv_runtime = `python3.9`
            iv_role = iv_role_arn
            iv_handler = iv_handler
            io_code = io_zip_file
            iv_description = 'AWS Lambda code example'
        ).
        MESSAGE 'Lambda function created.' TYPE 'I'.
      CATCH /aws1/cx_lmdcodesigningcfgno00.
        MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdcodestorageexcdex.
        MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
      CATCH /aws1/cx_lmdcodeverification00.
        MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvalidcodesigex.
        MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
```

```
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie CreateFunctionin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteAlias`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteAlias`.

CLI

AWS CLI

Um einen Alias einer Lambda-Funktion zu löschen

Im folgenden `delete-alias` Beispiel wird der Alias mit dem Namen `LIVE` aus der `my-function` Lambda-Funktion gelöscht.

```
aws lambda delete-alias \
    --function-name my-function \
    --name LIVE
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz DeleteAlias.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die im Befehl erwähnte Lambda-Funktion Alias gelöscht.

```
Remove-LMAlias -FunctionName "MylambdaFunction123" -Name "NewAlias"
```

- Einzelheiten zur API finden Sie unter DeleteAlias AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteFunction`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteFunction`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Delete an AWS Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// delete.</param>
    /// <returns>A Boolean value that indicates the success of the action.</
returns>
    public async Task<bool> DeleteFunctionAsync(string functionName)
    {
        var request = new DeleteFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.DeleteFunctionAsync(request);

        // A return value of NoContent means that the request was processed.
        // In this case, the function was deleted, and the return value
        // is intentionally blank.
        return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;
    }
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
 (overrides config file).
        // clientConfig.region = "us-east-1";
```

```
    Aws::Lambda::LambdaClient client(clientConfig);

    Aws::Lambda::Model::DeleteFunctionRequest request;
    request.SetFunctionName(LAMBDA_NAME);

    Aws::Lambda::Model::DeleteFunctionOutcome outcome = client.DeleteFunction(
            request);

    if (outcome.IsSuccess()) {
        std::cout << "The lambda function was successfully deleted." <<
 std::endl;
    }
    else {
        std::cerr << "Error with Lambda::DeleteFunction. "
                  << outcome.GetError().GetMessage()
                  << std::endl;
    }
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Beispiel 1: Eine Lambda-Funktion anhand des Funktionsnamens löschen

Im folgenden Beispiel für `delete-function` wird die Lambda-Funktion `my-function` durch Angabe des Funktionsnamens gelöscht.

```
aws lambda delete-function \
    --function-name my-function
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Beispiel 2: Eine Lambda-Funktion anhand des Funktions-ARN löschen

Im folgenden Beispiel für `delete-function` wird die Lambda-Funktion `my-function` durch Angabe des ARN der Funktion gelöscht.

```
aws lambda delete-function \
```

```
    --function-name arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Beispiel 3: Eine Lambda-Funktion anhand eines teilweisen Funktions-ARN löschen

Im folgenden Beispiel für `delete-function` wird die Lambda-Funktion `my-function` durch Angabe des teilweisen ARN der Funktion gelöscht.

```
aws lambda delete-function \
    --function-name 123456789012:function:my-function
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(functionName string) {
```

```
 _, err := wrapper.LambdaClient.DeleteFunction(context.TODO(),
 &lambda.DeleteFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
 }
}
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for Go API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.model.DeleteFunctionRequest;
import software.amazon.awssdk.services.lambda.model.LambdaException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */
public class DeleteFunction {
    public static void main(String[] args) {
        final String usage = """

                Usage:
```

```
                    <functionName>\s

                Where:
                    functionName - The name of the Lambda function.\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        Region region = Region.US_EAST_1;
        LambdaClient awsLambda = LambdaClient.builder()
                .region(region)
                .build();

        deleteLambdaFunction(awsLambda, functionName);
        awsLambda.close();
    }

    public static void deleteLambdaFunction(LambdaClient awsLambda, String
 functionName) {
        try {
            DeleteFunctionRequest request = DeleteFunctionRequest.builder()
                    .functionName(functionName)
                    .build();

            awsLambda.deleteFunction(request);
            System.out.println("The " + functionName + " function was deleted");

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for Java 2.x API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/**
 * @param {string} funcName
 */
const deleteFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new DeleteFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for JavaScript API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun delLambdaFunction(myFunctionName: String) {
    val request =
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
```

```
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

- Einzelheiten zur API finden Sie DeleteFunctionin der API-Referenz zum AWS SDK für Kotlin.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function deleteFunction($functionName)
    {
        return $this->lambdaClient->deleteFunction([
            'FunctionName' => $functionName,
        ]);
    }
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for PHP API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel löscht eine bestimmte Version einer Lambda-Funktion

```
Remove-LMFunction -FunctionName "MylambdaFunction123" -Qualifier '3'
```

- Einzelheiten zur API finden Sie unter DeleteFunction AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def delete_function(self, function_name):
        """
        Deletes a Lambda function.

        :param function_name: The name of the function to delete.
        """
        try:
            self.lambda_client.delete_function(FunctionName=function_name)
        except ClientError:
            logger.exception("Couldn't delete function %s.", function_name)
            raise
```

- Einzelheiten zur API finden Sie DeleteFunctionin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Deletes a Lambda function.
  # @param function_name: The name of the function to delete.
  def delete_function(function_name)
    print "Deleting function: #{function_name}..."
    @lambda_client.delete_function(
      function_name: function_name
    )
    print "Done!".green
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
  end
```

- Einzelheiten zur API finden Sie DeleteFunctionin der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
   pub async fn delete_function(
       &self,
       location: Option<String>,
   ) -> (
       Result<DeleteFunctionOutput, anyhow::Error>,
       Result<DeleteRoleOutput, anyhow::Error>,
       Option<Result<DeleteObjectOutput, anyhow::Error>>,
   ) {
       info!("Deleting lambda function {}", self.lambda_name);
       let delete_function = self
           .lambda_client
           .delete_function()
           .function_name(self.lambda_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from);

       info!("Deleting iam role {}", self.role_name);
       let delete_role = self
           .iam_client
           .delete_role()
           .role_name(self.role_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from);

       let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
           if let Some(location) = location {
               info!("Deleting object {location}");
               Some(
```

```
                    self.s3_client
                        .delete_object()
                        .bucket(self.bucket.clone())
                        .key(location)
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                info!(?location, "Skipping delete object");
                None
            };

        (delete_function, delete_role, delete_object)
    }
```

- Einzelheiten zur API finden Sie DeleteFunctionin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    TRY.
        lo_lmd->deletefunction( iv_functionname = iv_function_name ).
        MESSAGE 'Lambda function deleted.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
```

```
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie DeleteFunctionin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteFunctionConcurrency`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteFunctionConcurrency`.

CLI

AWS CLI

Um das reservierte Limit für gleichzeitige Ausführung aus einer Funktion zu entfernen

Im folgenden `delete-function-concurrency` Beispiel wird das reservierte Limit für gleichzeitige Ausführung aus der Funktion gelöscht. `my-function`

```
aws lambda delete-function-concurrency \
    --function-name  my-function
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Parallelität für eine Lambda-Funktion reservieren im Lambda Developer Guide AWS .

- Einzelheiten zur API finden Sie unter DeleteFunctionParallelität in der Befehlsreferenz.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die Function Concurrency der Lambda-Funktion entfernt.

```
Remove-LMFunctionConcurrency -FunctionName "MylambdaFunction123"
```

- Einzelheiten zur API finden Sie unter DeleteFunctionParallelität in AWS Tools for PowerShell der Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`DeleteProvisionedConcurrencyConfig`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`DeleteProvisionedConcurrencyConfig`.

CLI

AWS CLI

Um eine bereitgestellte Parallelitätskonfiguration zu löschen

Im folgenden `delete-provisioned-concurrency-config` Beispiel wird die bereitgestellte Parallelitätskonfiguration für den `GREEN` Alias der angegebenen Funktion gelöscht.

```
aws lambda delete-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier GREEN
```

- Einzelheiten zur API finden Sie unter Befehlsreferenz DeleteProvisionedConcurrencyConfig.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die Provisioned Concurrency Configuration für einen bestimmten Alias entfernt.

```
Remove-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

- Einzelheiten zur API finden Sie unter DeleteProvisionedConcurrencyConfig AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetAccountSettings`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetAccountSettings`.

CLI

AWS CLI

Um Details zu Ihrem Konto in einer AWS Region abzurufen

Im folgenden `get-account-settings` Beispiel werden die Lambda-Grenzwerte und Nutzungsinformationen für Ihr Konto angezeigt.

```
aws lambda get-account-settings
```

Ausgabe:

```
{
    "AccountLimit": {
       "CodeSizeUnzipped": 262144000,
       "UnreservedConcurrentExecutions": 1000,
       "ConcurrentExecutions": 1000,
       "CodeSizeZipped": 52428800,
       "TotalCodeSize": 80530636800
```

```
    },
    "AccountUsage": {
       "FunctionCount": 4,
       "TotalCodeSize": 9426
    }
}
```

Weitere Informationen finden Sie unter AWS Lambda Limits im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter GetAccountEinstellungen in der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel wird angezeigt, um das Kontolimit und die Kontonutzung zu vergleichen

```
Get-LMAccountSetting | Select-Object
 @{Name="TotalCodeSizeLimit";Expression={$_.AccountLimit.TotalCodeSize}},
 @{Name="TotalCodeSizeUsed";Expression={$_.AccountUsage.TotalCodeSize}}
```

Ausgabe:

```
TotalCodeSizeLimit TotalCodeSizeUsed
------------------ -----------------
       80530636800          15078795
```

- Einzelheiten zur API finden Sie unter GetAccountEinstellungen in der AWS Tools for PowerShell Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetAlias`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetAlias`.

CLI

AWS CLI

Um Details zu einem Funktionsalias abzurufen

Im folgenden `get-alias` Beispiel werden Details für den Alias angezeigt, der in `LIVE` der `my-function` Lambda-Funktion benannt ist.

```
aws lambda get-alias \
    --function-name my-function \
    --name LIVE
```

Ausgabe:

```
{
    "FunctionVersion": "3",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",
    "Description": "alias for live version of function"
}
```

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz GetAlias.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel werden die Gewichtungen der Routing-Konfiguration für einen bestimmten Lambda-Funktionsalias abgerufen.

```
Get-LMAlias -FunctionName "MylambdaFunction123" -Name "newlabel1" -Select
 RoutingConfig
```

Ausgabe:

```
AdditionalVersionWeights
------------------------
{[1, 0.6]}
```

- Einzelheiten zur API finden Sie unter GetAlias AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetFunction`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetFunction`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
    /// Gets information about a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function for
    /// which to retrieve information.</param>
    /// <returns>Async Task.</returns>
    public async Task<FunctionConfiguration> GetFunctionAsync(string
functionName)
    {
        var functionRequest = new GetFunctionRequest
```

```
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.GetFunctionAsync(functionRequest);
        return response.Configuration;
    }
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
       Aws::Client::ClientConfiguration clientConfig;
       // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
       // clientConfig.region = "us-east-1";

   Aws::Lambda::LambdaClient client(clientConfig);

       Aws::Lambda::Model::GetFunctionRequest request;
       request.SetFunctionName(functionName);

       Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

       if (outcome.IsSuccess()) {
           std::cout << "Function retrieve.\n" <<

outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
                     << std::endl;
       }
       else {
```

```
            std::cerr << "Error with Lambda::GetFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Informationen zu einer Funktion abrufen

Das folgende Beispiel für `get-function` zeigt Informationen zur Funktion `my-function` an.

```
aws lambda get-function \
    --function-name  my-function
```

Ausgabe:

```
{
    "Concurrency": {
        "ReservedConcurrentExecutions": 100
    },
    "Code": {
        "RepositoryType": "S3",
        "Location": "https://awslambda-us-west-2-tasks.s3.us-
west-2.amazonaws.com/snapshots/123456789012/my-function..."
    },
    "Configuration": {
        "TracingConfig": {
            "Mode": "PassThrough"
        },
        "Version": "$LATEST",
        "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
        "FunctionName": "my-function",
        "VpcConfig": {
            "SubnetIds": [],
            "VpcId": "",
            "SecurityGroupIds": []
        },
```

```
        "MemorySize": 128,
        "RevisionId": "28f0fb31-5c5c-43d3-8955-03e76c5c1075",
        "CodeSize": 304,
        "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
        "Handler": "index.handler",
        "Role": "arn:aws:iam::123456789012:role/service-role/helloWorldPython-
role-uy3l9qyq",
        "Timeout": 3,
        "LastModified": "2019-09-24T18:20:35.054+0000",
        "Runtime": "nodejs10.x",
        "Description": ""
    }
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie GetFunctionin der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(functionName string) types.State {
 var state types.State
```

```
 funcOutput, err := wrapper.LambdaClient.GetFunction(context.TODO(),
 &lambda.GetFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
 } else {
  state = funcOutput.Configuration.State
 }
 return state
}
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for Go API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const getFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new GetFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for JavaScript API-Referenz.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function getFunction($functionName)
    {
        return $this->lambdaClient->getFunction([
            'FunctionName' => $functionName,
        ]);
    }
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for PHP API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def get_function(self, function_name):
        """
        Gets data about a Lambda function.
```

```
        :param function_name: The name of the function.
        :return: The function data.
        """
        response = None
        try:
            response =
 self.lambda_client.get_function(FunctionName=function_name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceNotFoundException":
                logger.info("Function %s does not exist.", function_name)
            else:
                logger.error(
                    "Couldn't get function %s. Here's why: %s: %s",
                    function_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        return response
```

- Einzelheiten zur API finden Sie GetFunctionin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end
```

```
# Gets data about a Lambda function.
#
# @param function_name: The name of the function.
# @return response: The function data, or nil if no such function exists.
def get_function(function_name)
  @lambda_client.get_function(
    {
      function_name: function_name
    }
  )
rescue Aws::Lambda::Errors::ResourceNotFoundException => e
  @logger.debug("Could not find function: #{function_name}:\n #{e.message}")
  nil
end
```

- Einzelheiten zur API finden Sie GetFunctionin der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /** Get the Lambda function with this Manager's name. */
   pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
       info!("Getting lambda function");
       self.lambda_client
           .get_function()
           .function_name(self.lambda_name.clone())
           .send()
           .await
           .map_err(anyhow::Error::from)
   }
```

- Einzelheiten zur API finden Sie GetFunctionin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    TRY.
        oo_result =  lo_lmd->getfunction( iv_functionname = iv_function_name ).
     " oo_result is returned for testing purposes. "
        MESSAGE 'Lambda function information retrieved.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie GetFunctionin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetFunctionConcurrency`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetFunctionConcurrency`.

CLI

AWS CLI

Um die reservierte Parallelitätseinstellung für eine Funktion anzuzeigen

Im folgenden `get-function-concurrency` Beispiel wird die reservierte Parallelitätseinstellung für die angegebene Funktion abgerufen.

```
aws lambda get-function-concurrency \
    --function-name my-function
```

Ausgabe:

```
{
    "ReservedConcurrentExecutions": 250
}
```

- Einzelheiten zur API finden Sie unter GetFunctionParallelität in AWS CLI der Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die reservierte Parallelität für die Lambda-Funktion abgerufen

```
Get-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -Select *
```

Ausgabe:

```
ReservedConcurrentExecutions
----------------------------
100
```

- Einzelheiten zur API finden Sie unter GetFunctionParallelität in AWS Tools for PowerShell der Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetFunctionConfiguration`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetFunctionConfiguration`.

CLI

AWS CLI

Um die versionsspezifischen Einstellungen einer Lambda-Funktion abzurufen

Im folgenden `get-function-configuration` Beispiel werden die Einstellungen für Version 2 der Funktion angezeigt. `my-function`

```
aws lambda get-function-configuration \
    --function-name  my-function:2
```

Ausgabe:

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "2",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
```

```
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
    "Handler": "index.handler"
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie unter GetFunctionKonfiguration in der AWS CLI Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel gibt die versionsspezifische Konfiguration einer Lambda-Funktion zurück.

```
Get-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Qualifier
 "PowershellAlias"
```

Ausgabe:

```
CodeSha256                  : uWOW0R7z+f0VyLuUg7+/D08hkMFsq0SF4seuyUZJ/R8=
CodeSize                    : 1426
DeadLetterConfig            : Amazon.Lambda.Model.DeadLetterConfig
Description                 : Verson 3 to test Aliases
Environment                 : Amazon.Lambda.Model.EnvironmentResponse
FunctionArn                 : arn:aws:lambda:us-
east-1:123456789012:function:MylambdaFunction123
                              :PowershellAlias
FunctionName                : MylambdaFunction123
Handler                     : lambda_function.launch_instance
KMSKeyArn                   :
LastModified                : 2019-12-25T09:52:59.872+0000
LastUpdateStatus            : Successful
LastUpdateStatusReason      :
LastUpdateStatusReasonCode  :
Layers                      : {}
MasterArn                   :
```

```
MemorySize                  : 128
RevisionId                  : 5d7de38b-87f2-4260-8f8a-e87280e10c33
Role                        : arn:aws:iam::123456789012:role/service-role/lambda
Runtime                     : python3.8
State                       : Active
StateReason                 :
StateReasonCode             :
Timeout                     : 600
TracingConfig               : Amazon.Lambda.Model.TracingConfigResponse
Version                     : 4
VpcConfig                   : Amazon.Lambda.Model.VpcConfigDetail
```

- Einzelheiten zur API finden Sie unter GetFunctionKonfiguration in der AWS Tools for PowerShell Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`GetPolicy`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetPolicy`.

CLI

AWS CLI

Um die ressourcenbasierte IAM-Richtlinie für eine Funktion, Version oder einen Alias abzurufen

Im folgenden `get-policy` Beispiel werden Richtlinieninformationen zur `my-function` Lambda-Funktion angezeigt.

```
aws lambda get-policy \
    --function-name my-function
```

Ausgabe:

```
{
    "Policy": {
        "Version":"2012-10-17",
```

```
        "Id":"default",
        "Statement":
        [
            {
                "Sid":"iot-events",
                "Effect":"Allow",
                "Principal": {"Service":"iotevents.amazonaws.com"},
                "Action":"lambda:InvokeFunction",
                "Resource":"arn:aws:lambda:us-west-2:123456789012:function:my-
function"
            }
        ]
    },
    "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668"
}
```

Weitere Informationen finden Sie unter Using Resource-based Policies for AWS Lambda im Lambda Developer Guide AWS .

- Einzelheiten zur API finden Sie unter GetPolicyBefehlsreferenz.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die Funktionsrichtlinie der Lambda-Funktion angezeigt

```
Get-LMPolicy -FunctionName test -Select Policy
```

Ausgabe:

```
{"Version":"2012-10-17","Id":"default","Statement":
[{"Sid":"xxxx","Effect":"Allow","Principal":
{"Service":"sns.amazonaws.com"},"Action":"lambda:InvokeFunction","Resource":"arn:aws:lamb
east-1:123456789102:function:test"}]}
```

- Einzelheiten zur API finden Sie unter GetPolicy AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **GetProvisionedConcurrencyConfig** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`GetProvisionedConcurrencyConfig`.

CLI

AWS CLI

Um eine bereitgestellte Parallelitätskonfiguration anzuzeigen

Im folgenden `get-provisioned-concurrency-config` Beispiel werden Details zur bereitgestellten Parallelitätskonfiguration für den `BLUE` Alias der angegebenen Funktion angezeigt.

```
aws lambda get-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE
```

Ausgabe:

```
{
    "RequestedProvisionedConcurrentExecutions": 100,
    "AvailableProvisionedConcurrentExecutions": 100,
    "AllocatedProvisionedConcurrentExecutions": 100,
    "Status": "READY",
    "LastModified": "2019-12-31T20:28:49+0000"
}
```

- Einzelheiten zur API finden Sie unter GetProvisionedConcurrencyConfig AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die bereitgestellte Parallelitätskonfiguration für den angegebenen Alias der Lambda-Funktion abgerufen.

```
C:\>Get-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
Qualifier "NewAlias1"
```

Ausgabe:

```
AllocatedProvisionedConcurrentExecutions : 0
AvailableProvisionedConcurrentExecutions : 0
LastModified                             : 2020-01-15T03:21:26+0000
RequestedProvisionedConcurrentExecutions : 70
Status                                   : IN_PROGRESS
StatusReason                             :
```

- Einzelheiten zur API finden Sie unter GetProvisionedConcurrencyConfigCmdlet-Referenz.AWS Tools for PowerShell

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`Invoke`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`Invoke`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
```

```
    /// Invoke a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// invoke.</param
    /// <param name="parameters">The parameter values that will be passed to the
function.</param>
    /// <returns>A System Threading Task.</returns>
    public async Task<string> InvokeFunctionAsync(
        string functionName,
        string parameters)
    {
        var payload = parameters;
        var request = new InvokeRequest
        {
            FunctionName = functionName,
            Payload = payload,
        };

        var response = await _lambdaService.InvokeAsync(request);
        MemoryStream stream = response.Payload;
        string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
        return returnValue;
    }
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for .NET -API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
```

```
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::InvokeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetLogType(logType);
        std::shared_ptr<Aws::IOStream> payload =
Aws::MakeShared<Aws::StringStream>(
                "FunctionTest");
        *payload << jsonPayload.View().WriteReadable();
        request.SetBody(payload);
        request.SetContentType("application/json");
        Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

        if (outcome.IsSuccess()) {
            invokeResult = std::move(outcome.GetResult());
            result = true;
            break;
        }

        else {
            std::cerr << "Error with Lambda::InvokeRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            break;
        }
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for C++ -API-Referenz.

CLI

AWS CLI

Beispiel 1: Eine Lambda-Funktion synchron aufrufen

Im folgenden Beispiel für `invoke` wird die Funktion `my-function` synchron aufgerufen. Die `cli-binary-format` Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Weitere Informationen finden Sie unter Von der AWS CLI unterstützte globale Befehlszeilenoptionen im AWS -CLI-Benutzerhandbuch.

```
aws lambda invoke \
    --function-name my-function \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }' \
    response.json
```

Ausgabe:

```
{
    "ExecutedVersion": "$LATEST",
    "StatusCode": 200
}
```

Weitere Informationen finden Sie unter Synchroner Aufruf im AWS -Lambda-Entwicklerhandbuch.

Beispiel 2: Eine Lambda-Funktion asynchron aufrufen

Im folgenden Beispiel für `invoke` wird die Funktion `my-function` asynchron aufgerufen. Die `cli-binary-format` Option ist erforderlich, wenn Sie AWS CLI Version 2 verwenden. Weitere Informationen finden Sie unter Von der AWS CLI unterstützte globale Befehlszeilenoptionen im AWS -CLI-Benutzerhandbuch.

```
aws lambda invoke \
    --function-name my-function \
    --invocation-type Event \
    --cli-binary-format raw-in-base64-out \
    --payload '{ "name": "Bob" }' \
    response.json
```

Ausgabe:

```
{
    "StatusCode": 202
}
```

Weitere Informationen finden Sie unter Asynchroner Aufruf im AWS -Lambda-Entwicklerhandbuch.

- API-Details finden Sie unter Invoke in der AWS CLI -Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// Invoke invokes the Lambda function specified by functionName, passing the
 parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
 tells
// Lambda to include the last few log lines in the returned result.
func (wrapper FunctionWrapper) Invoke(functionName string, parameters any, getLog
 bool) *lambda.InvokeOutput {
 logType := types.LogTypeNone
 if getLog {
  logType = types.LogTypeTail
 }
 payload, err := json.Marshal(parameters)
 if err != nil {
  log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
 }
 invokeOutput, err := wrapper.LambdaClient.Invoke(context.TODO(),
 &lambda.InvokeInput{
  FunctionName: aws.String(functionName),
  LogType:      logType,
  Payload:      payload,
 })
 if err != nil {
  log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
```

```
 }
 return invokeOutput
}
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for Go -API-Referenz.

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
import org.json.JSONObject;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.services.lambda.LambdaClient;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.lambda.model.InvokeRequest;
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.services.lambda.model.InvokeResponse;
import software.amazon.awssdk.services.lambda.model.LambdaException;

public class LambdaInvoke {

    /*
     * Function names appear as
     * arn:aws:lambda:us-west-2:335556666777:function:HelloFunction
     * you can retrieve the value by looking at the function in the AWS Console
     *
     * Also, set up your development environment, including your credentials.
     *
     * For information, see this documentation topic:
     *
     * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.
     * html
     */
```

```
    public static void main(String[] args) {
        final String usage = """

                Usage:
                    <functionName>\s

                Where:
                    functionName - The name of the Lambda function\s
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
                .region(region)
                .build();

        invokeFunction(awsLambda, functionName);
        awsLambda.close();
    }

    public static void invokeFunction(LambdaClient awsLambda, String
functionName) {

        InvokeResponse res = null;
        try {
            // Need a SdkBytes instance for the payload.
            JSONObject jsonObj = new JSONObject();
            jsonObj.put("inputValue", "2000");
            String json = jsonObj.toString();
            SdkBytes payload = SdkBytes.fromUtf8String(json);

            // Setup an InvokeRequest.
            InvokeRequest request = InvokeRequest.builder()
                    .functionName(functionName)
                    .payload(payload)
                    .build();

            res = awsLambda.invoke(request);
```

```
            String value = res.payload().asUtf8String();
            System.out.println(value);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for Java 2.x -API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for JavaScript -API-Referenz.

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun invokeFunction(functionNameVal: String) {
    val json = """{"inputValue":"1000"}"""
    val byteArray = json.trimIndent().encodeToByteArray()
    val request =
        InvokeRequest {
            functionName = functionNameVal
            logType = LogType.Tail
            payload = byteArray
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val res = awsLambda.invoke(request)
        println("${res.payload?.toString(Charsets.UTF_8)}")
        println("The log result is ${res.logResult}")
    }
}
```

- Weitere API-Informationen finden Sie unter Invoke in der API-Referenz zum AWS -SDK für Kotlin.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function invoke($functionName, $params, $logType = 'None')
    {
        return $this->lambdaClient->invoke([
            'FunctionName' => $functionName,
            'Payload' => json_encode($params),
            'LogType' => $logType,
        ]);
    }
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for PHP -API-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def invoke_function(self, function_name, function_params, get_log=False):
        """
        Invokes a Lambda function.

        :param function_name: The name of the function to invoke.
        :param function_params: The parameters of the function as a dict. This
 dict
                                is serialized to JSON before it is sent to
 Lambda.
        :param get_log: When true, the last 4 KB of the execution log are
 included in
                        the response.
        :return: The response from the function invocation.
```

```
        """
        try:
            response = self.lambda_client.invoke(
                FunctionName=function_name,
                Payload=json.dumps(function_params),
                LogType="Tail" if get_log else "None",
            )
            logger.info("Invoked function %s.", function_name)
        except ClientError:
            logger.exception("Couldn't invoke function %s.", function_name)
            raise
        return response
```

- Weitere API-Informationen finden Sie unter Invoke in der API-Referenz zum AWS -SDK für Python (Boto3).

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Invokes a Lambda function.
  # @param function_name [String] The name of the function to invoke.
  # @param payload [nil] Payload containing runtime parameters.
  # @return [Object] The response from the function invocation.
```

```
  def invoke_function(function_name, payload = nil)
    params = { function_name: function_name}
    params[:payload] = payload unless payload.nil?
    @lambda_client.invoke(params)
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n
 #{e.message}")
  end
```

- Weitere API-Informationen finden Sie unter Invoke in der AWS SDK for Ruby -API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /** Invoke the lambda function using calculator InvokeArgs. */
    pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
 anyhow::Error> {
        info!(?args, "Invoking {}", self.lambda_name);
        let payload = serde_json::to_string(&args)?;
        debug!(?payload, "Sending payload");
        self.lambda_client
            .invoke()
            .function_name(self.lambda_name.clone())
            .payload(Blob::new(payload))
            .send()
            .await
            .map_err(anyhow::Error::from)
    }

fn log_invoke_output(invoke: &InvokeOutput, message: &str) {
    if let Some(payload) = invoke.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
```

```
        info!("Could not extract payload")
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}
```

- Weitere API-Informationen finden Sie unter Aufrufen in der API-Referenz zum AWS -SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    TRY.
        DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
          `{`  &&
            `"action": "increment",`  &&
            `"number": 10` &&
          `}`
        ).
        oo_result =  lo_lmd->invoke(                 " oo_result is returned for
testing purposes. "
                iv_functionname = iv_function_name
                iv_payload = lv_json
             ).
        MESSAGE 'Lambda function invoked.' TYPE 'I'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvrequestcontex.
        MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvalidzipfileex.
```

```
        MESSAGE 'The deployment package could not be unzipped.' TYPE 'E'.
      CATCH /aws1/cx_lmdrequesttoolargeex.
        MESSAGE 'Invoke request body JSON input limit was exceeded by the request
payload.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
      CATCH /aws1/cx_lmdunsuppedmediatyp00.
        MESSAGE 'Invoke request body does not have JSON as its content type.'
TYPE 'E'.
    ENDTRY.
```

- Weitere API-Informationen finden Sie unter Invoke (Aufrufen) in der API-Referenz für das AWS -SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListFunctions`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListFunctions`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/// <summary>
/// Get a list of Lambda functions.
/// </summary>
/// <returns>A list of FunctionConfiguration objects.</returns>
public async Task<List<FunctionConfiguration>> ListFunctionsAsync()
{
    var functionList = new List<FunctionConfiguration>();

    var functionPaginator =
        _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
    await foreach (var function in functionPaginator.Functions)
    {
        functionList.Add(function);
    }

    return functionList;
}
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
       Aws::Client::ClientConfiguration clientConfig;
       // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
       // clientConfig.region = "us-east-1";

   Aws::Lambda::LambdaClient client(clientConfig);

   std::vector<Aws::String> functions;
   Aws::String marker;

   do {
       Aws::Lambda::Model::ListFunctionsRequest request;
       if (!marker.empty()) {
           request.SetMarker(marker);
       }

       Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
               request);

       if (outcome.IsSuccess()) {
           const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
           std::cout << result.GetFunctions().size()
                     << " lambda functions were retrieved." << std::endl;

           for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
               functions.push_back(functionConfiguration.GetFunctionName());
               std::cout << functions.size() << "  "
                         << functionConfiguration.GetDescription() << std::endl;
               std::cout << "   "
                         <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                 functionConfiguration.GetRuntime()) << ": "
                         << functionConfiguration.GetHandler()
                         << std::endl;
           }
           marker = result.GetNextMarker();
       }
       else {
           std::cerr << "Error with Lambda::ListFunctions. "
                     << outcome.GetError().GetMessage()
                     << std::endl;
```

```
        }
    } while (!marker.empty());
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Eine Liste der Lambda-Funktionen abrufen

Im folgenden Beispiel für `list-functions` wird eine Liste aller Funktionen für den aktuellen Benutzer angezeigt.

```
aws lambda list-functions
```

Ausgabe:

```
{
    "Functions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
            "FunctionName": "helloworld",
            "MemorySize": 128,
            "RevisionId": "1718e831-badf-4253-9518-d0644210af7b",
            "CodeSize": 294,
            "FunctionArn": "arn:aws:lambda:us-
west-2:123456789012:function:helloworld",
            "Handler": "helloworld.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-
role-zgur6bf4",
            "Timeout": 3,
            "LastModified": "2023-09-23T18:32:33.857+0000",
            "Runtime": "nodejs18.x",
            "Description": ""
        },
        {
```

```
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2023-10-01T16:47:28.490+0000",
            "Runtime": "nodejs18.x",
            "Description": ""
        },
        {
            "Layers": [
                {
                    "CodeSize": 41784542,
                    "Arn": "arn:aws:lambda:us-
west-2:420165488524:layer:AWSLambda-Python37-SciPy1x:2"
                },
                {
                    "CodeSize": 4121,
                    "Arn": "arn:aws:lambda:us-
west-2:123456789012:layer:pythonLayer:1"
                }
            ],
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "ZQukCqxtkqFgyF2cU41Avj99TKQ/hNihPtDtRcc08mI=",
            "FunctionName": "my-python-function",
            "VpcConfig": {
```

```
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 128,
            "RevisionId": "80b4eabc-acf7-4ea8-919a-e874c213707d",
            "CodeSize": 299,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
python-function",
            "Handler": "lambda_function.lambda_handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/my-python-
function-role-z5g7dr6n",
            "Timeout": 3,
            "LastModified": "2023-10-01T19:40:41.643+0000",
            "Runtime": "python3.11",
            "Description": ""
        }
    ]
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie ListFunctionsin der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}
```

```
// ListFunctions lists up to maxItems functions for the account. This function
 uses a
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(maxItems int)
 []types.FunctionConfiguration {
 var functions []types.FunctionConfiguration
 paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
 &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 for paginator.HasMorePages() && len(functions) < maxItems {
  pageOutput, err := paginator.NextPage(context.TODO())
  if err != nil {
   log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
  }
  functions = append(functions, pageOutput.Functions...)
 }
 return functions
}
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for Go API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const listFunctions = () => {
  const client = new LambdaClient({});
  const command = new ListFunctionsCommand({});

  return client.send(command);
};
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for JavaScript API-Referenz.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function listFunctions($maxItems = 50, $marker = null)
    {
        if (is_null($marker)) {
            return $this->lambdaClient->listFunctions([
                'MaxItems' => $maxItems,
            ]);
        }

        return $this->lambdaClient->listFunctions([
            'Marker' => $marker,
            'MaxItems' => $maxItems,
        ]);
    }
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for PHP API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel werden alle Lambda-Funktionen mit sortierter Codegröße angezeigt

```
Get-LMFunctionList | Sort-Object -Property CodeSize | Select-Object FunctionName,
 RunTime, Timeout, CodeSize
```

Ausgabe:

```
FunctionName                                                  Runtime   Timeout
 CodeSize
------------                                                  -------   -------
 --------
test                                                          python2.7       3
   243
MylambdaFunction123                                           python3.8     600
   659
myfuncpython1                                                 python3.8     303
   675
```

- Einzelheiten zur API finden Sie unter ListFunctions AWS Tools for PowerShellCmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def list_functions(self):
        """
        Lists the Lambda functions for the current account.
        """
        try:
            func_paginator = self.lambda_client.get_paginator("list_functions")
            for func_page in func_paginator.paginate():
                for func in func_page["Functions"]:
                    print(func["FunctionName"])
```

```
                    desc = func.get("Description")
                    if desc:
                        print(f"\t{desc}")
                    print(f"\t{func['Runtime']}: {func['Handler']}")
        except ClientError as err:
            logger.error(
                "Couldn't list functions. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

- Einzelheiten zur API finden Sie ListFunctionsin AWS SDK for Python (Boto3) API Reference.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Lists the Lambda functions for the current account.
  def list_functions
    functions = []
    @lambda_client.list_functions.each do |response|
      response["functions"].each do |function|
        functions.append(function["function_name"])
      end
```

```
    end
    functions
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
  end
```

- Einzelheiten zur API finden Sie ListFunctionsin der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /** List all Lambda functions in the current Region. */
    pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
        info!("Listing lambda functions");
        self.lambda_client
            .list_functions()
            .send()
            .await
            .map_err(anyhow::Error::from)
    }
```

- Einzelheiten zur API finden Sie ListFunctionsin der API-Referenz zum AWS SDK für Rust.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   TRY.
       oo_result =  lo_lmd->listfunctions( ).       " oo_result is returned for
testing purposes. "
       DATA(lt_functions) = oo_result->get_functions( ).
       MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
     CATCH /aws1/cx_lmdinvparamvalueex.
       MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
     CATCH /aws1/cx_lmdserviceexception.
       MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
     CATCH /aws1/cx_lmdtoomanyrequestsex.
       MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
   ENDTRY.
```

- Einzelheiten zur API finden Sie ListFunctionsin der API-Referenz zum AWS SDK für SAP ABAP.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListProvisionedConcurrencyConfigs`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListProvisionedConcurrencyConfigs`.

CLI

AWS CLI

Um eine Liste der bereitgestellten Parallelitätskonfigurationen abzurufen

Im folgenden `list-provisioned-concurrency-configs` Beispiel werden die bereitgestellten Parallelitätskonfigurationen für die angegebene Funktion aufgeführt.

```
aws lambda list-provisioned-concurrency-configs \
    --function-name my-function
```

Ausgabe:

```
{
    "ProvisionedConcurrencyConfigs": [
        {
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:GREEN",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:29:00+0000"
        },
        {
            "FunctionArn": "arn:aws:lambda:us-east-2:123456789012:function:my-
function:BLUE",
            "RequestedProvisionedConcurrentExecutions": 100,
            "AvailableProvisionedConcurrentExecutions": 100,
            "AllocatedProvisionedConcurrentExecutions": 100,
            "Status": "READY",
            "LastModified": "2019-12-31T20:28:49+0000"
        }
    ]
}
```

- Einzelheiten zur API finden Sie unter ListProvisionedConcurrencyConfigs AWS CLIBefehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die Liste der bereitgestellten Parallelitätskonfigurationen für eine Lambda-Funktion abgerufen.

```
Get-LMProvisionedConcurrencyConfigList -FunctionName "MylambdaFunction123"
```

- Einzelheiten zur API finden Sie unter ListProvisionedConcurrencyConfigsCmdlet-Referenz.AWS Tools for PowerShell

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListTags`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListTags`.

CLI

AWS CLI

Um die Liste der Tags für eine Lambda-Funktion abzurufen

Im folgenden `list-tags` Beispiel werden die der `my-function` Lambda-Funktion angehängten Tags angezeigt.

```
aws lambda list-tags \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function
```

Ausgabe:

```
{
    "Tags": {
        "Category": "Web Tools",
        "Department": "Sales"
    }
}
```

Weitere Informationen finden Sie unter Tagging Lambda Functions im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie ListTagsin AWS CLI der Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Ruft die Tags und ihre Werte ab, die derzeit für die angegebene Funktion festgelegt sind.

```
Get-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction"
```

Ausgabe:

```
Key        Value
---        -----
California Sacramento
Oregon     Salem
Washington Olympia
```

- Einzelheiten zur API finden Sie unter ListTags AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`ListVersionsByFunction`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`ListVersionsByFunction`.

CLI

AWS CLI

Um eine Liste von Versionen einer Funktion abzurufen

Im folgenden `list-versions-by-function` Beispiel wird die Liste der Versionen für die `my-function` Lambda-Funktion angezeigt.

```
aws lambda list-versions-by-function \
    --function-name my-function
```

Ausgabe:

```
{
    "Versions": [
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "$LATEST",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "93017fc9-59cb-41dc-901b-4845ce4bf668",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:$LATEST",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": ""
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "1",
            "CodeSha256": "5tT2qgzYUHoqwR616pZ2dpkn/0J1FrzJmlKidWaaCgk=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
```

```
            },
            "MemorySize": 256,
            "RevisionId": "949c8914-012e-4795-998c-e467121951b1",
            "CodeSize": 304,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:1",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-09-26T20:28:40.438+0000",
            "Runtime": "nodejs10.x",
            "Description": "new version"
        },
        {
            "TracingConfig": {
                "Mode": "PassThrough"
            },
            "Version": "2",
            "CodeSha256": "sU0cJ2/hOZevwV/lTxCuQqK3gDZP3i8gUoqUUVRmY6E=",
            "FunctionName": "my-function",
            "VpcConfig": {
                "SubnetIds": [],
                "VpcId": "",
                "SecurityGroupIds": []
            },
            "MemorySize": 256,
            "RevisionId": "cd669f21-0f3d-4e1c-9566-948837f2e2ea",
            "CodeSize": 266,
            "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:2",
            "Handler": "index.handler",
            "Role": "arn:aws:iam::123456789012:role/service-role/
helloWorldPython-role-uy3l9qyq",
            "Timeout": 3,
            "LastModified": "2019-10-01T16:47:28.490+0000",
            "Runtime": "nodejs10.x",
            "Description": "newer version"
        }
    ]
}
```

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz ListVersionsByFunction.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel gibt die Liste der versionsspezifischen Konfigurationen für jede Version der Lambda-Funktion zurück.

```
Get-LMVersionsByFunction -FunctionName "MylambdaFunction123"
```

Ausgabe:

```
FunctionName        Runtime   MemorySize Timeout CodeSize LastModified
      RoleName
------------        -------   ---------- ------- -------- ------------
      --------
MylambdaFunction123 python3.8        128     600      659
 2020-01-10T03:20:56.390+0000 lambda
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:19:02.238+0000 lambda
MylambdaFunction123 python3.8        128       5     1426
 2019-12-25T09:39:36.779+0000 lambda
MylambdaFunction123 python3.8        128     600     1426
 2019-12-25T09:52:59.872+0000 lambda
```

- Einzelheiten zur API finden Sie unter ListVersionsByFunction AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`PublishVersion`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`PublishVersion`.

CLI

AWS CLI

Um eine neue Version einer Funktion zu veröffentlichen

Das folgende `publish-version` Beispiel veröffentlicht eine neue Version der `my-function` Lambda-Funktion.

```
aws lambda publish-version \
    --function-name my-function
```

Ausgabe:

```
{
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "dBG9m8SGdmlEjw/JYXlhhvCrAv5TxvXsbL/RMr0fT/I=",
    "FunctionName": "my-function",
    "CodeSize": 294,
    "RevisionId": "f31d3d39-cc63-4520-97d4-43cd44c94c20",
    "MemorySize": 128,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:3",
    "Version": "2",
    "Role": "arn:aws:iam::123456789012:role/service-role/MyTestFunction-role-
zgur6bf4",
    "Timeout": 3,
    "LastModified": "2019-09-23T18:32:33.857+0000",
    "Handler": "my-function.handler",
    "Runtime": "nodejs10.x",
    "Description": ""
}
```

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz PublishVersion.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird eine Version für den vorhandenen Snapshot von Lambda Function Code erstellt

```
Publish-LMVersion -FunctionName "MylambdaFunction123" -Description "Publishing
 Existing Snapshot of function code as a  new version through Powershell"
```

- Einzelheiten zur API finden Sie unter PublishVersion AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`PutFunctionConcurrency`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`PutFunctionConcurrency`.

CLI

AWS CLI

Um ein reserviertes Parallelitätslimit für eine Funktion zu konfigurieren

Im folgenden `put-function-concurrency` Beispiel werden 100 reservierte gleichzeitige Ausführungen für die Funktion konfiguriert. `my-function`

```
aws lambda put-function-concurrency \
    --function-name  my-function  \
    --reserved-concurrent-executions 100
```

Ausgabe:

```
{
    "ReservedConcurrentExecutions": 100
}
```

Weitere Informationen finden Sie unter Parallelität für eine Lambda-Funktion reservieren im Lambda Developer Guide AWS .

- Einzelheiten zur API finden Sie unter PutFunctionParallelität in der Befehlsreferenz.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel werden die Parallelitätseinstellungen für die gesamte Funktion angewendet.

```
Write-LMFunctionConcurrency -FunctionName "MylambdaFunction123" -
ReservedConcurrentExecution 100
```

- Einzelheiten zur API finden Sie unter PutFunctionParallelität in der AWS Tools for PowerShell Cmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`PutProvisionedConcurrencyConfig`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`PutProvisionedConcurrencyConfig`.

CLI

AWS CLI

Um bereitgestellte Parallelität zuzuweisen

Im folgenden `put-provisioned-concurrency-config` Beispiel werden 100 bereitgestellte Parallelität für den Alias der angegebenen Funktion zugewiesen. `BLUE`

```
aws lambda put-provisioned-concurrency-config \
    --function-name my-function \
    --qualifier BLUE \
```

```
    --provisioned-concurrent-executions 100
```

Ausgabe:

```
{
    "Requested ProvisionedConcurrentExecutions": 100,
    "Allocated ProvisionedConcurrentExecutions": 0,
    "Status": "IN_PROGRESS",
    "LastModified": "2019-11-21T19:32:12+0000"
}
```

- Einzelheiten zur API finden Sie unter PutProvisionedConcurrencyConfigBefehlsreferenz.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird dem Alias einer Funktion eine bereitgestellte Parallelitätskonfiguration hinzugefügt

```
Write-LMProvisionedConcurrencyConfig -FunctionName "MylambdaFunction123" -
ProvisionedConcurrentExecution 20 -Qualifier "NewAlias1"
```

- Einzelheiten zur API finden Sie unter PutProvisionedConcurrencyConfig AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`RemovePermission`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`RemovePermission`.

CLI

AWS CLI

So entfernen Sie Berechtigungen aus einer vorhandenen Lambda-Funktion

Im folgenden `remove-permission` Beispiel wird die Berechtigung zum Aufrufen einer Funktion mit dem Namen entfernt. `my-function`

```
aws lambda remove-permission \
    --function-name my-function \
    --statement-id sns
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Using Resource-based Policies for AWS Lambda im Lambda Developer Guide AWS .

- Einzelheiten zur API finden Sie unter RemovePermissionBefehlsreferenz.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: In diesem Beispiel wird die Funktionsrichtlinie für die angegebene StatementId Lambda-Funktion entfernt.

```
$policy =  Get-LMPolicy -FunctionName "MylambdaFunction123" -Select Policy |
 ConvertFrom-Json| Select-Object -ExpandProperty Statement
Remove-LMPermission -FunctionName "MylambdaFunction123" -StatementId
 $policy[0].Sid
```

- Einzelheiten zur API finden Sie unter RemovePermission AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`TagResource`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`TagResource`.

CLI

AWS CLI

Um einer vorhandenen Lambda-Funktion Tags hinzuzufügen

Im folgenden `tag-resource` Beispiel wird der angegebenen Lambda-Funktion ein Tag mit dem Schlüsselnamen `DEPARTMENT` und `Department A` dem Wert von hinzugefügt.

```
aws lambda tag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tags "DEPARTMENT=Department A"
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Tagging Lambda Functions im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie TagResourcein AWS CLI der Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Fügt die drei Tags (Washington, Oregon und Kalifornien) und ihre zugehörigen Werte der angegebenen Funktion hinzu, die durch ihren ARN identifiziert wird.

```
Add-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -Tag @{ "Washington" = "Olympia";
 "Oregon" = "Salem"; "California" = "Sacramento" }
```

- Einzelheiten zur API finden Sie unter TagResource AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`UntagResource`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`UntagResource`.

CLI

AWS CLI

Um Tags aus einer vorhandenen Lambda-Funktion zu entfernen

Im folgenden `untag-resource` Beispiel wird das Tag mit dem `DEPARTMENT` Schlüsselnamen-Tag aus der `my-function` Lambda-Funktion entfernt.

```
aws lambda untag-resource \
    --resource arn:aws:lambda:us-west-2:123456789012:function:my-function \
    --tag-keys DEPARTMENT
```

Mit diesem Befehl wird keine Ausgabe zurückgegeben.

Weitere Informationen finden Sie unter Tagging Lambda Functions im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie UntagResourcein AWS CLI der Befehlsreferenz.

PowerShell

Tools für PowerShell

Beispiel 1: Entfernt die bereitgestellten Tags aus einer Funktion. Das Cmdlet fordert Sie zur Bestätigung auf, bevor der Vorgang fortgesetzt wird, sofern der Schalter -Force nicht angegeben ist. Es wird ein einziger Aufruf an den Dienst gesendet, um die Tags zu entfernen.

```
Remove-LMResourceTag -Resource "arn:aws:lambda:us-
west-2:123456789012:function:MyFunction" -TagKey
 "Washington","Oregon","California"
```

Beispiel 2: Entfernt die bereitgestellten Tags aus einer Funktion. Das Cmdlet fordert Sie zur Bestätigung auf, bevor der Vorgang fortgesetzt wird, sofern der Schalter -Force nicht angegeben ist. Sobald der Dienst pro bereitgestelltem Tag aufgerufen wurde.

```
"Washington","Oregon","California" | Remove-LMResourceTag -Resource
 "arn:aws:lambda:us-west-2:123456789012:function:MyFunction"
```

- Einzelheiten zur API finden Sie unter UntagResource AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`UpdateAlias`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`UpdateAlias`.

CLI

AWS CLI

Um einen Funktionsalias zu aktualisieren

Im folgenden `update-alias` Beispiel wird der Aliasname so aktualisiert`LIVE`, dass er auf Version 3 der `my-function` Lambda-Funktion verweist.

```
aws lambda update-alias \
    --function-name my-function \
    --function-version 3 \
    --name LIVE
```

Ausgabe:

```
{
    "FunctionVersion": "3",
    "Name": "LIVE",
    "AliasArn": "arn:aws:lambda:us-west-2:123456789012:function:my-
function:LIVE",
    "RevisionId": "594f41fb-b85f-4c20-95c7-6ca5f2a92c93",
    "Description": "alias for live version of function"
}
```

Weitere Informationen finden Sie unter Konfiguration von AWS Lambda-Funktionsaliasen im AWS Lambda Developer Guide.

- Einzelheiten zur API finden Sie unter Befehlsreferenz UpdateAlias.AWS CLI

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel aktualisiert die Konfiguration einer vorhandenen Lambda-Funktion Alias. Der RoutingConfiguration Wert wird aktualisiert, sodass 60% (0,6) des Datenverkehrs auf Version 1 umgestellt werden

```
Update-LMAlias -FunctionName "MylambdaFunction123" -Description
 " Alias for version 2" -FunctionVersion 2 -Name "newlabel1" -
RoutingConfig_AdditionalVersionWeight @{Name="1";Value="0.6}
```

- Einzelheiten zur API finden Sie unter UpdateAlias AWS Tools for PowerShellCmdlet-Referenz.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`UpdateFunctionCode`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`UpdateFunctionCode`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /// <summary>
```

```
    /// Update an existing Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to update.</
param>
    /// <param name="bucketName">The bucket where the zip file containing
    /// the Lambda function code is stored.</param>
    /// <param name="key">The key name of the source code file.</param>
    /// <returns>Async Task.</returns>
    public async Task UpdateFunctionCodeAsync(
        string functionName,
        string bucketName,
        string key)
    {
        var functionCodeRequest = new UpdateFunctionCodeRequest
        {
            FunctionName = functionName,
            Publish = true,
            S3Bucket = bucketName,
            S3Key = key,
        };

        var response = await
 _lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
       Console.WriteLine($"The Function was last modified at
 {response.LastModified}.");
    }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
        Aws::Client::ClientConfiguration clientConfig;
        // Optional: Set to the AWS Region in which the bucket was created
 (overrides config file).
        // clientConfig.region = "us-east-1";

    Aws::Lambda::LambdaClient client(clientConfig);

        Aws::Lambda::Model::UpdateFunctionCodeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteLambdaFunction(client);
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();
        request.SetZipFile(
                Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                                       buffer.str().length()));
        request.SetPublish(true);

        Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
 client.UpdateFunctionCode(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda code was successfully updated." <<
 std::endl;
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionCode. "
```

```
                        << outcome.GetError().GetMessage()
                        << std::endl;
        }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Den Code einer Lambda-Funktion aktualisieren

Im folgenden Beispiel für `update-function-code` wird der Code der unveröffentlichten Version ($LATEST) der Funktion `my-function` durch den Inhalt der angegebenen ZIP-Datei ersetzt.

```
aws lambda update-function-code \
    --function-name  my-function \
    --zip-file fileb://my-function.zip
```

Ausgabe:

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
    "VpcConfig": {
        "SubnetIds": [],
```

```
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// UpdateFunctionCode updates the code for the Lambda function specified by
 functionName.
// The existing code for the Lambda function is entirely replaced by the code in
 the
// zipPackage buffer. After the update action is called, a
 lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(functionName string, zipPackage
 *bytes.Buffer) types.State {
 var state types.State
```

```
 _, err := wrapper.LambdaClient.UpdateFunctionCode(context.TODO(),
 &lambda.UpdateFunctionCodeInput{
  FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
 })
 if err != nil {
  log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
 functionName, err)
 } else {
  waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(context.TODO(),
 &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for Go API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const updateFunctionCode = async (funcName, newFunc) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
  const command = new UpdateFunctionCodeCommand({
```

```
    ZipFile: code,
    FunctionName: funcName,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for JavaScript API-Referenz.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function updateFunctionCode($functionName, $s3Bucket, $s3Key)
    {
        return $this->lambdaClient->updateFunctionCode([
            'FunctionName' => $functionName,
            'S3Bucket' => $s3Bucket,
            'S3Key' => $s3Key,
        ]);
    }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for PHP API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: Aktualisiert die Funktion mit dem Namen 'MyFunction' mit neuem Inhalt, der in der angegebenen ZIP-Datei enthalten ist. Für eine C#.NET Core Lambda-Funktion sollte die ZIP-Datei die kompilierte Assembly enthalten.

```
Update-LMFunctionCode -FunctionName MyFunction -ZipFilename .\UpdatedCode.zip
```

Beispiel 2: Dieses Beispiel ähnelt dem vorherigen, verwendet jedoch ein Amazon S3 S3-Objekt, das den aktualisierten Code enthält, um die Funktion zu aktualisieren.

```
Update-LMFunctionCode -FunctionName MyFunction -BucketName mybucket -Key
 UpdatedCode.zip
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in AWS Tools for PowerShell Cmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def update_function_code(self, function_name, deployment_package):
        """
        Updates the code for a Lambda function by submitting a .zip archive that
 contains
        the code for the function.
```

```
        :param function_name: The name of the function to update.
        :param deployment_package: The function code to update, packaged as bytes
 in
                                   .zip format.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_code(
                FunctionName=function_name, ZipFile=deployment_package
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in AWS SDK for Python (Boto3) API-Referenz.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
```

```
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the code for a Lambda function by submitting a .zip archive that
contains
  # the code for the function.

  # @param function_name: The name of the function to update.
  # @param deployment_package: The function code to update, packaged as bytes in
  #                            .zip format.
  # @return: Data about the update, including the status.
  def update_function_code(function_name, deployment_package)
    @lambda_client.update_function_code(
      function_name: function_name,
      zip_file: deployment_package
    )
    @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating function code for:
#{function_name}:\n #{e.message}")
    nil
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
  end
```

- Einzelheiten zur API finden Sie unter UpdateFunctionCode in der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /** Given a Path to a zip file, update the function's code and wait for the
 update to finish. */
    pub async fn update_function_code(
        &self,
        zip_file: PathBuf,
        key: String,
    ) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
        let function_code = self.prepare_function(zip_file, Some(key)).await?;

        info!("Updating code for {}", self.lambda_name);
        let update = self
            .lambda_client
            .update_function_code()
            .function_name(self.lambda_name.clone())
            .s3_bucket(self.bucket.clone())
            .s3_key(function_code.s3_key().unwrap().to_string())
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        Ok(update)
    }

    /**
     * Upload function code from a path to a zip file.
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
```

```
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
            .s3_key(key)
            .build())
    }
```

- Einzelheiten zur API finden Sie in der Referenz zum UpdateFunctionCode im AWS SDK für die Rust-API.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    TRY.
        oo_result = lo_lmd->updatefunctioncode(     " oo_result is returned for
testing purposes. "
```

```
              iv_functionname = iv_function_name
              iv_zipfile = io_zip_file
          ).

        MESSAGE 'Lambda function code updated.' TYPE 'I'.
      CATCH /aws1/cx_lmdcodesigningcfgno00.
        MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdcodestorageexcdex.
        MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
      CATCH /aws1/cx_lmdcodeverification00.
        MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvalidcodesigex.
        MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
      CATCH /aws1/cx_lmdinvparamvalueex.
        MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
      CATCH /aws1/cx_lmdresourceconflictex.
        MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
      CATCH /aws1/cx_lmdresourcenotfoundex.
        MESSAGE 'The requested resource does not exist.' TYPE 'E'.
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie in der Referenz zu UpdateFunctionCode in AWS SDK for SAP ABAP API.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung **`UpdateFunctionConfiguration`** mit einem AWS SDK oder CLI

Die folgenden Codebeispiele zeigen, wie es verwendet wird`UpdateFunctionConfiguration`.

Beispiele für Aktionen sind Codeauszüge aus größeren Programmen und müssen im Kontext ausgeführt werden. Im folgenden Codebeispiel können Sie diese Aktion im Kontext sehen:

- Erste Schritte mit Funktionen

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   /// <summary>
   /// Update the code of a Lambda function.
   /// </summary>
   /// <param name="functionName">The name of the function to update.</param>
   /// <param name="functionHandler">The code that performs the function's
actions.</param>
   /// <param name="environmentVariables">A dictionary of environment
variables.</param>
   /// <returns>A Boolean value indicating the success of the action.</returns>
   public async Task<bool> UpdateFunctionConfigurationAsync(
       string functionName,
       string functionHandler,
       Dictionary<string, string> environmentVariables)
   {
       var request = new UpdateFunctionConfigurationRequest
       {
           Handler = functionHandler,
           FunctionName = functionName,
           Environment = new Amazon.Lambda.Model.Environment { Variables =
environmentVariables },
       };

       var response = await
_lambdaService.UpdateFunctionConfigurationAsync(request);

       Console.WriteLine(response.LastModified);
```

```
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for .NET API-Referenz.

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
       Aws::Client::ClientConfiguration clientConfig;
       // Optional: Set to the AWS Region in which the bucket was created
(overrides config file).
       // clientConfig.region = "us-east-1";

   Aws::Lambda::LambdaClient client(clientConfig);

       Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;
       request.SetFunctionName(LAMBDA_NAME);
       Aws::Lambda::Model::Environment environment;
       environment.AddVariables("LOG_LEVEL", "DEBUG");
       request.SetEnvironment(environment);

       Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
client.UpdateFunctionConfiguration(
               request);

       if (outcome.IsSuccess()) {
           std::cout << "The lambda configuration was successfully updated."
                     << std::endl;
           break;
       }
```

```
        else {
            std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for C++ API-Referenz.

CLI

AWS CLI

Die Konfiguration einer Funktion ändern

Im folgenden Beispiel für `update-function-configuration` wird die Speichergröße für die unveröffentlichte Version ($LATEST) der Funktion `my-function` auf 256 MB geändert.

```
aws lambda update-function-configuration \
    --function-name  my-function \
    --memory-size 256
```

Ausgabe:

```
{
    "FunctionName": "my-function",
    "LastModified": "2019-09-26T20:28:40.438+0000",
    "RevisionId": "e52502d4-9320-4688-9cd6-152a6ab7490d",
    "MemorySize": 256,
    "Version": "$LATEST",
    "Role": "arn:aws:iam::123456789012:role/service-role/my-function-role-
uy3l9qyq",
    "Timeout": 3,
    "Runtime": "nodejs10.x",
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "CodeSha256": "5tT2qgzYUHaqwR716pZ2dpkn/0J1FrzJmlKidWoaCgk=",
    "Description": "",
```

```
    "VpcConfig": {
        "SubnetIds": [],
        "VpcId": "",
        "SecurityGroupIds": []
    },
    "CodeSize": 304,
    "FunctionArn": "arn:aws:lambda:us-west-2:123456789012:function:my-function",
    "Handler": "index.handler"
}
```

Weitere Informationen finden Sie unter Konfigurieren von AWS -Lambda-Funktionen im AWS -Lambda-Entwicklerhandbuch.

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS CLI Befehlsreferenz.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}



// UpdateFunctionConfiguration updates a map of environment variables configured
 for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(functionName string,
 envVars map[string]string) {
 _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(context.TODO(),
 &lambda.UpdateFunctionConfigurationInput{
```

```
  FunctionName: aws.String(functionName),
  Environment:  &types.Environment{Variables: envVars},
 })
 if err != nil {
  log.Panicf("Couldn't update configuration for %v. Here's why: %v",
 functionName, err)
 }
}
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for Go API-Referenz.

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
const updateFunctionConfiguration = (funcName) => {
  const client = new LambdaClient({});
  const config = readFileSync(`${dirname}../functions/config.json`).toString();
  const command = new UpdateFunctionConfigurationCommand({
    ...JSON.parse(config),
    FunctionName: funcName,
  });
  return client.send(command);
};
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for JavaScript API-Referenz.

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    public function updateFunctionConfiguration($functionName, $handler,
$environment = '')
    {
        return $this->lambdaClient->updateFunctionConfiguration([
            'FunctionName' => $functionName,
            'Handler' => "$handler.lambda_handler",
            'Environment' => $environment,
        ]);
    }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for PHP API-Referenz.

PowerShell

Tools für PowerShell

Beispiel 1: Dieses Beispiel aktualisiert die bestehende Lambda-Funktionskonfiguration

```
Update-LMFunctionConfiguration -FunctionName "MylambdaFunction123" -Handler
 "lambda_function.launch_instance" -Timeout 600 -Environment_Variable
 @{ "envvar1"="value";"envvar2"="value" } -Role arn:aws:iam::123456789101:role/
service-role/lambda -DeadLetterConfig_TargetArn arn:aws:sns:us-east-1:
 123456789101:MyfirstTopic
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS Tools for PowerShell Cmdlet-Referenz.

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    def update_function_configuration(self, function_name, env_vars):
        """
        Updates the environment variables for a Lambda function.

        :param function_name: The name of the function to update.
        :param env_vars: A dict of environment variables to update.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_configuration(
                FunctionName=function_name, Environment={"Variables": env_vars}
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function configuration %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration im AWS SDK for Python (Boto3) API-Referenz.

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
class LambdaWrapper
  attr_accessor :lambda_client

  def initialize
    @lambda_client = Aws::Lambda::Client.new
    @logger = Logger.new($stdout)
    @logger.level = Logger::WARN
  end

  # Updates the environment variables for a Lambda function.
  # @param function_name: The name of the function to update.
  # @param log_level: The log level of the function.
  # @return: Data about the update, including the status.
  def update_function_configuration(function_name, log_level)
    @lambda_client.update_function_configuration({
                                                   function_name: function_name,
                                                   environment: {
                                                     variables: {
                                                       "LOG_LEVEL" => log_level
                                                     }
                                                   }
                                                 })
    @lambda_client.wait_until(:function_updated_v2, { function_name:
 function_name}) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
```

```
    @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration in der AWS SDK for Ruby API-Referenz.

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
    /** Update the environment for a function. */
    pub async fn update_function_configuration(
        &self,
        environment: Environment,
    ) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
        info!(
            ?environment,
            "Updating environment for {}", self.lambda_name
        );
        let updated = self
            .lambda_client
            .update_function_configuration()
            .function_name(self.lambda_name.clone())
            .environment(environment)
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;
```

```
        Ok(updated)
    }
```

- Einzelheiten zur API finden Sie unter UpdateFunctionKonfiguration im AWS SDK für die Rust-API-Referenz.

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   TRY.
       oo_result = lo_lmd->updatefunctionconfiguration(     " oo_result is
returned for testing purposes. "
             iv_functionname = iv_function_name
             iv_runtime = iv_runtime
             iv_description  = 'Updated Lambda function'
             iv_memorysize  = iv_memory_size
         ).

       MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
     CATCH /aws1/cx_lmdcodesigningcfgno00.
       MESSAGE 'Code signing configuration does not exist.' TYPE 'E'.
     CATCH /aws1/cx_lmdcodeverification00.
       MESSAGE 'Code signature failed one or more validation checks for
signature mismatch or expiration.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvalidcodesigex.
       MESSAGE 'Code signature failed the integrity check.' TYPE 'E'.
     CATCH /aws1/cx_lmdinvparamvalueex.
       MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
     CATCH /aws1/cx_lmdresourceconflictex.
       MESSAGE 'Resource already exists or another operation is in progress.'
TYPE 'E'.
     CATCH /aws1/cx_lmdresourcenotfoundex.
       MESSAGE 'The requested resource does not exist.' TYPE 'E'.
```

```
      CATCH /aws1/cx_lmdserviceexception.
        MESSAGE 'An internal problem was encountered by the AWS Lambda service.'
TYPE 'E'.
      CATCH /aws1/cx_lmdtoomanyrequestsex.
        MESSAGE 'The maximum request throughput was reached.' TYPE 'E'.
    ENDTRY.
```

- Einzelheiten zur API finden Sie in der Referenz zur UpdateFunctionKonfiguration im AWS SDK für SAP ABAP API.

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Szenarien für Lambda mit SDKs AWS

Die folgenden Codebeispiele zeigen Ihnen, wie Sie allgemeine Szenarien in Lambda mit AWS SDKs implementieren. Diese Szenarien zeigen Ihnen, wie Sie bestimmte Aufgaben ausführen können, indem Sie mehrere Funktionen in Lambda aufrufen. Jedes Szenario enthält einen Link zu GitHub, wo Sie Anweisungen zur Einrichtung und Ausführung des Codes finden.

Beispiele

- Bestätigen Sie bekannte Amazon Cognito Cognito-Benutzer automatisch mit einer Lambda-Funktion mithilfe eines SDK AWS
- Automatisches Migrieren bekannter Amazon Cognito Cognito-Benutzer mit einer Lambda-Funktion mithilfe eines SDK AWS
- Erste Schritte beim Erstellen und Aufrufen von Lambda-Funktionen mithilfe eines SDK AWS
- Schreiben Sie benutzerdefinierte Aktivitätsdaten mit einer Lambda-Funktion nach der Amazon Cognito Cognito-Benutzerauthentifizierung mithilfe eines SDK AWS

Bestätigen Sie bekannte Amazon Cognito Cognito-Benutzer automatisch mit einer Lambda-Funktion mithilfe eines SDK AWS

Das folgende Codebeispiel zeigt, wie bekannte Amazon Cognito Cognito-Benutzer automatisch mit einer Lambda-Funktion bestätigt werden.

- Konfigurieren Sie einen Benutzerpool, um eine Lambda-Funktion für den `PreSignUp` Trigger aufzurufen.
- Melden Sie einen Benutzer bei Amazon Cognito an.
- Die Lambda-Funktion scannt eine DynamoDB-Tabelle und bestätigt automatisch bekannte Benutzer.
- Melden Sie sich als neuer Benutzer an und bereinigen Sie anschließend die Ressourcen.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
// AutoConfirm separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type AutoConfirm struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
 resources    Resources
 cognitoActor *actions.CognitoActions
}

// NewAutoConfirm constructs a new auto confirm runner.
func NewAutoConfirm(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) AutoConfirm {
 scenario := AutoConfirm{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
```

```
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddPreSignUpTrigger adds a Lambda handler as an invocation target for the
 PreSignUp trigger.
func (runner *AutoConfirm) AddPreSignUpTrigger(userPoolId string, functionArn
 string) {
 log.Printf("Let's add a Lambda function to handle the PreSignUp trigger from
 Cognito.\n" +
  "This trigger happens when a user signs up, and lets your function take action
 before the main Cognito\n" +
  "sign up processing occurs.\n")
 err := runner.cognitoActor.UpdateTriggers(
  userPoolId,
  actions.TriggerInfo{Trigger: actions.PreSignUp, HandlerArn:
 aws.String(functionArn)})
 if err != nil {
  panic(err)
 }
 log.Printf("Lambda function %v added to user pool %v to handle the PreSignUp
 trigger.\n",
  functionArn, userPoolId)
}

// SignUpUser signs up a user from the known user table with a password you
 specify.
func (runner *AutoConfirm) SignUpUser(clientId string, usersTable string)
 (string, string) {
 log.Println("Let's sign up a user to your Cognito user pool. When the user's
 email matches an email in the\n" +
  "DynamoDB known users table, it is automatically verified and the user is
 confirmed.")

 knownUsers, err := runner.helper.GetKnownUsers(usersTable)
 if err != nil {
  panic(err)
 }
 userChoice := runner.questioner.AskChoice("Which user do you want to use?\n",
 knownUsers.UserNameList())
 user := knownUsers.Users[userChoice]

 var signedUp bool
 var userConfirmed bool
```

```
 password := runner.questioner.AskPassword("Enter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !signedUp {
  log.Printf("Signing up user '%v' with email '%v' to Cognito.\n", user.UserName,
 user.UserEmail)
  userConfirmed, err = runner.cognitoActor.SignUp(clientId, user.UserName,
 password, user.UserEmail)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("Enter another password:", 8)
   } else {
    panic(err)
   }
  } else {
   signedUp = true
  }
 }
 log.Printf("User %v signed up, confirmed = %v.\n", user.UserName, userConfirmed)

 log.Println(strings.Repeat("-", 88))

 return user.UserName, password
}

// SignInUser signs in a user.
func (runner *AutoConfirm) SignInUser(clientId string, userName string, password
 string) string {
 runner.questioner.Ask("Press Enter when you're ready to continue.")
 log.Printf("Let's sign in as %v...\n", userName)
 authResult, err := runner.cognitoActor.SignIn(clientId, userName, password)
 if err != nil {
  panic(err)
 }
 log.Printf("Successfully signed in. Your access token starts with: %v...\n",
 (*authResult.AccessToken)[:10])
 log.Println(strings.Repeat("-", 88))
 return *authResult.AccessToken
}

// Run runs the scenario.
func (runner *AutoConfirm) Run(stackName string) {
 defer func() {
```

```
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup()
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Printf("Welcome\n")

 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(stackName)
 if err != nil {
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]
 runner.helper.PopulateUserTable(stackOutputs["TableName"])

 runner.AddPreSignUpTrigger(stackOutputs["UserPoolId"],
 stackOutputs["AutoConfirmFunctionArn"])
 runner.resources.triggers = append(runner.resources.triggers, actions.PreSignUp)
 userName, password := runner.SignUpUser(stackOutputs["UserPoolClientId"],
 stackOutputs["TableName"])
 runner.helper.ListRecentLogEvents(stackOutputs["AutoConfirmFunction"])
 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
  runner.SignInUser(stackOutputs["UserPoolClientId"], userName, password))

 runner.resources.Cleanup()

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Behandeln Sie den `PreSignUp` Trigger mit einer Lambda-Funktion.

```
const TABLE_NAME = "TABLE_NAME"

// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
```

```
type UserInfo struct {
 UserName  string `dynamodbav:"UserName"`
 UserEmail string `dynamodbav:"UserEmail"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
 userEmail, err := attributevalue.Marshal(user.UserEmail)
 if err != nil {
  panic(err)
 }
 return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
 dynamoClient *dynamodb.Client
}

// HandleRequest handles the PreSignUp event by looking up a user in an Amazon
 DynamoDB table and
// specifying whether they should be confirmed and verified.
func (h *handler) HandleRequest(ctx context.Context, event
 events.CognitoEventUserPoolsPreSignup) (events.CognitoEventUserPoolsPreSignup,
 error) {
 log.Printf("Received presignup from %v for user '%v'", event.TriggerSource,
 event.UserName)
 if event.TriggerSource != "PreSignUp_SignUp" {
  // Other trigger sources, such as PreSignUp_AdminInitiateAuth, ignore the
 response from this handler.
  return event, nil
 }
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserEmail: event.Request.UserAttributes["email"],
 }
 log.Printf("Looking up email %v in table %v.\n", user.UserEmail, tableName)
 output, err := h.dynamoClient.GetItem(ctx, &dynamodb.GetItemInput{
  Key:       user.GetKey(),
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Error looking up email %v.\n", user.UserEmail)
  return event, err
 }
```

```
 if output.Item == nil {
  log.Printf("Email %v not found. Email verification is required.\n",
 user.UserEmail)
  return event, err
 }

 err = attributevalue.UnmarshalMap(output.Item, &user)
 if err != nil {
  log.Printf("Couldn't unmarshal DynamoDB item. Here's why: %v\n", err)
  return event, err
 }

 if user.UserName != event.UserName {
  log.Printf("UserEmail %v found, but stored UserName '%v' does not match
 supplied UserName '%v'. Verification is required.\n",
   user.UserEmail, user.UserName, event.UserName)
 } else {
  log.Printf("UserEmail %v found with matching UserName %v. User is confirmed.
\n", user.UserEmail, user.UserName)
  event.Response.AutoConfirmUser = true
  event.Response.AutoVerifyEmail = true
 }

 return event, err
}

func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
}
```

Erstellen Sie eine Struktur, die allgemeine Aufgaben ausführt.

```
// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(stackName string) (actions.StackOutputs, error)
 PopulateUserTable(tableName string)
 GetKnownUsers(tableName string) (actions.UserList, error)
 AddKnownUser(tableName string, user actions.User)
 ListRecentLogEvents(functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}
```

```
// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
 (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
 err := helper.dynamoActor.PopulateTable(tableName)
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
 error) {
 knownUsers, err := helper.dynamoActor.Scan(tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
 return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
```

```
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
 events, err := helper.cwlActor.GetLogEvents(functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Erstellen Sie eine Struktur, die Amazon Cognito Cognito-Aktionen umschließt.

```
type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
```

```
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
 triggers ...TriggerInfo) error {
 output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
 })
 if err != nil {
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
```

```
func (actor CognitoActions) SignUp(clientId string, userName string, password
 string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(context.TODO(),
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}



// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
 string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
```

```
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}



// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
 (*types.CodeDeliveryDetailsType, error) {
 output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}



// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
 userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
```

```
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
 _, err := actor.CognitoClient.DeleteUser(context.TODO(),
 &cognitoidentityprovider.DeleteUserInput{
  AccessToken: aws.String(userAccessToken),
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
 userEmail string) error {
 _, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
 }
```

```
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
 string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
 &cognitoidentityprovider.AdminSetUserPasswordInput{
  Password:   aws.String(password),
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
}
```

Erstellen Sie eine Struktur, die DynamoDB-Aktionen umschließt.

```
// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
```

```
 UserName  string
 UserEmail string
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}

// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
 var err error
 var item map[string]types.AttributeValue
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
```

```
 _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
 &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
 var userList UserList
 output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Erstellen Sie eine Struktur, die Logs-Aktionen umschließt CloudWatch .

```
type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
 (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
 }
 return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
 logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(context.TODO(),
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
```

```
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Erstellen Sie eine Struktur, die Aktionen umschließt. AWS CloudFormation

```
// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(context.TODO(),
 &cloudformation.DescribeStacksInput{
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Ressourcen bereinigen.

```
// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
   log.Println("Use the AWS Management Console to remove any remaining resources
 \n" +
    "that were created for this scenario.")
  }
 }()

 wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
 resources that were created "+
  "during this demo (y/n)?", "y")
 if wantDelete {
  for _, accessToken := range resources.userAccessTokens {
   err := resources.cognitoActor.DeleteUser(accessToken)
   if err != nil {
    log.Println("Couldn't delete user during cleanup.")
    panic(err)
   }
   log.Println("Deleted user.")
  }
```

```
  triggerList := make([]actions.TriggerInfo, len(resources.triggers))
  for i := 0; i < len(resources.triggers); i++ {
   triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
 HandlerArn: nil}
  }
  err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,
 triggerList...)
  if err != nil {
   log.Println("Couldn't update Cognito triggers during cleanup.")
   panic(err)
  }
  log.Println("Removed Cognito triggers from user pool.")
 } else {
  log.Println("Be sure to remove resources when you're done with them to avoid
 unexpected charges!")
 }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Go -API-Referenz.
  - DeleteUser
  - InitiateAuth
  - SignUp
  - UpdateUserSchwimmbad

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Automatisches Migrieren bekannter Amazon Cognito Cognito-Benutzer mit einer Lambda-Funktion mithilfe eines SDK AWS

Das folgende Codebeispiel zeigt, wie bekannte Amazon Cognito Cognito-Benutzer mit einer Lambda-Funktion automatisch migriert werden.

- Konfigurieren Sie einen Benutzerpool, um eine Lambda-Funktion für den `MigrateUser` Trigger aufzurufen.

- Melden Sie sich bei Amazon Cognito mit einem Benutzernamen und einer E-Mail-Adresse an, die sich nicht im Benutzerpool befinden.
- Die Lambda-Funktion scannt eine DynamoDB-Tabelle und migriert bekannte Benutzer automatisch in den Benutzerpool.
- Führen Sie den Vorgang „Passwort vergessen“ aus, um das Passwort für den migrierten Benutzer zurückzusetzen.
- Melden Sie sich als neuer Benutzer an und bereinigen Sie anschließend die Ressourcen.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
import (
 "errors"
 "fmt"
 "log"
 "strings"
 "user_pools_and_lambda_triggers/actions"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider"
 "github.com/aws/aws-sdk-go-v2/service/cognitoidentityprovider/types"
 "github.com/awsdocs/aws-doc-sdk-examples/gov2/demotools"
)

// MigrateUser separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type MigrateUser struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
```

```
 resources    Resources
 cognitoActor *actions.CognitoActions
}

// NewMigrateUser constructs a new migrate user runner.
func NewMigrateUser(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) MigrateUser {
 scenario := MigrateUser{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddMigrateUserTrigger adds a Lambda handler as an invocation target for the
 MigrateUser trigger.
func (runner *MigrateUser) AddMigrateUserTrigger(userPoolId string, functionArn
 string) {
 log.Printf("Let's add a Lambda function to handle the MigrateUser trigger from
 Cognito.\n" +
  "This trigger happens when an unknown user signs in, and lets your function
 take action before Cognito\n" +
  "rejects the user.\n\n")
 err := runner.cognitoActor.UpdateTriggers(
  userPoolId,
  actions.TriggerInfo{Trigger: actions.UserMigration, HandlerArn:
 aws.String(functionArn)})
 if err != nil {
  panic(err)
 }
 log.Printf("Lambda function %v added to user pool %v to handle the MigrateUser
 trigger.\n",
  functionArn, userPoolId)

 log.Println(strings.Repeat("-", 88))
}

// SignInUser adds a new user to the known users table and signs that user in to
 Amazon Cognito.
```

```
func (runner *MigrateUser) SignInUser(usersTable string, clientId string) (bool,
 actions.User) {
 log.Println("Let's sign in a user to your Cognito user pool. When the username
 and email matches an entry in the\n" +
  "DynamoDB known users table, the email is automatically verified and the user
 is migrated to the Cognito user pool.")

 user := actions.User{}
 user.UserName = runner.questioner.Ask("\nEnter a username:")
 user.UserEmail = runner.questioner.Ask("\nEnter an email that you own. This
 email will be used to confirm user migration\n" +
  "during this example:")

 runner.helper.AddKnownUser(usersTable, user)

 var err error
 var resetRequired *types.PasswordResetRequiredException
 var authResult *types.AuthenticationResultType
 signedIn := false
 for !signedIn && resetRequired == nil {
  log.Printf("Signing in to Cognito as user '%v'. The expected result is a
 PasswordResetRequiredException.\n\n", user.UserName)
  authResult, err = runner.cognitoActor.SignIn(clientId, user.UserName, "_")
  if err != nil {
   if errors.As(err, &resetRequired) {
    log.Printf("\nUser '%v' is not in the Cognito user pool but was found in the
 DynamoDB known users table.\n"+
     "User migration is started and a password reset is required.",
 user.UserName)
   } else {
    panic(err)
   }
  } else {
   log.Printf("User '%v' successfully signed in. This is unexpected and probably
 means you have not\n"+
    "cleaned up a previous run of this scenario, so the user exist in the Cognito
 user pool.\n"+
    "You can continue this example and select to clean up resources, or manually
 remove\n"+
    "the user from your user pool and try again.", user.UserName)
   runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)
   signedIn = true
  }
```

```
 }

 log.Println(strings.Repeat("-", 88))
 return resetRequired != nil, user
}

// ResetPassword starts a password recovery flow.
func (runner *MigrateUser) ResetPassword(clientId string, user actions.User) {
 wantCode := runner.questioner.AskBool(fmt.Sprintf("In order to migrate the user
 to Cognito, you must be able to receive a confirmation\n"+
  "code by email at %v. Do you want to send a code (y/n)?", user.UserEmail), "y")
 if !wantCode {
  log.Println("To complete this example and successfully migrate a user to
 Cognito, you must enter an email\n" +
   "you own that can receive a confirmation code.")
  return
 }
 codeDelivery, err := runner.cognitoActor.ForgotPassword(clientId, user.UserName)
 if err != nil {
  panic(err)
 }
 log.Printf("\nA confirmation code has been sent to %v.",
 *codeDelivery.Destination)
 code := runner.questioner.Ask("Check your email and enter it here:")

 confirmed := false
 password := runner.questioner.AskPassword("\nEnter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !confirmed {
  log.Printf("\nConfirming password reset for user '%v'.\n", user.UserName)
  err = runner.cognitoActor.ConfirmForgotPassword(clientId, code, user.UserName,
 password)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("\nEnter another password:", 8)
   } else {
    panic(err)
   }
  } else {
   confirmed = true
  }
 }
```

```
 log.Printf("User '%v' successfully confirmed and migrated.\n", user.UserName)
 log.Println("Signing in with your username and password...")
 authResult, err := runner.cognitoActor.SignIn(clientId, user.UserName, password)
 if err != nil {
  panic(err)
 }
 log.Printf("Successfully signed in. Your access token starts with: %v...\n",
 (*authResult.AccessToken)[:10])
 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)

 log.Println(strings.Repeat("-", 88))
}

// Run runs the scenario.
func (runner *MigrateUser) Run(stackName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup()
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Printf("Welcome\n")

 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(stackName)
 if err != nil {
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]

 runner.AddMigrateUserTrigger(stackOutputs["UserPoolId"],
 stackOutputs["MigrateUserFunctionArn"])
 runner.resources.triggers = append(runner.resources.triggers,
 actions.UserMigration)
 resetNeeded, user := runner.SignInUser(stackOutputs["TableName"],
 stackOutputs["UserPoolClientId"])
 if resetNeeded {
  runner.helper.ListRecentLogEvents(stackOutputs["MigrateUserFunction"])
  runner.ResetPassword(stackOutputs["UserPoolClientId"], user)
 }
```

```
 runner.resources.Cleanup()

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Behandeln Sie den `MigrateUser` Trigger mit einer Lambda-Funktion.

```
const TABLE_NAME = "TABLE_NAME"

// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
type UserInfo struct {
 UserName  string `dynamodbav:"UserName"`
 UserEmail string `dynamodbav:"UserEmail"`
}

type handler struct {
 dynamoClient *dynamodb.Client
}

// HandleRequest handles the MigrateUser event by looking up a user in an Amazon
 DynamoDB table and
// specifying whether they should be migrated to the user pool.
func (h *handler) HandleRequest(ctx context.Context, event
 events.CognitoEventUserPoolsMigrateUser)
 (events.CognitoEventUserPoolsMigrateUser, error) {
 log.Printf("Received migrate trigger from %v for user '%v'",
 event.TriggerSource, event.UserName)
 if event.TriggerSource != "UserMigration_Authentication" {
  return event, nil
 }
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserName: event.UserName,
 }
 log.Printf("Looking up user '%v' in table %v.\n", user.UserName, tableName)
 filterEx := expression.Name("UserName").Equal(expression.Value(user.UserName))
```

```
 expr, err := expression.NewBuilder().WithFilter(filterEx).Build()
 if err != nil {
  log.Printf("Error building expression to query for user '%v'.\n",
 user.UserName)
  return event, err
 }
 output, err := h.dynamoClient.Scan(ctx, &dynamodb.ScanInput{
  TableName:                 aws.String(tableName),
  FilterExpression:          expr.Filter(),
  ExpressionAttributeNames:  expr.Names(),
  ExpressionAttributeValues: expr.Values(),
 })
 if err != nil {
  log.Printf("Error looking up user '%v'.\n", user.UserName)
  return event, err
 }
 if output.Items == nil || len(output.Items) == 0 {
  log.Printf("User '%v' not found, not migrating user.\n", user.UserName)
  return event, err
 }

 var users []UserInfo
 err = attributevalue.UnmarshalListOfMaps(output.Items, &users)
 if err != nil {
  log.Printf("Couldn't unmarshal DynamoDB items. Here's why: %v\n", err)
  return event, err
 }

 user = users[0]
 log.Printf("UserName '%v' found with email %v. User is migrated and must reset
 password.\n", user.UserName, user.UserEmail)
 event.CognitoEventUserPoolsMigrateUserResponse.UserAttributes =
 map[string]string{
  "email":          user.UserEmail,
  "email_verified": "true", // email_verified is required for the forgot password
 flow.
 }
 event.CognitoEventUserPoolsMigrateUserResponse.FinalUserStatus =
 "RESET_REQUIRED"
 event.CognitoEventUserPoolsMigrateUserResponse.MessageAction = "SUPPRESS"

 return event, err
}
```

```
func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
}
```

Erstellen Sie eine Struktur, die allgemeine Aufgaben ausführt.

```
// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(stackName string) (actions.StackOutputs, error)
 PopulateUserTable(tableName string)
 GetKnownUsers(tableName string) (actions.UserList, error)
 AddKnownUser(tableName string, user actions.User)
 ListRecentLogEvents(functionName string)
}

// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
```

```
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
 (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
 err := helper.dynamoActor.PopulateTable(tableName)
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
 error) {
 knownUsers, err := helper.dynamoActor.Scan(tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
 return knownUsers, err
```

```
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
 events, err := helper.cwlActor.GetLogEvents(functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Erstellen Sie eine Struktur, die Amazon Cognito Cognito-Aktionen umschließt.

```
type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
 triggers ...TriggerInfo) error {
 output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
 })
 if err != nil {
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
```

```
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(clientId string, userName string, password
 string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(context.TODO(),
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}
```

```
// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
 string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}



// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
 (*types.CodeDeliveryDetailsType, error) {
 output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}
```

```
// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
 userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
 _, err := actor.CognitoClient.DeleteUser(context.TODO(),
 &cognitoidentityprovider.DeleteUserInput{
  AccessToken: aws.String(userAccessToken),
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
 userEmail string) error {
```

```
 _, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
 }
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
 string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
 &cognitoidentityprovider.AdminSetUserPasswordInput{
  Password:   aws.String(password),
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
```

```
}
```

Erstellen Sie eine Struktur, die DynamoDB-Aktionen umschließt.

```
// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
 UserName  string
 UserEmail string
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}

// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}
```

```
// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
 var err error
 var item map[string]types.AttributeValue
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
 _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
 &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
 var userList UserList
 output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}
```

```
// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Erstellen Sie eine Struktur, die Logs-Aktionen umschließt CloudWatch .

```
type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
 (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
```

```
 }
 return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
 logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(context.TODO(),
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Erstellen Sie eine Struktur, die Aktionen umschließt. AWS CloudFormation

```
// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(context.TODO(),
 &cloudformation.DescribeStacksInput{
```

```
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Ressourcen bereinigen.

```
// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}

func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
```

```
    log.Println("Use the AWS Management Console to remove any remaining resources
  \n" +
     "that were created for this scenario.")
   }
  }()

  wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
  resources that were created "+
   "during this demo (y/n)?", "y")
  if wantDelete {
   for _, accessToken := range resources.userAccessTokens {
    err := resources.cognitoActor.DeleteUser(accessToken)
    if err != nil {
     log.Println("Couldn't delete user during cleanup.")
     panic(err)
    }
    log.Println("Deleted user.")
   }
   triggerList := make([]actions.TriggerInfo, len(resources.triggers))
   for i := 0; i < len(resources.triggers); i++ {
    triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
  HandlerArn: nil}
   }
   err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,
  triggerList...)
   if err != nil {
    log.Println("Couldn't update Cognito triggers during cleanup.")
    panic(err)
   }
   log.Println("Removed Cognito triggers from user pool.")
  } else {
   log.Println("Be sure to remove resources when you're done with them to avoid
  unexpected charges!")
  }
 }
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Go -API-Referenz.
  - ConfirmForgotPasswort
  - DeleteUser
  - ForgotPassword

- InitiateAuth
- SignUp
- UpdateUserSchwimmbad

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erste Schritte beim Erstellen und Aufrufen von Lambda-Funktionen mithilfe eines SDK AWS

Die folgenden Code-Beispiele veranschaulichen Folgendes:

- Erstellen Sie eine IAM-Rolle und eine Lambda-Funktion und laden Sie den Handlercode hoch.
- Rufen Sie die Funktion mit einem einzigen Parameter auf und erhalten Sie Ergebnisse.
- Aktualisieren Sie den Funktionscode und konfigurieren Sie mit einer Umgebungsvariablen.
- Rufen Sie die Funktion mit neuen Parametern auf und erhalten Sie Ergebnisse. Zeigt das zurückgegebene Ausführungsprotokoll an.
- Listen Sie die Funktionen für Ihr Konto auf und bereinigen Sie dann die Ressourcen.

Weitere Informationen zur Verwendung von Lambda finden Sie unter Erstellen einer Lambda-Funktion mit der Konsole.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie Methoden, die Lambda-Aktionen ausführen.

```
namespace LambdaActions;
```

```
using Amazon.Lambda;
using Amazon.Lambda.Model;

/// <summary>
/// A class that implements AWS Lambda methods.
/// </summary>
public class LambdaWrapper
{
    private readonly IAmazonLambda _lambdaService;

    /// <summary>
    /// Constructor for the LambdaWrapper class.
    /// </summary>
    /// <param name="lambdaService">An initialized Lambda service client.</param>
    public LambdaWrapper(IAmazonLambda lambdaService)
    {
        _lambdaService = lambdaService;
    }

    /// <summary>
    /// Creates a new Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the function.</param>
    /// <param name="s3Bucket">The Amazon Simple Storage Service (Amazon S3)
    /// bucket where the zip file containing the code is located.</param>
    /// <param name="s3Key">The Amazon S3 key of the zip file.</param>
    /// <param name="role">The Amazon Resource Name (ARN) of a role with the
    /// appropriate Lambda permissions.</param>
    /// <param name="handler">The name of the handler function.</param>
    /// <returns>The Amazon Resource Name (ARN) of the newly created
    /// Lambda function.</returns>
    public async Task<string> CreateLambdaFunctionAsync(
        string functionName,
        string s3Bucket,
        string s3Key,
        string role,
        string handler)
    {
        // Defines the location for the function code.
        // S3Bucket - The S3 bucket where the file containing
        //            the source code is stored.
        // S3Key    - The name of the file containing the code.
        var functionCode = new FunctionCode
        {
```

```
            S3Bucket = s3Bucket,
            S3Key = s3Key,
        };

        var createFunctionRequest = new CreateFunctionRequest
        {
            FunctionName = functionName,
            Description = "Created by the Lambda .NET API",
            Code = functionCode,
            Handler = handler,
            Runtime = Runtime.Dotnet6,
            Role = role,
        };

        var reponse = await
 _lambdaService.CreateFunctionAsync(createFunctionRequest);
        return reponse.FunctionArn;
    }


    /// <summary>
    /// Delete an AWS Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// delete.</param>
    /// <returns>A Boolean value that indicates the success of the action.</
returns>
    public async Task<bool> DeleteFunctionAsync(string functionName)
    {
        var request = new DeleteFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.DeleteFunctionAsync(request);

        // A return value of NoContent means that the request was processed.
        // In this case, the function was deleted, and the return value
        // is intentionally blank.
        return response.HttpStatusCode == System.Net.HttpStatusCode.NoContent;
    }


    /// <summary>
```

```
    /// Gets information about a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function for
    /// which to retrieve information.</param>
    /// <returns>Async Task.</returns>
    public async Task<FunctionConfiguration> GetFunctionAsync(string
functionName)
    {
        var functionRequest = new GetFunctionRequest
        {
            FunctionName = functionName,
        };

        var response = await _lambdaService.GetFunctionAsync(functionRequest);
        return response.Configuration;
    }



    /// <summary>
    /// Invoke a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to
    /// invoke.</param
    /// <param name="parameters">The parameter values that will be passed to the
function.</param>
    /// <returns>A System Threading Task.</returns>
    public async Task<string> InvokeFunctionAsync(
        string functionName,
        string parameters)
    {
        var payload = parameters;
        var request = new InvokeRequest
        {
            FunctionName = functionName,
            Payload = payload,
        };

        var response = await _lambdaService.InvokeAsync(request);
        MemoryStream stream = response.Payload;
        string returnValue =
System.Text.Encoding.UTF8.GetString(stream.ToArray());
        return returnValue;
    }
```

```
    /// <summary>
    /// Get a list of Lambda functions.
    /// </summary>
    /// <returns>A list of FunctionConfiguration objects.</returns>
    public async Task<List<FunctionConfiguration>> ListFunctionsAsync()
    {
        var functionList = new List<FunctionConfiguration>();

        var functionPaginator =
            _lambdaService.Paginators.ListFunctions(new ListFunctionsRequest());
        await foreach (var function in functionPaginator.Functions)
        {
            functionList.Add(function);
        }

        return functionList;
    }


    /// <summary>
    /// Update an existing Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the Lambda function to update.</
param>
    /// <param name="bucketName">The bucket where the zip file containing
    /// the Lambda function code is stored.</param>
    /// <param name="key">The key name of the source code file.</param>
    /// <returns>Async Task.</returns>
    public async Task UpdateFunctionCodeAsync(
        string functionName,
        string bucketName,
        string key)
    {
        var functionCodeRequest = new UpdateFunctionCodeRequest
        {
            FunctionName = functionName,
            Publish = true,
            S3Bucket = bucketName,
            S3Key = key,
        };

        var response = await
 _lambdaService.UpdateFunctionCodeAsync(functionCodeRequest);
```

```
        Console.WriteLine($"The Function was last modified at
{response.LastModified}.");
    }


    /// <summary>
    /// Update the code of a Lambda function.
    /// </summary>
    /// <param name="functionName">The name of the function to update.</param>
    /// <param name="functionHandler">The code that performs the function's
actions.</param>
    /// <param name="environmentVariables">A dictionary of environment
variables.</param>
    /// <returns>A Boolean value indicating the success of the action.</returns>
    public async Task<bool> UpdateFunctionConfigurationAsync(
        string functionName,
        string functionHandler,
        Dictionary<string, string> environmentVariables)
    {
        var request = new UpdateFunctionConfigurationRequest
        {
            Handler = functionHandler,
            FunctionName = functionName,
            Environment = new Amazon.Lambda.Model.Environment { Variables =
environmentVariables },
        };

        var response = await
_lambdaService.UpdateFunctionConfigurationAsync(request);

        Console.WriteLine(response.LastModified);

        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }


}
```

Erstellen Sie eine Funktion, die das Szenario ausführt.

```
global using System.Threading.Tasks;
```

```
global using Amazon.IdentityManagement;
global using Amazon.Lambda;
global using LambdaActions;
global using LambdaScenarioCommon;
global using Microsoft.Extensions.DependencyInjection;
global using Microsoft.Extensions.Hosting;
global using Microsoft.Extensions.Logging;
global using Microsoft.Extensions.Logging.Console;
global using Microsoft.Extensions.Logging.Debug;


using Amazon.Lambda.Model;
using Microsoft.Extensions.Configuration;

namespace LambdaBasics;

public class LambdaBasics
{
    private static ILogger logger = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the Amazon service.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft",
 LogLevel.Trace))
            .ConfigureServices((_, services) =>
            services.AddAWSService<IAmazonLambda>()
            .AddAWSService<IAmazonIdentityManagementService>()
            .AddTransient<LambdaWrapper>()
            .AddTransient<LambdaRoleWrapper>()
            .AddTransient<UIWrapper>()
        )
        .Build();

        var configuration = new ConfigurationBuilder()
            .SetBasePath(Directory.GetCurrentDirectory())
            .AddJsonFile("settings.json") // Load test settings from .json file.
            .AddJsonFile("settings.local.json",
            true) // Optionally load local settings.
```

```
        .Build();


        logger = LoggerFactory.Create(builder => { builder.AddConsole(); })
            .CreateLogger<LambdaBasics>();

        var lambdaWrapper = host.Services.GetRequiredService<LambdaWrapper>();
        var lambdaRoleWrapper =
host.Services.GetRequiredService<LambdaRoleWrapper>();
        var uiWrapper = host.Services.GetRequiredService<UIWrapper>();

        string functionName = configuration["FunctionName"]!;
        string roleName = configuration["RoleName"]!;
        string policyDocument = "{" +
            " \"Version\": \"2012-10-17\"," +
            " \"Statement\": [ " +
            "    {" +
            "        \"Effect\": \"Allow\"," +
            "        \"Principal\": {" +
            "            \"Service\": \"lambda.amazonaws.com\" " +
            "    }," +
            "        \"Action\": \"sts:AssumeRole\" " +
            "    }" +
            "]" +
        "}";

        var incrementHandler = configuration["IncrementHandler"];
        var calculatorHandler = configuration["CalculatorHandler"];
        var bucketName = configuration["BucketName"];
        var incrementKey = configuration["IncrementKey"];
        var calculatorKey = configuration["CalculatorKey"];
        var policyArn = configuration["PolicyArn"];

        uiWrapper.DisplayLambdaBasicsOverview();

        // Create the policy to use with the AWS Lambda functions and then attach
the
        // policy to a new role.
        var roleArn = await lambdaRoleWrapper.CreateLambdaRoleAsync(roleName,
policyDocument);

        Console.WriteLine("Waiting for role to become active.");
        uiWrapper.WaitABit(15, "Wait until the role is active before trying to
use it.");
```

```
        // Attach the appropriate AWS Identity and Access Management (IAM) role
policy to the new role.
        var success = await
lambdaRoleWrapper.AttachLambdaRolePolicyAsync(policyArn, roleName);
        uiWrapper.WaitABit(10, "Allow time for the IAM policy to be attached to
the role.");

        // Create the Lambda function using a zip file stored in an Amazon Simple
Storage Service
        // (Amazon S3) bucket.
        uiWrapper.DisplayTitle("Create Lambda Function");
        Console.WriteLine($"Creating the AWS Lambda function: {functionName}.");
        var lambdaArn = await lambdaWrapper.CreateLambdaFunctionAsync(
            functionName,
            bucketName,
            incrementKey,
            roleArn,
            incrementHandler);

        Console.WriteLine("Waiting for the new function to be available.");
        Console.WriteLine($"The AWS Lambda ARN is {lambdaArn}");

        // Get the Lambda function.
        Console.WriteLine($"Getting the {functionName} AWS Lambda function.");
        FunctionConfiguration config;
        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.State != State.Active);

        Console.WriteLine($"\nThe function, {functionName} has been created.");
        Console.WriteLine($"The runtime of this Lambda function is
{config.Runtime}.");

        uiWrapper.PressEnter();

        // List the Lambda functions.
        uiWrapper.DisplayTitle("Listing all Lambda functions.");
        var functions = await lambdaWrapper.ListFunctionsAsync();
        DisplayFunctionList(functions);
```

```
        uiWrapper.DisplayTitle("Invoke increment function");
        Console.WriteLine("Now that it has been created, invoke the Lambda
increment function.");
        string? value;
        do
        {
            Console.Write("Enter a value to increment: ");
            value = Console.ReadLine();
        }
        while (string.IsNullOrEmpty(value));

        string functionParameters = "{" +
            "\"action\": \"increment\", " +
            "\"x\": \"" + value + "\"" +
        "}";
        var answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
        Console.WriteLine($"{value} + 1 = {answer}.");

        uiWrapper.DisplayTitle("Update function");
        Console.WriteLine("Now update the Lambda function code.");
        await lambdaWrapper.UpdateFunctionCodeAsync(functionName, bucketName,
calculatorKey);

        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

        await lambdaWrapper.UpdateFunctionConfigurationAsync(
            functionName,
            calculatorHandler,
            new Dictionary<string, string> { { "LOG_LEVEL", "DEBUG" } });

        do
        {
            config = await lambdaWrapper.GetFunctionAsync(functionName);
            Console.Write(".");
        }
        while (config.LastUpdateStatus == LastUpdateStatus.InProgress);

        uiWrapper.DisplayTitle("Call updated function");
```

```
        Console.WriteLine("Now call the updated function...");

        bool done = false;

        do
        {
            string? opSelected;

            Console.WriteLine("Select the operation to perform:");
            Console.WriteLine("\t1. add");
            Console.WriteLine("\t2. subtract");
            Console.WriteLine("\t3. multiply");
            Console.WriteLine("\t4. divide");
            Console.WriteLine("\tOr enter \"q\" to quit.");
            Console.WriteLine("Enter the number (1, 2, 3, 4, or q) of the
operation you want to perform: ");
            do
            {
                Console.Write("Your choice? ");
                opSelected = Console.ReadLine();
            }
            while (opSelected == string.Empty);

            var operation = (opSelected) switch
            {
                "1" => "add",
                "2" => "subtract",
                "3" => "multiply",
                "4" => "divide",
                "q" => "quit",
                _ => "add",
            };

            if (operation == "quit")
            {
                done = true;
            }
            else
            {
                // Get two numbers and an action from the user.
                value = string.Empty;
                do
                {
                    Console.Write("Enter the first value: ");
```

```
                value = Console.ReadLine();
            }
            while (value == string.Empty);

            string? value2;
            do
            {
                Console.Write("Enter a second value: ");
                value2 = Console.ReadLine();
            }
            while (value2 == string.Empty);

            functionParameters = "{" +
                "\"action\": \"" + operation + "\", " +
                "\"x\": \"" + value + "\"," +
                "\"y\": \"" + value2 + "\"" +
            "}";

            answer = await lambdaWrapper.InvokeFunctionAsync(functionName,
functionParameters);
            Console.WriteLine($"The answer when we {operation} the two
numbers is: {answer}.");
        }

        uiWrapper.PressEnter();
    } while (!done);

    // Delete the function created earlier.

    uiWrapper.DisplayTitle("Clean up resources");
    // Detach the IAM policy from the IAM role.
    Console.WriteLine("First detach the IAM policy from the role.");
    success = await lambdaRoleWrapper.DetachLambdaRolePolicyAsync(policyArn,
roleName);
    uiWrapper.WaitABit(15, "Let's wait for the policy to be fully detached
from the role.");

    Console.WriteLine("Delete the AWS Lambda function.");
    success = await lambdaWrapper.DeleteFunctionAsync(functionName);
    if (success)
    {
        Console.WriteLine($"The {functionName} function was deleted.");
    }
    else
```

```
        {
            Console.WriteLine($"Could not remove the function {functionName}");
        }

        // Now delete the IAM role created for use with the functions
        // created by the application.
        Console.WriteLine("Now we can delete the role that we created.");
        success = await lambdaRoleWrapper.DeleteLambdaRoleAsync(roleName);
        if (success)
        {
            Console.WriteLine("The role has been successfully removed.");
        }
        else
        {
            Console.WriteLine("Couldn't delete the role.");
        }

        Console.WriteLine("The Lambda Scenario is now complete.");
        uiWrapper.PressEnter();

        // Displays a formatted list of existing functions returned by the
        // LambdaMethods.ListFunctions.
        void DisplayFunctionList(List<FunctionConfiguration> functions)
        {
            functions.ForEach(functionConfig =>
            {

 Console.WriteLine($"{functionConfig.FunctionName}\t{functionConfig.Description}");
            });
        }
    }
}


namespace LambdaActions;

using Amazon.IdentityManagement;
using Amazon.IdentityManagement.Model;

public class LambdaRoleWrapper
{
    private readonly IAmazonIdentityManagementService _lambdaRoleService;

    public LambdaRoleWrapper(IAmazonIdentityManagementService lambdaRoleService)
```

```
    {
        _lambdaRoleService = lambdaRoleService;
    }

    /// <summary>
    /// Attach an AWS Identity and Access Management (IAM) role policy to the
    /// IAM role to be assumed by the AWS Lambda functions created for the
 scenario.
    /// </summary>
    /// <param name="policyArn">The Amazon Resource Name (ARN) of the IAM
 policy.</param>
    /// <param name="roleName">The name of the IAM role to attach the IAM policy
 to.</param>
    /// <returns>A Boolean value indicating the success of the action.</returns>
    public async Task<bool> AttachLambdaRolePolicyAsync(string policyArn, string
 roleName)
    {
        var response = await _lambdaRoleService.AttachRolePolicyAsync(new
 AttachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    /// <summary>
    /// Create a new IAM role.
    /// </summary>
    /// <param name="roleName">The name of the IAM role to create.</param>
    /// <param name="policyDocument">The policy document for the new IAM role.</
param>
    /// <returns>A string representing the ARN for newly created role.</returns>
    public async Task<string> CreateLambdaRoleAsync(string roleName, string
 policyDocument)
    {
        var request = new CreateRoleRequest
        {
            AssumeRolePolicyDocument = policyDocument,
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.CreateRoleAsync(request);
        return response.Role.Arn;
    }

    /// <summary>
    /// Deletes an IAM role.
```

```
    /// </summary>
    /// <param name="roleName">The name of the role to delete.</param>
    /// <returns>A Boolean value indicating the success of the operation.</
returns>
    public async Task<bool> DeleteLambdaRoleAsync(string roleName)
    {
        var request = new DeleteRoleRequest
        {
            RoleName = roleName,
        };

        var response = await _lambdaRoleService.DeleteRoleAsync(request);
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }

    public async Task<bool> DetachLambdaRolePolicyAsync(string policyArn, string
 roleName)
    {
        var response = await _lambdaRoleService.DetachRolePolicyAsync(new
 DetachRolePolicyRequest { PolicyArn = policyArn, RoleName = roleName });
        return response.HttpStatusCode == System.Net.HttpStatusCode.OK;
    }
}


namespace LambdaScenarioCommon;
public class UIWrapper
{
    public readonly string SepBar = new('-', Console.WindowWidth);

    /// <summary>
    /// Show information about the AWS Lambda Basics scenario.
    /// </summary>
    public void DisplayLambdaBasicsOverview()
    {
        Console.Clear();

        DisplayTitle("Welcome to AWS Lambda Basics");
        Console.WriteLine("This example application does the following:");
        Console.WriteLine("\t1. Creates an AWS Identity and Access Management
 (IAM) role that will be assumed by the functions we create.");
        Console.WriteLine("\t2. Attaches an IAM role policy that has Lambda
 permissions.");
```

```
        Console.WriteLine("\t3. Creates a Lambda function that increments the
value passed to it.");
        Console.WriteLine("\t4. Calls the increment function and passes a
value.");
        Console.WriteLine("\t5. Updates the code so that the function is a simple
calculator.");
        Console.WriteLine("\t6. Calls the calculator function with the values
entered.");
        Console.WriteLine("\t7. Deletes the Lambda function.");
        Console.WriteLine("\t7. Detaches the IAM role policy.");
        Console.WriteLine("\t8. Deletes the IAM role.");
        PressEnter();
    }

    /// <summary>
    /// Display a message and wait until the user presses enter.
    /// </summary>
    public void PressEnter()
    {
        Console.Write("\nPress <Enter> to continue. ");
        _ = Console.ReadLine();
        Console.WriteLine();
    }

    /// <summary>
    /// Pad a string with spaces to center it on the console display.
    /// </summary>
    /// <param name="strToCenter">The string to be centered.</param>
    /// <returns>The padded string.</returns>
    public string CenterString(string strToCenter)
    {
        var padAmount = (Console.WindowWidth - strToCenter.Length) / 2;
        var leftPad = new string(' ', padAmount);
        return $"{leftPad}{strToCenter}";
    }

    /// <summary>
    /// Display a line of hyphens, the centered text of the title and another
    /// line of hyphens.
    /// </summary>
    /// <param name="strTitle">The string to be displayed.</param>
    public void DisplayTitle(string strTitle)
    {
        Console.WriteLine(SepBar);
```

```
        Console.WriteLine(CenterString(strTitle));
        Console.WriteLine(SepBar);
    }

    /// <summary>
    /// Display a countdown and wait for a number of seconds.
    /// </summary>
    /// <param name="numSeconds">The number of seconds to wait.</param>
    public void WaitABit(int numSeconds, string msg)
    {
        Console.WriteLine(msg);

        // Wait for the requested number of seconds.
        for (int i = numSeconds; i > 0; i--)
        {
            System.Threading.Thread.Sleep(1000);
            Console.Write($"{i}...");
        }

        PressEnter();
    }
}
```

Definieren Sie einen Lambda-Handler, der eine Zahl inkrementiert.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace LambdaIncrement;

public class Function
{

    /// <summary>
    /// A simple function increments the integer parameter.
    /// </summary>
    /// <param name="input">A JSON string containing an action, which must be
```

```
    /// "increment" and a string representing the value to increment.</param>
    /// <param name="context">The context object passed by Lambda containing
    /// information about invocation, function, and execution environment.</
param>
    /// <returns>A string representing the incremented value of the parameter.</
returns>
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext
 context)
    {
        if (input["action"] == "increment")
        {
            int inputValue = Convert.ToInt32(input["x"]);
            return inputValue + 1;
        }
        else
        {
            return 0;
        }
    }
}
```

Definieren Sie einen zweiten Lambda-Handler, der arithmetische Operationen ausführt.

```
using Amazon.Lambda.Core;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace LambdaCalculator;

public class Function
{

    /// <summary>
    /// A simple function that takes two number in string format and performs
    /// the requested arithmetic function.
    /// </summary>
    /// <param name="input">JSON data containing an action, and x and y values.
    /// Valid actions include: add, subtract, multiply, and divide.</param>
```

```
    /// <param name="context">The context object passed by Lambda containing
    /// information about invocation, function, and execution environment.</
param>
    /// <returns>A string representing the results of the calculation.</returns>
    public int FunctionHandler(Dictionary<string, string> input, ILambdaContext
 context)
    {
        var action = input["action"];
        int x = Convert.ToInt32(input["x"]);
        int y = Convert.ToInt32(input["y"]);
        int result;
        switch (action)
        {
            case "add":
                result = x + y;
                break;
            case "subtract":
                result = x - y;
                break;
            case "multiply":
                result = x * y;
                break;
            case "divide":
                if (y == 0)
                {
                    Console.Error.WriteLine("Divide by zero error.");
                    result = 0;
                }
                else
                    result = x / y;
                break;
            default:
                Console.Error.WriteLine($"{action} is not a valid operation.");
                result = 0;
                break;
        }
        return result;
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for .NET -API-Referenz.

- CreateFunction
- DeleteFunction
- GetFunction
- Aufrufen
- ListFunctions
- UpdateFunctionKode
- UpdateFunctionKonfiguration

C++

SDK für C++

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
//! Get started with functions scenario.
/*!
 \param clientConfig: AWS client configuration.
 \return bool: Successful completion.
 */
bool AwsDoc::Lambda::getStartedWithFunctionsScenario(
        const Aws::Client::ClientConfiguration &clientConfig) {

    Aws::Lambda::LambdaClient client(clientConfig);

    // 1. Create an AWS Identity and Access Management (IAM) role for Lambda
 function.
    Aws::String roleArn;
    if (!getIamRoleArn(roleArn, clientConfig)) {
        return false;
    }

    // 2. Create a Lambda function.
    int seconds = 0;
    do {
        Aws::Lambda::Model::CreateFunctionRequest request;
```

```
        request.SetFunctionName(LAMBDA_NAME);
        request.SetDescription(LAMBDA_DESCRIPTION); // Optional.
#if USE_CPP_LAMBDA_FUNCTION
        request.SetRuntime(Aws::Lambda::Model::Runtime::provided_al2);
        request.SetTimeout(15);
        request.SetMemorySize(128);

        // Assume the AWS Lambda function was built in Docker with same
 architecture
        // as this code.
#if  defined(__x86_64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::x86_64});
#elif defined(__aarch64__)
        request.SetArchitectures({Aws::Lambda::Model::Architecture::arm64});
#else
#error "Unimplemented architecture"
#endif // defined(architecture)
#else
        request.SetRuntime(Aws::Lambda::Model::Runtime::python3_8);
#endif
        request.SetRole(roleArn);
        request.SetHandler(LAMBDA_HANDLER_NAME);
        request.SetPublish(true);
        Aws::Lambda::Model::FunctionCode code;
        std::ifstream ifstream(INCREMENT_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();
```

```
        code.SetZipFile(Aws::Utils::ByteBuffer((unsigned char *)
buffer.str().c_str(),
                                               buffer.str().length()));
        request.SetCode(code);

        Aws::Lambda::Model::CreateFunctionOutcome outcome =
client.CreateFunction(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda function was successfully created. " <<
seconds
                      << " seconds elapsed." << std::endl;
            break;
        }
        else if (outcome.GetError().GetErrorType() ==
                 Aws::Lambda::LambdaErrors::INVALID_PARAMETER_VALUE &&
                 outcome.GetError().GetMessage().find("role") >= 0) {
            if ((seconds % 5) == 0) { // Log status every 10 seconds.
                std::cout
                        << "Waiting for the IAM role to become available as a
CreateFunction parameter. "
                        << seconds
                        << " seconds elapsed." << std::endl;

                std::cout << outcome.GetError().GetMessage() << std::endl;
            }
        }
        else {
            std::cerr << "Error with CreateFunction. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            deleteIamRole(clientConfig);
            return false;
        }
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
    } while (60 > seconds);

    std::cout << "The current Lambda function increments 1 by an input." <<
std::endl;

    // 3.  Invoke the Lambda function.
    {
```

```
        int increment = askQuestionForInt("Enter an increment integer: ");

        Aws::Lambda::Model::InvokeResult invokeResult;
        Aws::Utils::Json::JsonValue jsonPayload;
        jsonPayload.WithString("action", "increment");
        jsonPayload.WithInteger("number", increment);
        if (invokeLambdaFunction(jsonPayload, Aws::Lambda::Model::LogType::Tail,
                                 invokeResult, client)) {
            Aws::Utils::Json::JsonValue jsonValue(invokeResult.GetPayload());
            Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
                    jsonValue.View().GetAllObjects();
            auto iter = values.find("result");
            if (iter != values.end() && iter->second.IsIntegerType()) {
                {
                    std::cout << INCREMENT_RESUlT_PREFIX
                              << iter->second.AsInteger() << std::endl;
                }
            }
            else {
                std::cout << "There was an error in execution. Here is the log."
                          << std::endl;
                Aws::Utils::ByteBuffer buffer =
Aws::Utils::HashingUtils::Base64Decode(
                        invokeResult.GetLogResult());
                std::cout << "With log " << buffer.GetUnderlyingData() <<
std::endl;
            }
        }
    }

    std::cout
            << "The Lambda function will now be updated with new code. Press
return to continue, ";
    Aws::String answer;
    std::getline(std::cin, answer);

    // 4.  Update the Lambda function code.
    {
        Aws::Lambda::Model::UpdateFunctionCodeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        std::ifstream ifstream(CALCULATOR_LAMBDA_CODE.c_str(),
                               std::ios_base::in | std::ios_base::binary);
        if (!ifstream.is_open()) {
```

```
            std::cerr << "Error opening file " << INCREMENT_LAMBDA_CODE << "." <<
 std::endl;

#if USE_CPP_LAMBDA_FUNCTION
            std::cerr
                    << "The cpp Lambda function must be built following the
 instructions in the cpp_lambda/README.md file. "
                    << std::endl;
#endif
            deleteLambdaFunction(client);
            deleteIamRole(clientConfig);
            return false;
        }

        Aws::StringStream buffer;
        buffer << ifstream.rdbuf();
        request.SetZipFile(
                Aws::Utils::ByteBuffer((unsigned char *) buffer.str().c_str(),
                                       buffer.str().length()));
        request.SetPublish(true);

        Aws::Lambda::Model::UpdateFunctionCodeOutcome outcome =
 client.UpdateFunctionCode(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda code was successfully updated." <<
 std::endl;
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionCode. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    }

    std::cout
            << "This function uses an environment variable to control the logging
 level."
            << std::endl;
    std::cout
            << "UpdateFunctionConfiguration will be used to set the LOG_LEVEL to
 DEBUG."
            << std::endl;
```

```
    seconds = 0;

    // 5.  Update the Lambda function configuration.
    do {
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
        Aws::Lambda::Model::UpdateFunctionConfigurationRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        Aws::Lambda::Model::Environment environment;
        environment.AddVariables("LOG_LEVEL", "DEBUG");
        request.SetEnvironment(environment);

        Aws::Lambda::Model::UpdateFunctionConfigurationOutcome outcome =
client.UpdateFunctionConfiguration(
                request);

        if (outcome.IsSuccess()) {
            std::cout << "The lambda configuration was successfully updated."
                      << std::endl;
            break;
        }

            // RESOURCE_IN_USE: function code update not completed.
        else if (outcome.GetError().GetErrorType() !=
                 Aws::Lambda::LambdaErrors::RESOURCE_IN_USE) {
            if ((seconds % 10) == 0) { // Log status every 10 seconds.
                std::cout << "Lambda function update in progress . After " <<
seconds
                          << " seconds elapsed." << std::endl;
            }
        }
        else {
            std::cerr << "Error with Lambda::UpdateFunctionConfiguration. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }

    } while (0 < seconds);

    if (0 > seconds) {
        std::cerr << "Function failed to become active." << std::endl;
    }
    else {
        std::cout << "Updated function active after " << seconds << " seconds."
```

```
                  << std::endl;
    }

    std::cout
            << "\nThe new code applies an arithmetic operator to two variables, x
 an y."
            << std::endl;
    std::vector<Aws::String> operators = {"plus", "minus", "times", "divided-
by"};
    for (size_t i = 0; i < operators.size(); ++i) {
        std::cout << "   " << i + 1 << " " << operators[i] << std::endl;
    }

    // 6.  Invoke the updated Lambda function.
    do {
        int operatorIndex = askQuestionForIntRange("Select an operator index 1 -
 4 ", 1,
                                                   4);
        int x = askQuestionForInt("Enter an integer for the x value ");
        int y = askQuestionForInt("Enter an integer for the y value ");

        Aws::Utils::Json::JsonValue calculateJsonPayload;
        calculateJsonPayload.WithString("action", operators[operatorIndex - 1]);
        calculateJsonPayload.WithInteger("x", x);
        calculateJsonPayload.WithInteger("y", y);
        Aws::Lambda::Model::InvokeResult calculatedResult;
        if (invokeLambdaFunction(calculateJsonPayload,
                                 Aws::Lambda::Model::LogType::Tail,
                                 calculatedResult, client)) {
            Aws::Utils::Json::JsonValue jsonValue(calculatedResult.GetPayload());
            Aws::Map<Aws::String, Aws::Utils::Json::JsonView> values =
                    jsonValue.View().GetAllObjects();
            auto iter = values.find("result");
            if (iter != values.end() && iter->second.IsIntegerType()) {
                std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                          << operators[operatorIndex - 1] << " "
                          << y << " is " << iter->second.AsInteger() <<
 std::endl;
            }
            else if (iter != values.end() && iter->second.IsFloatingPointType())
 {
                std::cout << ARITHMETIC_RESULT_PREFIX << x << " "
                          << operators[operatorIndex - 1] << " "
                          << y << " is " << iter->second.AsDouble() << std::endl;
```

```
            }
            else {
                std::cout << "There was an error in execution. Here is the log."
                          << std::endl;
                Aws::Utils::ByteBuffer buffer =
Aws::Utils::HashingUtils::Base64Decode(
                        calculatedResult.GetLogResult());
                std::cout << "With log " << buffer.GetUnderlyingData() <<
std::endl;
            }
        }

        answer = askQuestion("Would you like to try another operation? (y/n) ");
    } while (answer == "y");

    std::cout
            << "A list of the lambda functions will be retrieved. Press return to
continue, ";
    std::getline(std::cin, answer);

    // 7.  List the Lambda functions.

    std::vector<Aws::String> functions;
    Aws::String marker;

    do {
        Aws::Lambda::Model::ListFunctionsRequest request;
        if (!marker.empty()) {
            request.SetMarker(marker);
        }

        Aws::Lambda::Model::ListFunctionsOutcome outcome = client.ListFunctions(
                request);

        if (outcome.IsSuccess()) {
            const Aws::Lambda::Model::ListFunctionsResult &result =
outcome.GetResult();
            std::cout << result.GetFunctions().size()
                      << " lambda functions were retrieved." << std::endl;

            for (const Aws::Lambda::Model::FunctionConfiguration
&functionConfiguration: result.GetFunctions()) {
                functions.push_back(functionConfiguration.GetFunctionName());
                std::cout << functions.size() << "  "
```

```
                        << functionConfiguration.GetDescription() << std::endl;
                std::cout << "   "
                        <<
Aws::Lambda::Model::RuntimeMapper::GetNameForRuntime(
                                functionConfiguration.GetRuntime()) << ": "
                        << functionConfiguration.GetHandler()
                        << std::endl;
            }
            marker = result.GetNextMarker();
        }
        else {
            std::cerr << "Error with Lambda::ListFunctions. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
        }
    } while (!marker.empty());

    // 8.  Get a Lambda function.
    if (!functions.empty()) {
        std::stringstream question;
        question << "Choose a function to retrieve between 1 and " <<
functions.size()
                 << " ";
        int functionIndex = askQuestionForIntRange(question.str(), 1,

static_cast<int>(functions.size()));

        Aws::String functionName = functions[functionIndex - 1];

        Aws::Lambda::Model::GetFunctionRequest request;
        request.SetFunctionName(functionName);

        Aws::Lambda::Model::GetFunctionOutcome outcome =
client.GetFunction(request);

        if (outcome.IsSuccess()) {
            std::cout << "Function retrieve.\n" <<

outcome.GetResult().GetConfiguration().Jsonize().View().WriteReadable()
                      << std::endl;
        }
        else {
            std::cerr << "Error with Lambda::GetFunction. "
                      << outcome.GetError().GetMessage()
```

```
                        << std::endl;
        }
    }

    std::cout << "The resources will be deleted. Press return to continue, ";
    std::getline(std::cin, answer);

    // 9.  Delete the Lambda function.
    bool result = deleteLambdaFunction(client);

    // 10. Delete the IAM role.
    return result && deleteIamRole(clientConfig);
}

//! Routine which invokes a Lambda function and returns the result.
/*!
 \param jsonPayload: Payload for invoke function.
 \param logType: Log type setting for invoke function.
 \param invokeResult: InvokeResult object to receive the result.
 \param client: Lambda client.
 \return bool: Successful completion.
 */
bool
AwsDoc::Lambda::invokeLambdaFunction(const Aws::Utils::Json::JsonValue
 &jsonPayload,
                                     Aws::Lambda::Model::LogType logType,
                                     Aws::Lambda::Model::InvokeResult
 &invokeResult,
                                     const Aws::Lambda::LambdaClient &client) {
    int seconds = 0;
    bool result = false;
    /*
     * In this example, the Invoke function can be called before recently created
 resources are
     * available.  The Invoke function is called repeatedly until the resources
 are
     * available.
     */
    do {
        Aws::Lambda::Model::InvokeRequest request;
        request.SetFunctionName(LAMBDA_NAME);
        request.SetLogType(logType);
        std::shared_ptr<Aws::IOStream> payload =
 Aws::MakeShared<Aws::StringStream>(
```

```
                "FunctionTest");
        *payload << jsonPayload.View().WriteReadable();
        request.SetBody(payload);
        request.SetContentType("application/json");
        Aws::Lambda::Model::InvokeOutcome outcome = client.Invoke(request);

        if (outcome.IsSuccess()) {
            invokeResult = std::move(outcome.GetResult());
            result = true;
            break;
        }

            // ACCESS_DENIED: because the role is not available yet.
            // RESOURCE_CONFLICT: because the Lambda function is being created or
 updated.
        else if ((outcome.GetError().GetErrorType() ==
                  Aws::Lambda::LambdaErrors::ACCESS_DENIED) ||
                 (outcome.GetError().GetErrorType() ==
                  Aws::Lambda::LambdaErrors::RESOURCE_CONFLICT)) {
            if ((seconds % 5) == 0) { // Log status every 10 seconds.
                std::cout << "Waiting for the invoke api to be available, status
 " <<
                          ((outcome.GetError().GetErrorType() ==
                            Aws::Lambda::LambdaErrors::ACCESS_DENIED ?
                            "ACCESS_DENIED" : "RESOURCE_CONFLICT")) << ". " <<
 seconds
                          << " seconds elapsed." << std::endl;
            }
        }
        else {
            std::cerr << "Error with Lambda::InvokeRequest. "
                      << outcome.GetError().GetMessage()
                      << std::endl;
            break;
        }
        ++seconds;
        std::this_thread::sleep_for(std::chrono::seconds(1));
    } while (seconds < 60);

    return result;
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for C++ -API-Referenz.

- CreateFunction
- DeleteFunction
- GetFunction
- Aufrufen
- ListFunctions
- UpdateFunctionKode
- UpdateFunctionKonfiguration

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie ein interaktives Szenario, das Ihnen zeigt, wie Sie mit Lambda-Funktionen loslegen können.

```
// GetStartedFunctionsScenario shows you how to use AWS Lambda to perform the
 following
// actions:
//
//  1. Create an AWS Identity and Access Management (IAM) role and Lambda
 function, then upload handler code.
//  2. Invoke the function with a single parameter and get results.
//  3. Update the function code and configure with an environment variable.
//  4. Invoke the function with new parameters and get results. Display the
 returned execution log.
//  5. List the functions for your account, then clean up resources.
type GetStartedFunctionsScenario struct {
 sdkConfig       aws.Config
 functionWrapper actions.FunctionWrapper
 questioner      demotools.IQuestioner
 helper          IScenarioHelper
 isTestRun       bool
```

```
}

// NewGetStartedFunctionsScenario constructs a GetStartedFunctionsScenario
 instance from a configuration.
// It uses the specified config to get a Lambda client and create wrappers for
 the actions
// used in the scenario.
func NewGetStartedFunctionsScenario(sdkConfig aws.Config, questioner
 demotools.IQuestioner,
 helper IScenarioHelper) GetStartedFunctionsScenario {
 lambdaClient := lambda.NewFromConfig(sdkConfig)
 return GetStartedFunctionsScenario{
  sdkConfig:       sdkConfig,
  functionWrapper: actions.FunctionWrapper{LambdaClient: lambdaClient},
  questioner:      questioner,
  helper:          helper,
 }
}

// Run runs the interactive scenario.
func (scenario GetStartedFunctionsScenario) Run() {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong with the demo.\n")
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Println("Welcome to the AWS Lambda get started with functions demo.")
 log.Println(strings.Repeat("-", 88))

 role := scenario.GetOrCreateRole()
 funcName := scenario.CreateFunction(role)
 scenario.InvokeIncrement(funcName)
 scenario.UpdateFunction(funcName)
 scenario.InvokeCalculator(funcName)
 scenario.ListFunctions()
 scenario.Cleanup(role, funcName)

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

```
// GetOrCreateRole checks whether the specified role exists and returns it if it
 does.
// Otherwise, a role is created that specifies Lambda as a trusted principal.
// The AWSLambdaBasicExecutionRole managed policy is attached to the role and the
 role
// is returned.
func (scenario GetStartedFunctionsScenario) GetOrCreateRole() *iamtypes.Role {
 var role *iamtypes.Role
 iamClient := iam.NewFromConfig(scenario.sdkConfig)
 log.Println("First, we need an IAM role that Lambda can assume.")
 roleName := scenario.questioner.Ask("Enter a name for the role:",
 demotools.NotEmpty{})
 getOutput, err := iamClient.GetRole(context.TODO(), &iam.GetRoleInput{
  RoleName: aws.String(roleName)})
 if err != nil {
  var noSuch *iamtypes.NoSuchEntityException
  if errors.As(err, &noSuch) {
   log.Printf("Role %v doesn't exist. Creating it....\n", roleName)
  } else {
   log.Panicf("Couldn't check whether role %v exists. Here's why: %v\n",
    roleName, err)
  }
 } else {
  role = getOutput.Role
  log.Printf("Found role %v.\n", *role.RoleName)
 }
 if role == nil {
  trustPolicy := PolicyDocument{
   Version: "2012-10-17",
   Statement: []PolicyStatement{{
    Effect:    "Allow",
    Principal: map[string]string{"Service": "lambda.amazonaws.com"},
    Action:    []string{"sts:AssumeRole"},
   }},
  }
  policyArn := "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
  createOutput, err := iamClient.CreateRole(context.TODO(), &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(trustPolicy.String()),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Panicf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  }
  role = createOutput.Role
```

```
  _, err = iamClient.AttachRolePolicy(context.TODO(), &iam.AttachRolePolicyInput{
   PolicyArn: aws.String(policyArn),
   RoleName:  aws.String(roleName),
  })
  if err != nil {
   log.Panicf("Couldn't attach a policy to role %v. Here's why: %v\n", roleName,
 err)
  }
  log.Printf("Created role %v.\n", *role.RoleName)
  log.Println("Let's give AWS a few seconds to propagate resources...")
  scenario.helper.Pause(10)
 }
 log.Println(strings.Repeat("-", 88))
 return role
}

// CreateFunction creates a Lambda function and uploads a handler written in
 Python.
// The code for the Python handler is packaged as a []byte in .zip format.
func (scenario GetStartedFunctionsScenario) CreateFunction(role *iamtypes.Role)
 string {
 log.Println("Let's create a function that increments a number.\n" +
  "The function uses the 'lambda_handler_basic.py' script found in the \n" +
  "'handlers' directory of this project.")
 funcName := scenario.questioner.Ask("Enter a name for the Lambda function:",
 demotools.NotEmpty{})
 zipPackage := scenario.helper.CreateDeploymentPackage("lambda_handler_basic.py",
 fmt.Sprintf("%v.py", funcName))
 log.Printf("Creating function %v and waiting for it to be ready.", funcName)
 funcState := scenario.functionWrapper.CreateFunction(funcName,
 fmt.Sprintf("%v.lambda_handler", funcName),
  role.Arn, zipPackage)
 log.Printf("Your function is %v.", funcState)
 log.Println(strings.Repeat("-", 88))
 return funcName
}

// InvokeIncrement invokes a Lambda function that increments a number. The
 function
// parameters are contained in a Go struct that is used to serialize the
 parameters to
// a JSON payload that is passed to the function.
// The result payload is deserialized into a Go struct that contains an int
 value.
```

```
func (scenario GetStartedFunctionsScenario) InvokeIncrement(funcName string) {
 parameters := actions.IncrementParameters{Action: "increment"}
 log.Println("Let's invoke our function. This function increments a number.")
 parameters.Number = scenario.questioner.AskInt("Enter a number to increment:",
 demotools.NotEmpty{})
 log.Printf("Invoking %v with %v...\n", funcName, parameters.Number)
 invokeOutput := scenario.functionWrapper.Invoke(funcName, parameters, false)
 var payload actions.LambdaResultInt
 err := json.Unmarshal(invokeOutput.Payload, &payload)
 if err != nil {
  log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
   funcName, err)
 }
 log.Printf("Invoking %v with %v returned %v.\n", funcName, parameters.Number,
 payload)
 log.Println(strings.Repeat("-", 88))
}

// UpdateFunction updates the code for a Lambda function by uploading a simple
 arithmetic
// calculator written in Python. The code for the Python handler is packaged as a
// []byte in .zip format.
// After the code is updated, the configuration is also updated with a new log
// level that instructs the handler to log additional information.
func (scenario GetStartedFunctionsScenario) UpdateFunction(funcName string) {
 log.Println("Let's update the function to an arithmetic calculator.\n" +
  "The function uses the 'lambda_handler_calculator.py' script found in the \n" +
  "'handlers' directory of this project.")
 scenario.questioner.Ask("Press Enter when you're ready.")
 log.Println("Creating deployment package...")
 zipPackage :=
 scenario.helper.CreateDeploymentPackage("lambda_handler_calculator.py",
  fmt.Sprintf("%v.py", funcName))
 log.Println("...and updating the Lambda function and waiting for it to be
 ready.")
 funcState := scenario.functionWrapper.UpdateFunctionCode(funcName, zipPackage)
 log.Printf("Updated function %v. Its current state is %v.", funcName, funcState)
 log.Println("This function uses an environment variable to control logging
 level.")
 log.Println("Let's set it to DEBUG to get the most logging.")
 scenario.functionWrapper.UpdateFunctionConfiguration(funcName,
  map[string]string{"LOG_LEVEL": "DEBUG"})
 log.Println(strings.Repeat("-", 88))
}
```

```
// InvokeCalculator invokes the Lambda calculator function. The parameters are
 stored in a
// Go struct that is used to serialize the parameters to a JSON payload. That
 payload is then passed
// to the function.
// The result payload is deserialized to a Go struct that stores the result as
 either an
// int or float32, depending on the kind of operation that was specified.
func (scenario GetStartedFunctionsScenario) InvokeCalculator(funcName string) {
 wantInvoke := true
 choices := []string{"plus", "minus", "times", "divided-by"}
 for wantInvoke {
  choice := scenario.questioner.AskChoice("Select an arithmetic operation:\n",
 choices)
  x := scenario.questioner.AskInt("Enter a value for x:", demotools.NotEmpty{})
  y := scenario.questioner.AskInt("Enter a value for y:", demotools.NotEmpty{})
  log.Printf("Invoking %v %v %v...", x, choices[choice], y)
  calcParameters := actions.CalculatorParameters{
   Action: choices[choice],
   X:      x,
   Y:      y,
  }
  invokeOutput := scenario.functionWrapper.Invoke(funcName, calcParameters, true)
  var payload any
  if choice == 3 { // divide-by results in a float.
   payload = actions.LambdaResultFloat{}
  } else {
   payload = actions.LambdaResultInt{}
  }
  err := json.Unmarshal(invokeOutput.Payload, &payload)
  if err != nil {
   log.Panicf("Couldn't unmarshal payload from invoking %v. Here's why: %v\n",
    funcName, err)
  }
  log.Printf("Invoking %v with %v %v %v returned %v.\n", funcName,
   calcParameters.X, calcParameters.Action, calcParameters.Y, payload)
  scenario.questioner.Ask("Press Enter to see the logs from the call.")
  logRes, err := base64.StdEncoding.DecodeString(*invokeOutput.LogResult)
  if err != nil {
   log.Panicf("Couldn't decode log result. Here's why: %v\n", err)
  }
  log.Println(string(logRes))
```

```
  wantInvoke = scenario.questioner.AskBool("Do you want to calculate again? (y/
n)", "y")
 }
 log.Println(strings.Repeat("-", 88))
}

// ListFunctions lists up to the specified number of functions for your account.
func (scenario GetStartedFunctionsScenario) ListFunctions() {
 count := scenario.questioner.AskInt(
  "Let's list functions for your account. How many do you want to see?",
 demotools.NotEmpty{})
 functions := scenario.functionWrapper.ListFunctions(count)
 log.Printf("Found %v functions:", len(functions))
 for _, function := range functions {
  log.Printf("\t%v", *function.FunctionName)
 }
 log.Println(strings.Repeat("-", 88))
}

// Cleanup removes the IAM and Lambda resources created by the example.
func (scenario GetStartedFunctionsScenario) Cleanup(role *iamtypes.Role, funcName
 string) {
 if scenario.questioner.AskBool("Do you want to clean up resources created for
 this example? (y/n)",
  "y") {
  iamClient := iam.NewFromConfig(scenario.sdkConfig)
  policiesOutput, err := iamClient.ListAttachedRolePolicies(context.TODO(),
   &iam.ListAttachedRolePoliciesInput{RoleName: role.RoleName})
  if err != nil {
   log.Panicf("Couldn't get policies attached to role %v. Here's why: %v\n",
    *role.RoleName, err)
  }
  for _, policy := range policiesOutput.AttachedPolicies {
   _, err = iamClient.DetachRolePolicy(context.TODO(),
 &iam.DetachRolePolicyInput{
    PolicyArn: policy.PolicyArn, RoleName: role.RoleName,
   })
   if err != nil {
    log.Panicf("Couldn't detach policy %v from role %v. Here's why: %v\n",
     *policy.PolicyArn, *role.RoleName, err)
   }
  }
  _, err = iamClient.DeleteRole(context.TODO(), &iam.DeleteRoleInput{RoleName:
 role.RoleName})
```

```
  if err != nil {
   log.Panicf("Couldn't delete role %v. Here's why: %v\n", *role.RoleName, err)
  }
  log.Printf("Deleted role %v.\n", *role.RoleName)

  scenario.functionWrapper.DeleteFunction(funcName)
  log.Printf("Deleted function %v.\n", funcName)
 } else {
  log.Println("Okay. Don't forget to delete the resources when you're done with
 them.")
 }
}
```

Erstellen einer Struktur, die die einzelnen Lambda-Aktionen umschließt.

```
// FunctionWrapper encapsulates function actions used in the examples.
// It contains an AWS Lambda service client that is used to perform user actions.
type FunctionWrapper struct {
 LambdaClient *lambda.Client
}


// GetFunction gets data about the Lambda function specified by functionName.
func (wrapper FunctionWrapper) GetFunction(functionName string) types.State {
 var state types.State
 funcOutput, err := wrapper.LambdaClient.GetFunction(context.TODO(),
 &lambda.GetFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't get function %v. Here's why: %v\n", functionName, err)
 } else {
  state = funcOutput.Configuration.State
 }
 return state
}
```

```
// CreateFunction creates a new Lambda function from code contained in the
 zipPackage
// buffer. The specified handlerName must match the name of the file and function
// contained in the uploaded code. The role specified by iamRoleArn is assumed by
// Lambda and grants specific permissions.
// When the function already exists, types.StateActive is returned.
// When the function is created, a lambda.FunctionActiveV2Waiter is used to wait
 until the
// function is active.
func (wrapper FunctionWrapper) CreateFunction(functionName string, handlerName
 string,
 iamRoleArn *string, zipPackage *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.CreateFunction(context.TODO(),
 &lambda.CreateFunctionInput{
  Code:         &types.FunctionCode{ZipFile: zipPackage.Bytes()},
  FunctionName: aws.String(functionName),
  Role:         iamRoleArn,
  Handler:      aws.String(handlerName),
  Publish:      true,
  Runtime:      types.RuntimePython38,
 })
 if err != nil {
  var resConflict *types.ResourceConflictException
  if errors.As(err, &resConflict) {
   log.Printf("Function %v already exists.\n", functionName)
   state = types.StateActive
  } else {
   log.Panicf("Couldn't create function %v. Here's why: %v\n", functionName, err)
  }
 } else {
  waiter := lambda.NewFunctionActiveV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(context.TODO(),
 &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}
```

```
// UpdateFunctionCode updates the code for the Lambda function specified by
 functionName.
// The existing code for the Lambda function is entirely replaced by the code in
 the
// zipPackage buffer. After the update action is called, a
 lambda.FunctionUpdatedV2Waiter
// is used to wait until the update is successful.
func (wrapper FunctionWrapper) UpdateFunctionCode(functionName string, zipPackage
 *bytes.Buffer) types.State {
 var state types.State
 _, err := wrapper.LambdaClient.UpdateFunctionCode(context.TODO(),
 &lambda.UpdateFunctionCodeInput{
  FunctionName: aws.String(functionName), ZipFile: zipPackage.Bytes(),
 })
 if err != nil {
  log.Panicf("Couldn't update code for function %v. Here's why: %v\n",
 functionName, err)
 } else {
  waiter := lambda.NewFunctionUpdatedV2Waiter(wrapper.LambdaClient)
  funcOutput, err := waiter.WaitForOutput(context.TODO(),
 &lambda.GetFunctionInput{
   FunctionName: aws.String(functionName)}, 1*time.Minute)
  if err != nil {
   log.Panicf("Couldn't wait for function %v to be active. Here's why: %v\n",
 functionName, err)
  } else {
   state = funcOutput.Configuration.State
  }
 }
 return state
}



// UpdateFunctionConfiguration updates a map of environment variables configured
 for
// the Lambda function specified by functionName.
func (wrapper FunctionWrapper) UpdateFunctionConfiguration(functionName string,
 envVars map[string]string) {
 _, err := wrapper.LambdaClient.UpdateFunctionConfiguration(context.TODO(),
 &lambda.UpdateFunctionConfigurationInput{
```

```
  FunctionName: aws.String(functionName),
  Environment:  &types.Environment{Variables: envVars},
 })
 if err != nil {
  log.Panicf("Couldn't update configuration for %v. Here's why: %v",
 functionName, err)
 }
}



// ListFunctions lists up to maxItems functions for the account. This function
 uses a
// lambda.ListFunctionsPaginator to paginate the results.
func (wrapper FunctionWrapper) ListFunctions(maxItems int)
 []types.FunctionConfiguration {
 var functions []types.FunctionConfiguration
 paginator := lambda.NewListFunctionsPaginator(wrapper.LambdaClient,
 &lambda.ListFunctionsInput{
  MaxItems: aws.Int32(int32(maxItems)),
 })
 for paginator.HasMorePages() && len(functions) < maxItems {
  pageOutput, err := paginator.NextPage(context.TODO())
  if err != nil {
   log.Panicf("Couldn't list functions for your account. Here's why: %v\n", err)
  }
  functions = append(functions, pageOutput.Functions...)
 }
 return functions
}



// DeleteFunction deletes the Lambda function specified by functionName.
func (wrapper FunctionWrapper) DeleteFunction(functionName string) {
 _, err := wrapper.LambdaClient.DeleteFunction(context.TODO(),
 &lambda.DeleteFunctionInput{
  FunctionName: aws.String(functionName),
 })
 if err != nil {
  log.Panicf("Couldn't delete function %v. Here's why: %v\n", functionName, err)
 }
}
```

```
// Invoke invokes the Lambda function specified by functionName, passing the
 parameters
// as a JSON payload. When getLog is true, types.LogTypeTail is specified, which
 tells
// Lambda to include the last few log lines in the returned result.
func (wrapper FunctionWrapper) Invoke(functionName string, parameters any, getLog
 bool) *lambda.InvokeOutput {
 logType := types.LogTypeNone
 if getLog {
  logType = types.LogTypeTail
 }
 payload, err := json.Marshal(parameters)
 if err != nil {
  log.Panicf("Couldn't marshal parameters to JSON. Here's why %v\n", err)
 }
 invokeOutput, err := wrapper.LambdaClient.Invoke(context.TODO(),
 &lambda.InvokeInput{
  FunctionName: aws.String(functionName),
  LogType:      logType,
  Payload:      payload,
 })
 if err != nil {
  log.Panicf("Couldn't invoke function %v. Here's why: %v\n", functionName, err)
 }
 return invokeOutput
}



// IncrementParameters is used to serialize parameters to the increment Lambda
 handler.
type IncrementParameters struct {
 Action string `json:"action"`
 Number int    `json:"number"`
}

// CalculatorParameters is used to serialize parameters to the calculator Lambda
 handler.
type CalculatorParameters struct {
 Action string `json:"action"`
 X      int    `json:"x"`
 Y      int    `json:"y"`
```

```
}

// LambdaResultInt is used to deserialize an int result from a Lambda handler.
type LambdaResultInt struct {
 Result int `json:"result"`
}

// LambdaResultFloat is used to deserialize a float32 result from a Lambda
 handler.
type LambdaResultFloat struct {
 Result float32 `json:"result"`
}
```

Erstellen Sie eine Struktur, die Funktionen implementiert, um das Szenario auszuführen.

```
// IScenarioHelper abstracts I/O and wait functions from a scenario so that they
// can be mocked for unit testing.
type IScenarioHelper interface {
 Pause(secs int)
 CreateDeploymentPackage(sourceFile string, destinationFile string) *bytes.Buffer
}

// ScenarioHelper lets the caller specify the path to Lambda handler functions.
type ScenarioHelper struct {
 HandlerPath string
}

// Pause waits for the specified number of seconds.
func (helper *ScenarioHelper) Pause(secs int) {
 time.Sleep(time.Duration(secs) * time.Second)
}

// CreateDeploymentPackage creates an AWS Lambda deployment package from a source
 file. The
// deployment package is stored in .zip format in a bytes.Buffer. The buffer can
 be
// used to pass a []byte to Lambda when creating the function.
// The specified destinationFile is the name to give the file when it's deployed
 to Lambda.
```

```
func (helper *ScenarioHelper) CreateDeploymentPackage(sourceFile string,
 destinationFile string) *bytes.Buffer {
 var err error
 buffer := &bytes.Buffer{}
 writer := zip.NewWriter(buffer)
 zFile, err := writer.Create(destinationFile)
 if err != nil {
  log.Panicf("Couldn't create destination archive %v. Here's why: %v\n",
 destinationFile, err)
 }
 sourceBody, err := os.ReadFile(fmt.Sprintf("%v/%v", helper.HandlerPath,
 sourceFile))
 if err != nil {
  log.Panicf("Couldn't read handler source file %v. Here's why: %v\n",
   sourceFile, err)
 } else {
  _, err = zFile.Write(sourceBody)
  if err != nil {
   log.Panicf("Couldn't write handler %v to zip archive. Here's why: %v\n",
    sourceFile, err)
  }
 }
 err = writer.Close()
 if err != nil {
  log.Panicf("Couldn't close zip writer. Here's why: %v\n", err)
 }
 return buffer
}
```

Definieren Sie einen Lambda-Handler, der eine Zahl inkrementiert.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)


def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
 number,
```

```
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
    result = None
    action = event.get("action")
    if action == "increment":
        result = event.get("number", 0) + 1
        logger.info("Calculated result of %s", result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {"result": result}
    return response
```

Definieren Sie einen zweiten Lambda-Handler, der arithmetische Operationen ausführt.

```
import logging
import os


logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
 function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}


def lambda_handler(event, context):
    """
```

```
    Accepts an action and two numbers, performs the specified action on the
numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
    """
    # Set the log level based on a variable configured in the Lambda environment.
    logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
    logger.debug("Event: %s", event)

    action = event.get("action")
    func = ACTIONS.get(action)
    x = event.get("x")
    y = event.get("y")
    result = None
    try:
        if func is not None and x is not None and y is not None:
            result = func(x, y)
            logger.info("%s %s %s is %s", x, action, y, result)
        else:
            logger.error("I can't calculate %s %s %s.", x, action, y)
    except ZeroDivisionError:
        logger.warning("I can't divide %s by 0!", x)

    response = {"result": result}
    return response
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Go -API-Referenz.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode

- UpdateFunctionKonfiguration

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
/*
 *  Lambda function names appear as:
 *
 *  arn:aws:lambda:us-west-2:335556666777:function:HelloFunction
 *
 *  To find this value, look at the function in the AWS Management Console.
 *
 *  Before running this Java code example, set up your development environment,
 including your credentials.
 *
 *  For more information, see this documentation topic:
 *
 *  https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 *
 *  This example performs the following tasks:
 *
 * 1. Creates an AWS Lambda function.
 * 2. Gets a specific AWS Lambda function.
 * 3. Lists all Lambda functions.
 * 4. Invokes a Lambda function.
 * 5. Updates the Lambda function code and invokes it again.
 * 6. Updates a Lambda function's configuration value.
 * 7. Deletes a Lambda function.
 */

public class LambdaScenario {
    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");
```

```
    public static void main(String[] args) throws InterruptedException {
        final String usage = """

                Usage:
                    <functionName> <filePath> <role> <handler> <bucketName> <key>
\s

                Where:
                    functionName - The name of the Lambda function.\s
                    filePath - The path to the .zip or .jar where the code is
 located.\s
                    role - The AWS Identity and Access Management (IAM) service
 role that has Lambda permissions.\s
                    handler - The fully qualified method name (for example,
 example.Handler::handleRequest).\s
                    bucketName - The Amazon Simple Storage Service (Amazon S3)
 bucket name that contains the .zip or .jar used to update the Lambda function's
 code.\s
                    key - The Amazon S3 key name that represents the .zip or .jar
 (for example, LambdaHello-1.0-SNAPSHOT.jar).
                    """;

        if (args.length != 6) {
            System.out.println(usage);
            System.exit(1);
        }

        String functionName = args[0];
        String filePath = args[1];
        String role = args[2];
        String handler = args[3];
        String bucketName = args[4];
        String key = args[5];

        Region region = Region.US_WEST_2;
        LambdaClient awsLambda = LambdaClient.builder()
                .region(region)
                .build();

        System.out.println(DASHES);
        System.out.println("Welcome to the AWS Lambda example scenario.");
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("1. Create an AWS Lambda function.");
        String funArn = createLambdaFunction(awsLambda, functionName, filePath,
role, handler);
        System.out.println("The AWS Lambda ARN is " + funArn);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get the " + functionName + " AWS Lambda
function.");
        getFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. List all AWS Lambda functions.");
        listFunctions(awsLambda);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("4. Invoke the Lambda function.");
        System.out.println("*** Sleep for 1 min to get Lambda function ready.");
        Thread.sleep(60000);
        invokeFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("5. Update the Lambda function code and invoke it
again.");
        updateFunctionCode(awsLambda, functionName, bucketName, key);
        System.out.println("*** Sleep for 1 min to get Lambda function ready.");
        Thread.sleep(60000);
        invokeFunction(awsLambda, functionName);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("6. Update a Lambda function's configuration value.");
        updateFunctionConfiguration(awsLambda, functionName, handler);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("7. Delete the AWS Lambda function.");
        LambdaScenario.deleteLambdaFunction(awsLambda, functionName);
        System.out.println(DASHES);
```

```
        System.out.println(DASHES);
        System.out.println("The AWS Lambda scenario completed successfully");
        System.out.println(DASHES);
        awsLambda.close();
    }

    public static String createLambdaFunction(LambdaClient awsLambda,
            String functionName,
            String filePath,
            String role,
            String handler) {

        try {
            LambdaWaiter waiter = awsLambda.waiter();
            InputStream is = new FileInputStream(filePath);
            SdkBytes fileToUpload = SdkBytes.fromInputStream(is);

            FunctionCode code = FunctionCode.builder()
                    .zipFile(fileToUpload)
                    .build();

            CreateFunctionRequest functionRequest =
CreateFunctionRequest.builder()
                    .functionName(functionName)
                    .description("Created by the Lambda Java API")
                    .code(code)
                    .handler(handler)
                    .runtime(Runtime.JAVA8)
                    .role(role)
                    .build();

            // Create a Lambda function using a waiter
            CreateFunctionResponse functionResponse =
awsLambda.createFunction(functionRequest);
            GetFunctionRequest getFunctionRequest = GetFunctionRequest.builder()
                    .functionName(functionName)
                    .build();
            WaiterResponse<GetFunctionResponse> waiterResponse =
waiter.waitUntilFunctionExists(getFunctionRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            return functionResponse.functionArn();

        } catch (LambdaException | FileNotFoundException e) {
            System.err.println(e.getMessage());
```

```
            System.exit(1);
        }
        return "";
    }

    public static void getFunction(LambdaClient awsLambda, String functionName) {
        try {
            GetFunctionRequest functionRequest = GetFunctionRequest.builder()
                    .functionName(functionName)
                    .build();

            GetFunctionResponse response =
awsLambda.getFunction(functionRequest);
            System.out.println("The runtime of this Lambda function is " +
response.configuration().runtime());

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void listFunctions(LambdaClient awsLambda) {
        try {
            ListFunctionsResponse functionResult = awsLambda.listFunctions();
            List<FunctionConfiguration> list = functionResult.functions();
            for (FunctionConfiguration config : list) {
                System.out.println("The function name is " +
config.functionName());
            }

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void invokeFunction(LambdaClient awsLambda, String
functionName) {

        InvokeResponse res;
        try {
            // Need a SdkBytes instance for the payload.
            JSONObject jsonObj = new JSONObject();
```

```
            jsonObj.put("inputValue", "2000");
            String json = jsonObj.toString();
            SdkBytes payload = SdkBytes.fromUtf8String(json);

            InvokeRequest request = InvokeRequest.builder()
                    .functionName(functionName)
                    .payload(payload)
                    .build();

            res = awsLambda.invoke(request);
            String value = res.payload().asUtf8String();
            System.out.println(value);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void updateFunctionCode(LambdaClient awsLambda, String
functionName, String bucketName, String key) {
        try {
            LambdaWaiter waiter = awsLambda.waiter();
            UpdateFunctionCodeRequest functionCodeRequest =
UpdateFunctionCodeRequest.builder()
                    .functionName(functionName)
                    .publish(true)
                    .s3Bucket(bucketName)
                    .s3Key(key)
                    .build();

            UpdateFunctionCodeResponse response =
awsLambda.updateFunctionCode(functionCodeRequest);
            GetFunctionConfigurationRequest getFunctionConfigRequest =
GetFunctionConfigurationRequest.builder()
                    .functionName(functionName)
                    .build();

            WaiterResponse<GetFunctionConfigurationResponse> waiterResponse =
waiter
                    .waitUntilFunctionUpdated(getFunctionConfigRequest);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println("The last modified value is " +
response.lastModified());
```

```
        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void updateFunctionConfiguration(LambdaClient awsLambda, String
 functionName, String handler) {
        try {
            UpdateFunctionConfigurationRequest configurationRequest =
 UpdateFunctionConfigurationRequest.builder()
                    .functionName(functionName)
                    .handler(handler)
                    .runtime(Runtime.JAVA11)
                    .build();

            awsLambda.updateFunctionConfiguration(configurationRequest);

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void deleteLambdaFunction(LambdaClient awsLambda, String
 functionName) {
        try {
            DeleteFunctionRequest request = DeleteFunctionRequest.builder()
                    .functionName(functionName)
                    .build();

            awsLambda.deleteFunction(request);
            System.out.println("The " + functionName + " function was deleted");

        } catch (LambdaException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Java 2.x -API-Referenz.

- CreateFunction
- DeleteFunction
- GetFunction
- Aufrufen
- ListFunctions
- UpdateFunctionKode
- UpdateFunctionKonfiguration

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle, die Lambda die Berechtigung erteilt, in Protokolle zu schreiben.

```
    log(`Creating role (${NAME_ROLE_LAMBDA})...`);
    const response = await createRole(NAME_ROLE_LAMBDA);

import { AttachRolePolicyCommand, IAMClient } from "@aws-sdk/client-iam";

const client = new IAMClient({});

/**
 *
 * @param {string} policyArn
 * @param {string} roleName
 */
export const attachRolePolicy = (policyArn, roleName) => {
  const command = new AttachRolePolicyCommand({
    PolicyArn: policyArn,
    RoleName: roleName,
  });
```

```
  return client.send(command);
};
```

Erstellen Sie eine Lambda-Funktion und laden Sie Handlercode hoch.

```
const createFunction = async (funcName, roleArn) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${funcName}.zip`);

  const command = new CreateFunctionCommand({
    Code: { ZipFile: code },
    FunctionName: funcName,
    Role: roleArn,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};
```

Rufen Sie die Funktion mit einem einzigen Parameter auf und erhalten Sie Ergebnisse.

```
const invoke = async (funcName, payload) => {
  const client = new LambdaClient({});
  const command = new InvokeCommand({
    FunctionName: funcName,
    Payload: JSON.stringify(payload),
    LogType: LogType.Tail,
  });

  const { Payload, LogResult } = await client.send(command);
  const result = Buffer.from(Payload).toString();
  const logs = Buffer.from(LogResult, "base64").toString();
  return { logs, result };
};
```

Aktualisieren Sie den Funktionscode und konfigurieren Sie seine Lambda-Umgebung mit einer Umgebungsvariablen.

```
const updateFunctionCode = async (funcName, newFunc) => {
  const client = new LambdaClient({});
  const code = await readFile(`${dirname}../functions/${newFunc}.zip`);
  const command = new UpdateFunctionCodeCommand({
    ZipFile: code,
    FunctionName: funcName,
    Architectures: [Architecture.arm64],
    Handler: "index.handler", // Required when sending a .zip file
    PackageType: PackageType.Zip, // Required when sending a .zip file
    Runtime: Runtime.nodejs16x, // Required when sending a .zip file
  });

  return client.send(command);
};

const updateFunctionConfiguration = (funcName) => {
  const client = new LambdaClient({});
  const config = readFileSync(`${dirname}../functions/config.json`).toString();
  const command = new UpdateFunctionConfigurationCommand({
    ...JSON.parse(config),
    FunctionName: funcName,
  });
  return client.send(command);
};
```

Listen Sie die Funktionen für Ihr Konto auf.

```
const listFunctions = () => {
  const client = new LambdaClient({});
  const command = new ListFunctionsCommand({});

  return client.send(command);
};
```

Löschen Sie die IAM-Rolle für Ihre Lambda-Funktion.

```
import { DeleteRoleCommand, IAMClient } from "@aws-sdk/client-iam";
```

```
const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const deleteRole = (roleName) => {
  const command = new DeleteRoleCommand({ RoleName: roleName });
  return client.send(command);
};

/**
 * @param {string} funcName
 */
const deleteFunction = (funcName) => {
  const client = new LambdaClient({});
  const command = new DeleteFunctionCommand({ FunctionName: funcName });
  return client.send(command);
};
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for JavaScript -API-Referenz.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

Kotlin

SDK für Kotlin

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
suspend fun main(args: Array<String>) {
    val usage = """
        Usage:
            <functionName> <role> <handler> <bucketName> <updatedBucketName>
 <key>

        Where:
            functionName - The name of the AWS Lambda function.
            role - The AWS Identity and Access Management (IAM) service role that
 has AWS Lambda permissions.
            handler - The fully qualified method name (for example,
 example.Handler::handleRequest).
            bucketName - The Amazon Simple Storage Service (Amazon S3) bucket
 name that contains the ZIP or JAR used for the Lambda function's code.
            updatedBucketName - The Amazon S3 bucket name that contains the .zip
 or .jar used to update the Lambda function's code.
            key - The Amazon S3 key name that represents the .zip or .jar file
 (for example, LambdaHello-1.0-SNAPSHOT.jar).
            """

    if (args.size != 6) {
        println(usage)
        exitProcess(1)
    }

    val functionName = args[0]
    val role = args[1]
    val handler = args[2]
    val bucketName = args[3]
    val updatedBucketName = args[4]
    val key = args[5]
```

```
    println("Creating a Lambda function named $functionName.")
    val funArn = createScFunction(functionName, bucketName, key, handler, role)
    println("The AWS Lambda ARN is $funArn")

    // Get a specific Lambda function.
    println("Getting the $functionName AWS Lambda function.")
    getFunction(functionName)

    // List the Lambda functions.
    println("Listing all AWS Lambda functions.")
    listFunctionsSc()

    // Invoke the Lambda function.
    println("*** Invoke the Lambda function.")
    invokeFunctionSc(functionName)

    // Update the AWS Lambda function code.
    println("*** Update the Lambda function code.")
    updateFunctionCode(functionName, updatedBucketName, key)

    // println("*** Invoke the function again after updating the code.")
    invokeFunctionSc(functionName)

    // Update the AWS Lambda function configuration.
    println("Update the run time of the function.")
    updateFunctionConfiguration(functionName, handler)

    // Delete the AWS Lambda function.
    println("Delete the AWS Lambda function.")
    delFunction(functionName)
}

suspend fun createScFunction(
    myFunctionName: String,
    s3BucketName: String,
    myS3Key: String,
    myHandler: String,
    myRole: String
): String {
    val functionCode =
        FunctionCode {
            s3Bucket = s3BucketName
            s3Key = myS3Key
        }
```

```
    val request =
        CreateFunctionRequest {
            functionName = myFunctionName
            code = functionCode
            description = "Created by the Lambda Kotlin API"
            handler = myHandler
            role = myRole
            runtime = Runtime.Java8
        }

    // Create a Lambda function using a waiter
    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val functionResponse = awsLambda.createFunction(request)
        awsLambda.waitUntilFunctionActive {
            functionName = myFunctionName
        }
        return functionResponse.functionArn.toString()
    }
}

suspend fun getFunction(functionNameVal: String) {
    val functionRequest =
        GetFunctionRequest {
            functionName = functionNameVal
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val response = awsLambda.getFunction(functionRequest)
        println("The runtime of this Lambda function is
 ${response.configuration?.runtime}")
    }
}

suspend fun listFunctionsSc() {
    val request =
        ListFunctionsRequest {
            maxItems = 10
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val response = awsLambda.listFunctions(request)
        response.functions?.forEach { function ->
            println("The function name is ${function.functionName}")
```

```
        }
    }
}

suspend fun invokeFunctionSc(functionNameVal: String) {
    val json = """{"inputValue":"1000"}"""
    val byteArray = json.trimIndent().encodeToByteArray()
    val request =
        InvokeRequest {
            functionName = functionNameVal
            payload = byteArray
            logType = LogType.Tail
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val res = awsLambda.invoke(request)
        println("The function payload is
 ${res.payload?.toString(Charsets.UTF_8)}")
    }
}

suspend fun updateFunctionCode(
    functionNameVal: String?,
    bucketName: String?,
    key: String?
) {
    val functionCodeRequest =
        UpdateFunctionCodeRequest {
            functionName = functionNameVal
            publish = true
            s3Bucket = bucketName
            s3Key = key
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        val response = awsLambda.updateFunctionCode(functionCodeRequest)
        awsLambda.waitUntilFunctionUpdated {
            functionName = functionNameVal
        }
        println("The last modified value is " + response.lastModified)
    }
}

suspend fun updateFunctionConfiguration(
```

```
    functionNameVal: String?,
    handlerVal: String?
) {
    val configurationRequest =
        UpdateFunctionConfigurationRequest {
            functionName = functionNameVal
            handler = handlerVal
            runtime = Runtime.Java11
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        awsLambda.updateFunctionConfiguration(configurationRequest)
    }
}

suspend fun delFunction(myFunctionName: String) {
    val request =
        DeleteFunctionRequest {
            functionName = myFunctionName
        }

    LambdaClient { region = "us-west-2" }.use { awsLambda ->
        awsLambda.deleteFunction(request)
        println("$myFunctionName was deleted")
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Kotlin.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
namespace Lambda;

use Aws\S3\S3Client;
use GuzzleHttp\Psr7\Stream;
use Iam\IAMService;

class GettingStartedWithLambda
{
    public function run()
    {
        echo("\n");
        echo("---------------------------------------\n");
        print("Welcome to the AWS Lambda getting started demo using PHP!\n");
        echo("---------------------------------------\n");

        $clientArgs = [
            'region' => 'us-west-2',
            'version' => 'latest',
            'profile' => 'default',
        ];
        $uniqid = uniqid();

        $iamService = new IAMService();
        $s3client = new S3Client($clientArgs);
        $lambdaService = new LambdaService();

        echo "First, let's create a role to run our Lambda code.\n";
        $roleName = "test-lambda-role-$uniqid";
        $rolePolicyDocument = "{
            \"Version\": \"2012-10-17\",
            \"Statement\": [
                {
```

```
                    \"Effect\": \"Allow\",
                    \"Principal\": {
                        \"Service\": \"lambda.amazonaws.com\"
                    },
                    \"Action\": \"sts:AssumeRole\"
                }
            ]
        }";
        $role = $iamService->createRole($roleName, $rolePolicyDocument);
        echo "Created role {$role['RoleName']}.\n";

        $iamService->attachRolePolicy(
            $role['RoleName'],
            "arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole"
        );
        echo "Attached the AWSLambdaBasicExecutionRole to {$role['RoleName']}.
\n";

        echo "\nNow let's create an S3 bucket and upload our Lambda code there.
\n";
        $bucketName = "test-example-bucket-$uniqid";
        $s3client->createBucket([
            'Bucket' => $bucketName,
        ]);
        echo "Created bucket $bucketName.\n";

        $functionName = "doc_example_lambda_$uniqid";
        $codeBasic = __DIR__ . "/lambda_handler_basic.zip";
        $handler = "lambda_handler_basic";
        $file = file_get_contents($codeBasic);
        $s3client->putObject([
            'Bucket' => $bucketName,
            'Key' => $functionName,
            'Body' => $file,
        ]);
        echo "Uploaded the Lambda code.\n";

        $createLambdaFunction = $lambdaService->createFunction($functionName,
 $role, $bucketName, $handler);
        // Wait until the function has finished being created.
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['State'] == "Pending");
```

```
        echo "Created Lambda function {$getLambdaFunction['Configuration']
['FunctionName']}.\n";

        sleep(1);

        echo "\nOk, let's invoke that Lambda code.\n";
        $basicParams = [
            'action' => 'increment',
            'number' => 3,
        ];
        /** @var Stream $invokeFunction */
        $invokeFunction = $lambdaService->invoke($functionName, $basicParams)
['Payload'];
        $result = json_decode($invokeFunction->getContents())->result;
        echo "After invoking the Lambda code with the input of
 {$basicParams['number']} we received $result.\n";

        echo "\nSince that's working, let's update the Lambda code.\n";
        $codeCalculator = "lambda_handler_calculator.zip";
        $handlerCalculator = "lambda_handler_calculator";
        echo "First, put the new code into the S3 bucket.\n";
        $file = file_get_contents($codeCalculator);
        $s3client->putObject([
            'Bucket' => $bucketName,
            'Key' => $functionName,
            'Body' => $file,
        ]);
        echo "New code uploaded.\n";

        $lambdaService->updateFunctionCode($functionName, $bucketName,
 $functionName);
        // Wait for the Lambda code to finish updating.
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
 "Successful");
        echo "New Lambda code uploaded.\n";

        $environment = [
            'Variable' => ['Variables' => ['LOG_LEVEL' => 'DEBUG']],
        ];
        $lambdaService->updateFunctionConfiguration($functionName,
 $handlerCalculator, $environment);
```

```
        do {
            $getLambdaFunction = $lambdaService-
>getFunction($createLambdaFunction['FunctionName']);
        } while ($getLambdaFunction['Configuration']['LastUpdateStatus'] !==
 "Successful");
        echo "Lambda code updated with new handler and a LOG_LEVEL of DEBUG for
 more information.\n";

        echo "Invoke the new code with some new data.\n";
        $calculatorParams = [
            'action' => 'plus',
            'x' => 5,
            'y' => 4,
        ];
        $invokeFunction = $lambdaService->invoke($functionName,
 $calculatorParams, "Tail");
        $result = json_decode($invokeFunction['Payload']->getContents())->result;
        echo "Indeed, {$calculatorParams['x']} + {$calculatorParams['y']} does
 equal $result.\n";
        echo "Here's the extra debug info: ";
        echo base64_decode($invokeFunction['LogResult']) . "\n";

        echo "\nBut what happens if you try to divide by zero?\n";
        $divZeroParams = [
            'action' => 'divide',
            'x' => 5,
            'y' => 0,
        ];
        $invokeFunction = $lambdaService->invoke($functionName, $divZeroParams,
 "Tail");
        $result = json_decode($invokeFunction['Payload']->getContents())->result;
        echo "You get a |$result| result.\n";
        echo "And an error message: ";
        echo base64_decode($invokeFunction['LogResult']) . "\n";

        echo "\nHere's all the Lambda functions you have in this Region:\n";
        $listLambdaFunctions = $lambdaService->listFunctions(5);
        $allLambdaFunctions = $listLambdaFunctions['Functions'];
        $next = $listLambdaFunctions->get('NextMarker');
        while ($next != false) {
            $listLambdaFunctions = $lambdaService->listFunctions(5, $next);
            $next = $listLambdaFunctions->get('NextMarker');
            $allLambdaFunctions = array_merge($allLambdaFunctions,
 $listLambdaFunctions['Functions']);
```

```
        }
        foreach ($allLambdaFunctions as $function) {
            echo "{$function['FunctionName']}\n";
        }

        echo "\n\nAnd don't forget to clean up your data!\n";

        $lambdaService->deleteFunction($functionName);
        echo "Deleted Lambda function.\n";
        $iamService->deleteRole($role['RoleName']);
        echo "Deleted Role.\n";
        $deleteObjects = $s3client->listObjectsV2([
            'Bucket' => $bucketName,
        ]);
        $deleteObjects = $s3client->deleteObjects([
            'Bucket' => $bucketName,
            'Delete' => [
                'Objects' => $deleteObjects['Contents'],
            ]
        ]);
        echo "Deleted all objects from the S3 bucket.\n";
        $s3client->deleteBucket(['Bucket' => $bucketName]);
        echo "Deleted the bucket.\n";
    }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for PHP -API-Referenz.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Definieren Sie einen Lambda-Handler, der eine Zahl inkrementiert.

```
import logging

logger = logging.getLogger()
logger.setLevel(logging.INFO)


def lambda_handler(event, context):
    """
    Accepts an action and a single number, performs the specified action on the
 number,
    and returns the result. The only allowable action is 'increment'.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the action.
    """
    result = None
    action = event.get("action")
    if action == "increment":
        result = event.get("number", 0) + 1
        logger.info("Calculated result of %s", result)
    else:
        logger.error("%s is not a valid action.", action)

    response = {"result": result}
    return response
```

Definieren Sie einen zweiten Lambda-Handler, der arithmetische Operationen ausführt.

```
import logging
import os


logger = logging.getLogger()

# Define a list of Python lambda functions that are called by this AWS Lambda
 function.
ACTIONS = {
    "plus": lambda x, y: x + y,
    "minus": lambda x, y: x - y,
    "times": lambda x, y: x * y,
    "divided-by": lambda x, y: x / y,
}


def lambda_handler(event, context):
    """
    Accepts an action and two numbers, performs the specified action on the
 numbers,
    and returns the result.

    :param event: The event dict that contains the parameters sent when the
 function
                  is invoked.
    :param context: The context in which the function is called.
    :return: The result of the specified action.
    """
    # Set the log level based on a variable configured in the Lambda environment.
    logger.setLevel(os.environ.get("LOG_LEVEL", logging.INFO))
    logger.debug("Event: %s", event)

    action = event.get("action")
    func = ACTIONS.get(action)
    x = event.get("x")
    y = event.get("y")
    result = None
    try:
        if func is not None and x is not None and y is not None:
```

```
            result = func(x, y)
            logger.info("%s %s %s is %s", x, action, y, result)
        else:
            logger.error("I can't calculate %s %s %s.", x, action, y)
    except ZeroDivisionError:
        logger.warning("I can't divide %s by 0!", x)

    response = {"result": result}
    return response
```

Erstellen Sie Funktionen, die Lambda-Aktionen umschließen.

```
class LambdaWrapper:
    def __init__(self, lambda_client, iam_resource):
        self.lambda_client = lambda_client
        self.iam_resource = iam_resource


    @staticmethod
    def create_deployment_package(source_file, destination_file):
        """
        Creates a Lambda deployment package in .zip format in an in-memory
 buffer. This
        buffer can be passed directly to Lambda when creating the function.

        :param source_file: The name of the file that contains the Lambda handler
                            function.
        :param destination_file: The name to give the file when it's deployed to
 Lambda.
        :return: The deployment package.
        """
        buffer = io.BytesIO()
        with zipfile.ZipFile(buffer, "w") as zipped:
            zipped.write(source_file, destination_file)
        buffer.seek(0)
        return buffer.read()

    def get_iam_role(self, iam_role_name):
        """
        Get an AWS Identity and Access Management (IAM) role.
```

```
        :param iam_role_name: The name of the role to retrieve.
        :return: The IAM role.
        """
        role = None
        try:
            temp_role = self.iam_resource.Role(iam_role_name)
            temp_role.load()
            role = temp_role
            logger.info("Got IAM role %s", role.name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "NoSuchEntity":
                logger.info("IAM role %s does not exist.", iam_role_name)
            else:
                logger.error(
                    "Couldn't get IAM role %s. Here's why: %s: %s",
                    iam_role_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        return role

    def create_iam_role_for_lambda(self, iam_role_name):
        """
        Creates an IAM role that grants the Lambda function basic permissions. If
a
        role with the specified name already exists, it is used for the demo.

        :param iam_role_name: The name of the role to create.
        :return: The role and a value that indicates whether the role is newly
created.
        """
        role = self.get_iam_role(iam_role_name)
        if role is not None:
            return role, False

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

```
                }
            ],
        }
        policy_arn = "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole"

        try:
            role = self.iam_resource.create_role(
                RoleName=iam_role_name,
                AssumeRolePolicyDocument=json.dumps(lambda_assume_role_policy),
            )
            logger.info("Created role %s.", role.name)
            role.attach_policy(PolicyArn=policy_arn)
            logger.info("Attached basic execution policy to role %s.", role.name)
        except ClientError as error:
            if error.response["Error"]["Code"] == "EntityAlreadyExists":
                role = self.iam_resource.Role(iam_role_name)
                logger.warning("The role %s already exists. Using it.",
 iam_role_name)
            else:
                logger.exception(
                    "Couldn't create role %s or attach policy %s.",
                    iam_role_name,
                    policy_arn,
                )
                raise

        return role, True

    def get_function(self, function_name):
        """
        Gets data about a Lambda function.

        :param function_name: The name of the function.
        :return: The function data.
        """
        response = None
        try:
            response =
 self.lambda_client.get_function(FunctionName=function_name)
        except ClientError as err:
            if err.response["Error"]["Code"] == "ResourceNotFoundException":
                logger.info("Function %s does not exist.", function_name)
            else:
```

```
                logger.error(
                    "Couldn't get function %s. Here's why: %s: %s",
                    function_name,
                    err.response["Error"]["Code"],
                    err.response["Error"]["Message"],
                )
                raise
        return response


    def create_function(
        self, function_name, handler_name, iam_role, deployment_package
    ):
        """
        Deploys a Lambda function.

        :param function_name: The name of the Lambda function.
        :param handler_name: The fully qualified name of the handler function.
This
                             must include the file name and the function name.
        :param iam_role: The IAM role to use for the function.
        :param deployment_package: The deployment package that contains the
function
                                   code in .zip format.
        :return: The Amazon Resource Name (ARN) of the newly created function.
        """
        try:
            response = self.lambda_client.create_function(
                FunctionName=function_name,
                Description="AWS Lambda doc example",
                Runtime="python3.8",
                Role=iam_role.arn,
                Handler=handler_name,
                Code={"ZipFile": deployment_package},
                Publish=True,
            )
            function_arn = response["FunctionArn"]
            waiter = self.lambda_client.get_waiter("function_active_v2")
            waiter.wait(FunctionName=function_name)
            logger.info(
                "Created function '%s' with ARN: '%s'.",
                function_name,
                response["FunctionArn"],
            )
```

```
        except ClientError:
            logger.error("Couldn't create function %s.", function_name)
            raise
        else:
            return function_arn


    def delete_function(self, function_name):
        """
        Deletes a Lambda function.

        :param function_name: The name of the function to delete.
        """
        try:
            self.lambda_client.delete_function(FunctionName=function_name)
        except ClientError:
            logger.exception("Couldn't delete function %s.", function_name)
            raise


    def invoke_function(self, function_name, function_params, get_log=False):
        """
        Invokes a Lambda function.

        :param function_name: The name of the function to invoke.
        :param function_params: The parameters of the function as a dict. This
dict
                                is serialized to JSON before it is sent to
Lambda.
        :param get_log: When true, the last 4 KB of the execution log are
included in
                        the response.
        :return: The response from the function invocation.
        """
        try:
            response = self.lambda_client.invoke(
                FunctionName=function_name,
                Payload=json.dumps(function_params),
                LogType="Tail" if get_log else "None",
            )
            logger.info("Invoked function %s.", function_name)
        except ClientError:
            logger.exception("Couldn't invoke function %s.", function_name)
            raise
```

```
        return response


    def update_function_code(self, function_name, deployment_package):
        """
        Updates the code for a Lambda function by submitting a .zip archive that
contains
        the code for the function.

        :param function_name: The name of the function to update.
        :param deployment_package: The function code to update, packaged as bytes
in
                                   .zip format.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_code(
                FunctionName=function_name, ZipFile=deployment_package
            )
        except ClientError as err:
            logger.error(
                "Couldn't update function %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def update_function_configuration(self, function_name, env_vars):
        """
        Updates the environment variables for a Lambda function.

        :param function_name: The name of the function to update.
        :param env_vars: A dict of environment variables to update.
        :return: Data about the update, including the status.
        """
        try:
            response = self.lambda_client.update_function_configuration(
                FunctionName=function_name, Environment={"Variables": env_vars}
            )
        except ClientError as err:
```

```
            logger.error(
                "Couldn't update function configuration %s. Here's why: %s: %s",
                function_name,
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
        else:
            return response


    def list_functions(self):
        """
        Lists the Lambda functions for the current account.
        """
        try:
            func_paginator = self.lambda_client.get_paginator("list_functions")
            for func_page in func_paginator.paginate():
                for func in func_page["Functions"]:
                    print(func["FunctionName"])
                    desc = func.get("Description")
                    if desc:
                        print(f"\t{desc}")
                    print(f"\t{func['Runtime']}: {func['Handler']}")
        except ClientError as err:
            logger.error(
                "Couldn't list functions. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Erstellen Sie eine Funktion, die das Szenario ausführt.

```
class UpdateFunctionWaiter(CustomWaiter):
    """A custom waiter that waits until a function is successfully updated."""

    def __init__(self, client):
        super().__init__(
```

```
            "UpdateSuccess",
            "GetFunction",
            "Configuration.LastUpdateStatus",
            {"Successful": WaitState.SUCCESS, "Failed": WaitState.FAILURE},
            client,
        )

    def wait(self, function_name):
        self._wait(FunctionName=function_name)


def run_scenario(lambda_client, iam_resource, basic_file, calculator_file,
 lambda_name):
    """
    Runs the scenario.

    :param lambda_client: A Boto3 Lambda client.
    :param iam_resource: A Boto3 IAM resource.
    :param basic_file: The name of the file that contains the basic Lambda
 handler.
    :param calculator_file: The name of the file that contains the calculator
 Lambda handler.
    :param lambda_name: The name to give resources created for the scenario, such
 as the
                        IAM role and the Lambda function.
    """
    logging.basicConfig(level=logging.INFO, format="%(levelname)s: %(message)s")

    print("-" * 88)
    print("Welcome to the AWS Lambda getting started with functions demo.")
    print("-" * 88)

    wrapper = LambdaWrapper(lambda_client, iam_resource)

    print("Checking for IAM role for Lambda...")
    iam_role, should_wait = wrapper.create_iam_role_for_lambda(lambda_name)
    if should_wait:
        logger.info("Giving AWS time to create resources...")
        wait(10)

    print(f"Looking for function {lambda_name}...")
    function = wrapper.get_function(lambda_name)
    if function is None:
        print("Zipping the Python script into a deployment package...")
```

```
        deployment_package = wrapper.create_deployment_package(
            basic_file, f"{lambda_name}.py"
        )
        print(f"...and creating the {lambda_name} Lambda function.")
        wrapper.create_function(
            lambda_name, f"{lambda_name}.lambda_handler", iam_role,
deployment_package
        )
    else:
        print(f"Function {lambda_name} already exists.")
    print("-" * 88)

    print(f"Let's invoke {lambda_name}. This function increments a number.")
    action_params = {
        "action": "increment",
        "number": q.ask("Give me a number to increment: ", q.is_int),
    }
    print(f"Invoking {lambda_name}...")
    response = wrapper.invoke_function(lambda_name, action_params)
    print(
        f"Incrementing {action_params['number']} resulted in "
        f"{json.load(response['Payload'])}"
    )
    print("-" * 88)

    print(f"Let's update the function to an arithmetic calculator.")
    q.ask("Press Enter when you're ready.")
    print("Creating a new deployment package...")
    deployment_package = wrapper.create_deployment_package(
        calculator_file, f"{lambda_name}.py"
    )
    print(f"...and updating the {lambda_name} Lambda function.")
    update_waiter = UpdateFunctionWaiter(lambda_client)
    wrapper.update_function_code(lambda_name, deployment_package)
    update_waiter.wait(lambda_name)
    print(f"This function uses an environment variable to control logging
level.")
    print(f"Let's set it to DEBUG to get the most logging.")
    wrapper.update_function_configuration(
        lambda_name, {"LOG_LEVEL": logging.getLevelName(logging.DEBUG)}
    )

    actions = ["plus", "minus", "times", "divided-by"]
    want_invoke = True
```

```
    while want_invoke:
        print(f"Let's invoke {lambda_name}. You can invoke these actions:")
        for index, action in enumerate(actions):
            print(f"{index + 1}: {action}")
        action_params = {}
        action_index = q.ask(
            "Enter the number of the action you want to take: ",
            q.is_int,
            q.in_range(1, len(actions)),
        )
        action_params["action"] = actions[action_index - 1]
        print(f"You've chosen to invoke 'x {action_params['action']} y'.")
        action_params["x"] = q.ask("Enter a value for x: ", q.is_int)
        action_params["y"] = q.ask("Enter a value for y: ", q.is_int)
        print(f"Invoking {lambda_name}...")
        response = wrapper.invoke_function(lambda_name, action_params, True)
        print(
            f"Calculating {action_params['x']} {action_params['action']}
{action_params['y']} "
            f"resulted in {json.load(response['Payload'])}"
        )
        q.ask("Press Enter to see the logs from the call.")
        print(base64.b64decode(response["LogResult"]).decode())
        want_invoke = q.ask("That was fun. Shall we do it again? (y/n) ",
q.is_yesno)
    print("-" * 88)

    if q.ask(
        "Do you want to list all of the functions in your account? (y/n) ",
q.is_yesno
    ):
        wrapper.list_functions()
    print("-" * 88)

    if q.ask("Ready to delete the function and role? (y/n) ", q.is_yesno):
        for policy in iam_role.attached_policies.all():
            policy.detach_role(RoleName=iam_role.name)
        iam_role.delete()
        print(f"Deleted role {lambda_name}.")
        wrapper.delete_function(lambda_name)
        print(f"Deleted function {lambda_name}.")

    print("\nThanks for watching!")
    print("-" * 88)
```

```
if __name__ == "__main__":
    try:
        run_scenario(
            boto3.client("lambda"),
            boto3.resource("iam"),
            "lambda_handler_basic.py",
            "lambda_handler_calculator.py",
            "doc_example_lambda_calculator",
        )
    except Exception:
        logging.exception("Something went wrong with the demo!")
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS -SDK für Python (Boto3).
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Richten Sie die erforderlichen IAM-Berechtigungen für eine Lambda-Funktion ein, die Protokolle schreiben kann.

```
  # Get an AWS Identity and Access Management (IAM) role.
  #
  # @param iam_role_name: The name of the role to retrieve.
  # @param action: Whether to create or destroy the IAM apparatus.
  # @return: The IAM role.
  def manage_iam(iam_role_name, action)
    role_policy = {
      'Version': "2012-10-17",
      'Statement': [
        {
          'Effect': "Allow",
          'Principal': {
            'Service': "lambda.amazonaws.com"
          },
          'Action': "sts:AssumeRole"
        }
      ]
    }
    case action
    when "create"
      role = $iam_client.create_role(
        role_name: iam_role_name,
        assume_role_policy_document: role_policy.to_json
      )
      $iam_client.attach_role_policy(
        {
          policy_arn: "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole",
          role_name: iam_role_name
        }
      )
      $iam_client.wait_until(:role_exists, { role_name: iam_role_name }) do |w|
        w.max_attempts = 5
        w.delay = 5
      end
      @logger.debug("Successfully created IAM role: #{role['role']['arn']}")
      @logger.debug("Enforcing a 10-second sleep to allow IAM role to activate
 fully.")
      sleep(10)
      return role, role_policy.to_json
    when "destroy"
      $iam_client.detach_role_policy(
        {
```

```
          policy_arn: "arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole",
          role_name: iam_role_name
        }
      )
      $iam_client.delete_role(
        role_name: iam_role_name
      )
      @logger.debug("Detached policy & deleted IAM role: #{iam_role_name}")
    else
      raise "Incorrect action provided. Must provide 'create' or 'destroy'"
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error creating role or attaching policy:\n
 #{e.message}")
  end
```

Definieren Sie einen Lambda-Handler, der eine als Aufrufparameter bereitgestellte Zahl inkrementiert.

```
require "logger"

# A function that increments a whole number by one (1) and logs the result.
# Requires a manually-provided runtime parameter, 'number', which must be Int
#
# @param event [Hash] Parameters sent when the function is invoked
# @param context [Hash] Methods and properties that provide information
# about the invocation, function, and execution environment.
# @return incremented_number [String] The incremented number.
def lambda_handler(event:, context:)
  logger = Logger.new($stdout)
  log_level = ENV["LOG_LEVEL"]
  logger.level = case log_level
                 when "debug"
                   Logger::DEBUG
                 when "info"
                   Logger::INFO
                 else
                   Logger::ERROR
                 end
  logger.debug("This is a debug log message.")
  logger.info("This is an info log message. Code executed successfully!")
```

```
  number = event["number"].to_i
  incremented_number = number + 1
  logger.info("You provided #{number.round} and it was incremented to
 #{incremented_number.round}")
  incremented_number.round.to_s
end
```

Komprimieren (ZIP) Sie Ihre Lambda-Funktion in ein Bereitstellungspaket.

```
  # Creates a Lambda deployment package in .zip format.
  # This zip can be passed directly as a string to Lambda when creating the
 function.
  #
  # @param source_file: The name of the object, without suffix, for the Lambda
 file and zip.
  # @return: The deployment package.
  def create_deployment_package(source_file)
    Dir.chdir(File.dirname(__FILE__))
    if File.exist?("lambda_function.zip")
      File.delete("lambda_function.zip")
      @logger.debug("Deleting old zip: lambda_function.zip")
    end
    Zip::File.open("lambda_function.zip", create: true) {
      |zipfile|
      zipfile.add("lambda_function.rb", "#{source_file}.rb")
    }
    @logger.debug("Zipping #{source_file}.rb into: lambda_function.zip.")
    File.read("lambda_function.zip").to_s
  rescue StandardError => e
    @logger.error("There was an error creating deployment package:\n
 #{e.message}")
  end
```

Erstellen Sie eine neue Lambda-Funktion.

```
  # Deploys a Lambda function.
  #
  # @param function_name: The name of the Lambda function.
  # @param handler_name: The fully qualified name of the handler function. This
  #                      must include the file name and the function name.
  # @param role_arn: The IAM role to use for the function.
```

```
  # @param deployment_package: The deployment package that contains the function
  #                            code in .zip format.
  # @return: The Amazon Resource Name (ARN) of the newly created function.
  def create_function(function_name, handler_name, role_arn, deployment_package)
    response = @lambda_client.create_function({
                                                role: role_arn.to_s,
                                                function_name: function_name,
                                                handler: handler_name,
                                                runtime: "ruby2.7",
                                                code: {
                                                  zip_file: deployment_package
                                                },
                                                environment: {
                                                  variables: {
                                                    "LOG_LEVEL" => "info"
                                                  }
                                                }
                                              })
    @lambda_client.wait_until(:function_active_v2, { function_name:
function_name}) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
    response
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error creating #{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

Rufen Sie Ihre Lambda-Funktion mit optionalen Laufzeitparametern auf.

```
  # Invokes a Lambda function.
  # @param function_name [String] The name of the function to invoke.
  # @param payload [nil] Payload containing runtime parameters.
  # @return [Object] The response from the function invocation.
  def invoke_function(function_name, payload = nil)
    params = { function_name: function_name}
    params[:payload] = payload unless payload.nil?
    @lambda_client.invoke(params)
  rescue Aws::Lambda::Errors::ServiceException => e
```

```
    @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
  end
```

Aktualisieren Sie die Konfiguration Ihrer Lambda-Funktion, um eine neue Umgebungsvariable einzufügen.

```
  # Updates the environment variables for a Lambda function.
  # @param function_name: The name of the function to update.
  # @param log_level: The log level of the function.
  # @return: Data about the update, including the status.
  def update_function_configuration(function_name, log_level)
    @lambda_client.update_function_configuration({
                                                   function_name: function_name,
                                                   environment: {
                                                     variables: {
                                                       "LOG_LEVEL" => log_level
                                                     }
                                                   }
                                                 })
    @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
      w.max_attempts = 5
      w.delay = 5
    end
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error updating configurations for
#{function_name}:\n #{e.message}")
  rescue Aws::Waiters::Errors::WaiterFailed => e
    @logger.error("Failed waiting for #{function_name} to activate:\n
#{e.message}")
  end
```

Aktualisieren Sie den Code Ihrer Lambda-Funktion mit einem anderen Bereitstellungspaket, das anderen Code enthält.

```
  # Updates the code for a Lambda function by submitting a .zip archive that
contains
  # the code for the function.

  # @param function_name: The name of the function to update.
```

```
 # @param deployment_package: The function code to update, packaged as bytes in
 #                            .zip format.
 # @return: Data about the update, including the status.
 def update_function_code(function_name, deployment_package)
   @lambda_client.update_function_code(
     function_name: function_name,
     zip_file: deployment_package
   )
   @lambda_client.wait_until(:function_updated_v2, { function_name:
function_name}) do |w|
     w.max_attempts = 5
     w.delay = 5
   end
 rescue Aws::Lambda::Errors::ServiceException => e
   @logger.error("There was an error updating function code for:
#{function_name}:\n #{e.message}")
   nil
 rescue Aws::Waiters::Errors::WaiterFailed => e
   @logger.error("Failed waiting for #{function_name} to update:\n
#{e.message}")
 end
```

Listen Sie alle vorhandenen Lambda-Funktionen mithilfe des eingebauten Paginators auf.

```
 # Lists the Lambda functions for the current account.
 def list_functions
   functions = []
   @lambda_client.list_functions.each do |response|
     response["functions"].each do |function|
       functions.append(function["function_name"])
     end
   end
   functions
 rescue Aws::Lambda::Errors::ServiceException => e
   @logger.error("There was an error executing #{function_name}:\n
#{e.message}")
 end
```

Löschen Sie eine bestimmte Lambda-Funktion.

```
 # Deletes a Lambda function.
```

```
  # @param function_name: The name of the function to delete.
  def delete_function(function_name)
    print "Deleting function: #{function_name}..."
    @lambda_client.delete_function(
      function_name: function_name
    )
    print "Done!".green
  rescue Aws::Lambda::Errors::ServiceException => e
    @logger.error("There was an error deleting #{function_name}:\n #{e.message}")
  end
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Ruby -API-Referenz.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Die Datei „Cargo.toml“ mit in diesem Szenario verwendeten Abhängigkeiten.

```
[package]
name = "lambda-code-examples"
version = "0.1.0"
edition = "2021"
```

```
# See more keys and their definitions at https://doc.rust-lang.org/cargo/
reference/manifest.html

[dependencies]
aws-config = { version = "1.0.1", features = ["behavior-version-latest"] }
aws-sdk-ec2 = { version = "1.3.0" }
aws-sdk-iam = { version = "1.3.0" }
aws-sdk-lambda = { version = "1.3.0" }
aws-sdk-s3 = { version = "1.4.0" }
aws-smithy-types = { version = "1.0.1" }
aws-types = { version = "1.0.1" }
clap = { version = "~4.4", features = ["derive"] }
tokio = { version = "1.20.1", features = ["full"] }
tracing-subscriber = { version = "0.3.15", features = ["env-filter"] }
tracing = "0.1.37"
serde_json = "1.0.94"
anyhow = "1.0.71"
uuid = { version = "1.3.3", features = ["v4"] }
lambda_runtime = "0.8.0"
serde = "1.0.164"
```

Eine Sammlung von Hilfsprogrammen, die das Aufrufen von Lambda für dieses Szenario optimieren. Diese Datei ist „src/ations.rs“ in der Kiste.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use anyhow::anyhow;
use aws_sdk_iam::operation::{create_role::CreateRoleError,
 delete_role::DeleteRoleOutput};
use aws_sdk_lambda::{
    operation::{
        delete_function::DeleteFunctionOutput, get_function::GetFunctionOutput,
        invoke::InvokeOutput, list_functions::ListFunctionsOutput,
        update_function_code::UpdateFunctionCodeOutput,
        update_function_configuration::UpdateFunctionConfigurationOutput,
    },
    primitives::ByteStream,
    types::{Environment, FunctionCode, LastUpdateStatus, State},
};
use aws_sdk_s3::{
    error::ErrorMetadata,
```

```
    operation::{delete_bucket::DeleteBucketOutput,
 delete_object::DeleteObjectOutput},
    types::CreateBucketConfiguration,
};
use aws_smithy_types::Blob;
use serde::{ser::SerializeMap, Serialize};
use std::{path::PathBuf, str::FromStr, time::Duration};
use tracing::{debug, info, warn};

/* Operation describes  */
#[derive(Clone, Copy, Debug, Serialize)]
pub enum Operation {
    #[serde(rename = "plus")]
    Plus,
    #[serde(rename = "minus")]
    Minus,
    #[serde(rename = "times")]
    Times,
    #[serde(rename = "divided-by")]
    DividedBy,
}

impl FromStr for Operation {
    type Err = anyhow::Error;

    fn from_str(s: &str) -> Result<Self, Self::Err> {
        match s {
            "plus" => Ok(Operation::Plus),
            "minus" => Ok(Operation::Minus),
            "times" => Ok(Operation::Times),
            "divided-by" => Ok(Operation::DividedBy),
            _ => Err(anyhow!("Unknown operation {s}")),
        }
    }
}

impl ToString for Operation {
    fn to_string(&self) -> String {
        match self {
            Operation::Plus => "plus".to_string(),
            Operation::Minus => "minus".to_string(),
            Operation::Times => "times".to_string(),
            Operation::DividedBy => "divided-by".to_string(),
        }
```

```
    }
}

/**
 * InvokeArgs will be serialized as JSON and sent to the AWS Lambda handler.
 */
#[derive(Debug)]
pub enum InvokeArgs {
    Increment(i32),
    Arithmetic(Operation, i32, i32),
}

impl Serialize for InvokeArgs {
    fn serialize<S>(&self, serializer: S) -> Result<S::Ok, S::Error>
    where
        S: serde::Serializer,
    {
        match self {
            InvokeArgs::Increment(i) => serializer.serialize_i32(*i),
            InvokeArgs::Arithmetic(o, i, j) => {
                let mut map: S::SerializeMap =
 serializer.serialize_map(Some(3))?;
                map.serialize_key(&"op".to_string())?;
                map.serialize_value(&o.to_string())?;
                map.serialize_key(&"i".to_string())?;
                map.serialize_value(&i)?;
                map.serialize_key(&"j".to_string())?;
                map.serialize_value(&j)?;
                map.end()
            }
        }
    }
}

/** A policy document allowing Lambda to execute this function on the account's
 behalf. */
const ROLE_POLICY_DOCUMENT: &str = r#"{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "Service": "lambda.amazonaws.com" },
            "Action": "sts:AssumeRole"
        }
```

```
    ]
}"#;

/**
 * A LambdaManager gathers all the resources necessary to run the Lambda example
 scenario.
 * This includes instantiated aws_sdk clients and details of resource names.
 */
pub struct LambdaManager {
    iam_client: aws_sdk_iam::Client,
    lambda_client: aws_sdk_lambda::Client,
    s3_client: aws_sdk_s3::Client,
    lambda_name: String,
    role_name: String,
    bucket: String,
    own_bucket: bool,
}

// These unit type structs provide nominal typing on top of String parameters for
 LambdaManager::new
pub struct LambdaName(pub String);
pub struct RoleName(pub String);
pub struct Bucket(pub String);
pub struct OwnBucket(pub bool);

impl LambdaManager {
    pub fn new(
        iam_client: aws_sdk_iam::Client,
        lambda_client: aws_sdk_lambda::Client,
        s3_client: aws_sdk_s3::Client,
        lambda_name: LambdaName,
        role_name: RoleName,
        bucket: Bucket,
        own_bucket: OwnBucket,
    ) -> Self {
        Self {
            iam_client,
            lambda_client,
            s3_client,
            lambda_name: lambda_name.0,
            role_name: role_name.0,
            bucket: bucket.0,
            own_bucket: own_bucket.0,
        }
```

```
    }

    /**
     * Load the AWS configuration from the environment.
     * Look up lambda_name and bucket if none are given, or generate a random
name if not present in the environment.
     * If the bucket name is provided, the caller needs to have created the
bucket.
     * If the bucket name is generated, it will be created.
     */
    pub async fn load_from_env(lambda_name: Option<String>, bucket:
Option<String>) -> Self {
        let sdk_config = aws_config::load_from_env().await;
        let lambda_name = LambdaName(lambda_name.unwrap_or_else(|| {
            std::env::var("LAMBDA_NAME").unwrap_or_else(|_|
"rust_lambda_example".to_string())
        }));
        let role_name = RoleName(format!("{}_role", lambda_name.0));
        let (bucket, own_bucket) =
            match bucket {
                Some(bucket) => (Bucket(bucket), false),
                None => (
                    Bucket(std::env::var("LAMBDA_BUCKET").unwrap_or_else(|_| {
                        format!("rust-lambda-example-{}", uuid::Uuid::new_v4())
                    })),
                    true,
                ),
            };

        let s3_client = aws_sdk_s3::Client::new(&sdk_config);

        if own_bucket {
            info!("Creating bucket for demo: {}", bucket.0);
            s3_client
                .create_bucket()
                .bucket(bucket.0.clone())
                .create_bucket_configuration(
                    CreateBucketConfiguration::builder()

.location_constraint(aws_sdk_s3::types::BucketLocationConstraint::from(
                            sdk_config.region().unwrap().as_ref(),
                        ))
                        .build(),
                )
```

```
                .send()
                .await
                .unwrap();
        }

        Self::new(
            aws_sdk_iam::Client::new(&sdk_config),
            aws_sdk_lambda::Client::new(&sdk_config),
            s3_client,
            lambda_name,
            role_name,
            bucket,
            OwnBucket(own_bucket),
        )
    }

    // snippet-start:[lambda.rust.scenario.prepare_function]
    /**
     * Upload function code from a path to a zip file.
     * The zip file must have an AL2 Linux-compatible binary called `bootstrap`.
     * The easiest way to create such a zip is to use `cargo lambda build --
output-format Zip`.
     */
    async fn prepare_function(
        &self,
        zip_file: PathBuf,
        key: Option<String>,
    ) -> Result<FunctionCode, anyhow::Error> {
        let body = ByteStream::from_path(zip_file).await?;

        let key = key.unwrap_or_else(|| format!("{}_code", self.lambda_name));

        info!("Uploading function code to s3://{}/{}", self.bucket, key);
        let _ = self
            .s3_client
            .put_object()
            .bucket(self.bucket.clone())
            .key(key.clone())
            .body(body)
            .send()
            .await?;

        Ok(FunctionCode::builder()
            .s3_bucket(self.bucket.clone())
```

```
            .s3_key(key)
            .build())
    }
    // snippet-end:[lambda.rust.scenario.prepare_function]

    // snippet-start:[lambda.rust.scenario.create_function]
    /**
     * Create a function, uploading from a zip file.
     */
    pub async fn create_function(&self, zip_file: PathBuf) -> Result<String,
anyhow::Error> {
        let code = self.prepare_function(zip_file, None).await?;

        let key = code.s3_key().unwrap().to_string();

        let role = self.create_role().await.map_err(|e| anyhow!(e))?;

        info!("Created iam role, waiting 15s for it to become active");
        tokio::time::sleep(Duration::from_secs(15)).await;

        info!("Creating lambda function {}", self.lambda_name);
        let _ = self
            .lambda_client
            .create_function()
            .function_name(self.lambda_name.clone())
            .code(code)
            .role(role.arn())
            .runtime(aws_sdk_lambda::types::Runtime::Providedal2)
            .handler("_unused")
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        self.lambda_client
            .publish_version()
            .function_name(self.lambda_name.clone())
            .send()
            .await?;

        Ok(key)
    }
    // snippet-end:[lambda.rust.scenario.create_function]
```

```
   /**
    * Create an IAM execution role for the managed Lambda function.
    * If the role already exists, use that instead.
    */
   async fn create_role(&self) -> Result<aws_sdk_iam::types::Role,
CreateRoleError> {
       info!("Creating execution role for function");
       let get_role = self
           .iam_client
           .get_role()
           .role_name(self.role_name.clone())
           .send()
           .await;
       if let Ok(get_role) = get_role {
           if let Some(role) = get_role.role {
               return Ok(role);
           }
       }

       let create_role = self
           .iam_client
           .create_role()
           .role_name(self.role_name.clone())
           .assume_role_policy_document(ROLE_POLICY_DOCUMENT)
           .send()
           .await;

       match create_role {
           Ok(create_role) => match create_role.role {
               Some(role) => Ok(role),
               None => Err(CreateRoleError::generic(
                   ErrorMetadata::builder()
                       .message("CreateRole returned empty success")
                       .build(),
               )),
           },
           Err(err) => Err(err.into_service_error()),
       }
   }

   /**
    * Poll `is_function_ready` with a 1-second delay. It returns when the
function is ready or when there's an error checking the function's state.
```

```
     */
    pub async fn wait_for_function_ready(&self) -> Result<(), anyhow::Error> {
        info!("Waiting for function");
        while !self.is_function_ready(None).await? {
            info!("Function is not ready, sleeping 1s");
            tokio::time::sleep(Duration::from_secs(1)).await;
        }
        Ok(())
    }

    /**
     * Check if a Lambda function is ready to be invoked.
     * A Lambda function is ready for this scenario when its state is active and
its LastUpdateStatus is Successful.
     * Additionally, if a sha256 is provided, the function must have that as its
current code hash.
     * Any missing properties or failed requests will be reported as an Err.
     */
    async fn is_function_ready(
        &self,
        expected_code_sha256: Option<&str>,
    ) -> Result<bool, anyhow::Error> {
        match self.get_function().await {
            Ok(func) => {
                if let Some(config) = func.configuration() {
                    if let Some(state) = config.state() {
                        info!(?state, "Checking if function is active");
                        if !matches!(state, State::Active) {
                            return Ok(false);
                        }
                    }
                    match config.last_update_status() {
                        Some(last_update_status) => {
                            info!(?last_update_status, "Checking if function is
ready");
                            match last_update_status {
                                LastUpdateStatus::Successful => {
                                    // continue
                                }
                                LastUpdateStatus::Failed |
LastUpdateStatus::InProgress => {
                                    return Ok(false);
                                }
                                unknown => {
```

```
                                    warn!(
                                        status_variant = unknown.as_str(),
                                        "LastUpdateStatus unknown"
                                    );
                                    return Err(anyhow!(
                                        "Unknown LastUpdateStatus, fn config is
{config:?}"
                                    ));
                                }
                            }
                        }
                        None => {
                            warn!("Missing last update status");
                            return Ok(false);
                        }
                    };
                    if expected_code_sha256.is_none() {
                        return Ok(true);
                    }
                    if let Some(code_sha256) = config.code_sha256() {
                        return Ok(code_sha256 ==
expected_code_sha256.unwrap_or_default());
                    }
                }
            }
            Err(e) => {
                warn!(?e, "Could not get function while waiting");
            }
        }
        Ok(false)
    }

    // snippet-start:[lambda.rust.scenario.get_function]
    /** Get the Lambda function with this Manager's name. */
    pub async fn get_function(&self) -> Result<GetFunctionOutput, anyhow::Error>
{
        info!("Getting lambda function");
        self.lambda_client
            .get_function()
            .function_name(self.lambda_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from)
    }
```

```
    // snippet-end:[lambda.rust.scenario.get_function]

    // snippet-start:[lambda.rust.scenario.list_functions]
    /** List all Lambda functions in the current Region. */
    pub async fn list_functions(&self) -> Result<ListFunctionsOutput,
anyhow::Error> {
        info!("Listing lambda functions");
        self.lambda_client
            .list_functions()
            .send()
            .await
            .map_err(anyhow::Error::from)
    }
    // snippet-end:[lambda.rust.scenario.list_functions]

    // snippet-start:[lambda.rust.scenario.invoke]
    /** Invoke the lambda function using calculator InvokeArgs. */
    pub async fn invoke(&self, args: InvokeArgs) -> Result<InvokeOutput,
anyhow::Error> {
        info!(?args, "Invoking {}", self.lambda_name);
        let payload = serde_json::to_string(&args)?;
        debug!(?payload, "Sending payload");
        self.lambda_client
            .invoke()
            .function_name(self.lambda_name.clone())
            .payload(Blob::new(payload))
            .send()
            .await
            .map_err(anyhow::Error::from)
    }
    // snippet-end:[lambda.rust.scenario.invoke]

    // snippet-start:[lambda.rust.scenario.update_function_code]
    /** Given a Path to a zip file, update the function's code and wait for the
update to finish. */
    pub async fn update_function_code(
        &self,
        zip_file: PathBuf,
        key: String,
    ) -> Result<UpdateFunctionCodeOutput, anyhow::Error> {
        let function_code = self.prepare_function(zip_file, Some(key)).await?;

        info!("Updating code for {}", self.lambda_name);
        let update = self
```

```
            .lambda_client
            .update_function_code()
            .function_name(self.lambda_name.clone())
            .s3_bucket(self.bucket.clone())
            .s3_key(function_code.s3_key().unwrap().to_string())
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        Ok(update)
    }
    // snippet-end:[lambda.rust.scenario.update_function_code]

    // snippet-start:[lambda.rust.scenario.update_function_configuration]
    /** Update the environment for a function. */
    pub async fn update_function_configuration(
        &self,
        environment: Environment,
    ) -> Result<UpdateFunctionConfigurationOutput, anyhow::Error> {
        info!(
            ?environment,
            "Updating environment for {}", self.lambda_name
        );
        let updated = self
            .lambda_client
            .update_function_configuration()
            .function_name(self.lambda_name.clone())
            .environment(environment)
            .send()
            .await
            .map_err(anyhow::Error::from)?;

        self.wait_for_function_ready().await?;

        Ok(updated)
    }
    // snippet-end:[lambda.rust.scenario.update_function_configuration]

    // snippet-start:[lambda.rust.scenario.delete_function]
    /** Delete a function and its role, and if possible or necessary, its
associated code object and bucket. */
    pub async fn delete_function(
```

```
        &self,
        location: Option<String>,
    ) -> (
        Result<DeleteFunctionOutput, anyhow::Error>,
        Result<DeleteRoleOutput, anyhow::Error>,
        Option<Result<DeleteObjectOutput, anyhow::Error>>,
    ) {
        info!("Deleting lambda function {}", self.lambda_name);
        let delete_function = self
            .lambda_client
            .delete_function()
            .function_name(self.lambda_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from);

        info!("Deleting iam role {}", self.role_name);
        let delete_role = self
            .iam_client
            .delete_role()
            .role_name(self.role_name.clone())
            .send()
            .await
            .map_err(anyhow::Error::from);

        let delete_object: Option<Result<DeleteObjectOutput, anyhow::Error>> =
            if let Some(location) = location {
                info!("Deleting object {location}");
                Some(
                    self.s3_client
                        .delete_object()
                        .bucket(self.bucket.clone())
                        .key(location)
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                info!(?location, "Skipping delete object");
                None
            };

        (delete_function, delete_role, delete_object)
    }
```

```
    // snippet-end:[lambda.rust.scenario.delete_function]

    pub async fn cleanup(
        &self,
        location: Option<String>,
    ) -> (
        (
            Result<DeleteFunctionOutput, anyhow::Error>,
            Result<DeleteRoleOutput, anyhow::Error>,
            Option<Result<DeleteObjectOutput, anyhow::Error>>,
        ),
        Option<Result<DeleteBucketOutput, anyhow::Error>>,
    ) {
        let delete_function = self.delete_function(location).await;

        let delete_bucket = if self.own_bucket {
            info!("Deleting bucket {}", self.bucket);
            if delete_function.2.is_none() ||
 delete_function.2.as_ref().unwrap().is_ok() {
                Some(
                    self.s3_client
                        .delete_bucket()
                        .bucket(self.bucket.clone())
                        .send()
                        .await
                        .map_err(anyhow::Error::from),
                )
            } else {
                None
            }
        } else {
            info!("No bucket to clean up");
            None
        };

        (delete_function, delete_bucket)
    }
}

/**
 * Testing occurs primarily as an integration test running the `scenario` bin
 successfully.
 * Each action relies deeply on the internal workings and state of Amazon Simple
 Storage Service (Amazon S3), Lambda, and IAM working together.
```

```
 * It is therefore infeasible to mock the clients to test the individual actions.
 */
#[cfg(test)]
mod test {
    use super::{InvokeArgs, Operation};
    use serde_json::json;

    /** Make sure that the JSON output of serializing InvokeArgs is what's
 expected by the calculator. */
    #[test]
    fn test_serialize() {
        assert_eq!(json!(InvokeArgs::Increment(5)), 5);
        assert_eq!(
            json!(InvokeArgs::Arithmetic(Operation::Plus, 5, 7)).to_string(),
            r#"{"op":"plus","i":5,"j":7}"#.to_string(),
        );
    }
}
```

Eine Binärdatei, um das Szenario vom Anfang bis Ende auszuführen, wobei Befehlszeilen-Flags verwendet werden, um einige Verhaltensweisen zu steuern. Diese Datei ist „src/bin/scenario.rs“ in der Kiste.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

/*
## Service actions

Service actions wrap the SDK call, taking a client and any specific parameters
 necessary for the call.

* CreateFunction
* GetFunction
* ListFunctions
* Invoke
* UpdateFunctionCode
* UpdateFunctionConfiguration
* DeleteFunction

## Scenario
```

```
A scenario runs at a command prompt and prints output to the user on the result
 of each service action. A scenario can run in one of two ways: straight through,
 printing out progress as it goes, or as an interactive question/answer script.

## Getting started with functions

Use an SDK to manage AWS Lambda functions: create a function, invoke it, update
 its code, invoke it again, view its output and logs, and delete it.

This scenario uses two Lambda handlers:
_Note: Handlers don't use AWS SDK API calls._

The increment handler is straightforward:

1. It accepts a number, increments it, and returns the new value.
2. It performs simple logging of the result.

The arithmetic handler is more complex:
1. It accepts a set of actions ['plus', 'minus', 'times', 'divided-by'] and two
 numbers, and returns the result of the calculation.
2. It uses an environment variable to control log level (such as DEBUG, INFO,
 WARNING, ERROR).
It logs a few things at different levels, such as:
    * DEBUG: Full event data.
    * INFO: The calculation result.
    * WARN~ING~: When a divide by zero error occurs.
    * This will be the typical `RUST_LOG` variable.


The steps of the scenario are:

1. Create an AWS Identity and Access Management (IAM) role that meets the
 following requirements:
    * Has an assume_role policy that grants 'lambda.amazonaws.com' the
 'sts:AssumeRole' action.
    * Attaches the 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole' managed role.
    * _You must wait for ~10 seconds after the role is created before you can use
 it!_
2. Create a function (CreateFunction) for the increment handler by packaging it
 as a zip and doing one of the following:
    * Adding it with CreateFunction Code.ZipFile.
    * --or--
```

```
    * Uploading it to Amazon Simple Storage Service (Amazon S3) and adding it
 with CreateFunction Code.S3Bucket/S3Key.
    * _Note: Zipping the file does not have to be done in code._
    * If you have a waiter, use it to wait until the function is active.
 Otherwise, call GetFunction until State is Active.
3. Invoke the function with a number and print the result.
4. Update the function (UpdateFunctionCode) to the arithmetic handler by
 packaging it as a zip and doing one of the following:
    * Adding it with UpdateFunctionCode ZipFile.
    * --or--
    * Uploading it to Amazon S3 and adding it with UpdateFunctionCode S3Bucket/
S3Key.
5. Call GetFunction until Configuration.LastUpdateStatus is 'Successful' (or
 'Failed').
6. Update the environment variable by calling UpdateFunctionConfiguration and
 pass it a log level, such as:
    * Environment={'Variables': {'RUST_LOG': 'TRACE'}}
7. Invoke the function with an action from the list and a couple of values.
 Include LogType='Tail' to get logs in the result. Print the result of the
 calculation and the log.
8. [Optional] Invoke the function to provoke a divide-by-zero error and show the
 log result.
9. List all functions for the account, using pagination (ListFunctions).
10. Delete the function (DeleteFunction).
11. Delete the role.

Each step should use the function created in Service Actions to abstract calling
 the SDK.
 */

use aws_sdk_lambda::{operation::invoke::InvokeOutput, types::Environment};
use clap::Parser;
use std::{collections::HashMap, path::PathBuf};
use tracing::{debug, info, warn};
use tracing_subscriber::EnvFilter;

use lambda_code_examples::actions::{
    InvokeArgs::{Arithmetic, Increment},
    LambdaManager, Operation,
};

#[derive(Debug, Parser)]
pub struct Opt {
    /// The AWS Region.
```

```
    #[structopt(short, long)]
    pub region: Option<String>,

    // The bucket to use for the FunctionCode.
    #[structopt(short, long)]
    pub bucket: Option<String>,

    // The name of the Lambda function.
    #[structopt(short, long)]
    pub lambda_name: Option<String>,

    // The number to increment.
    #[structopt(short, long, default_value = "12")]
    pub inc: i32,

    // The left operand.
    #[structopt(long, default_value = "19")]
    pub num_a: i32,

    // The right operand.
    #[structopt(long, default_value = "23")]
    pub num_b: i32,

    // The arithmetic operation.
    #[structopt(short, long, default_value = "plus")]
    pub operation: Operation,

    #[structopt(long)]
    pub cleanup: Option<bool>,

    #[structopt(long)]
    pub no_cleanup: Option<bool>,
}

fn code_path(lambda: &str) -> PathBuf {
    PathBuf::from(format!("../target/lambda/{lambda}/bootstrap.zip"))
}

// snippet-start:[lambda.rust.scenario.log_invoke_output]
fn log_invoke_output(invoke: &InvokeOutput, message: &str) {
    if let Some(payload) = invoke.payload().cloned() {
        let payload = String::from_utf8(payload.into_inner());
        info!(?payload, message);
    } else {
```

```
        info!("Could not extract payload")
    }
    if let Some(logs) = invoke.log_result() {
        debug!(?logs, "Invoked function logs")
    } else {
        debug!("Invoked function had no logs")
    }
}
// snippet-end:[lambda.rust.scenario.log_invoke_output]

async fn main_block(
    opt: &Opt,
    manager: &LambdaManager,
    code_location: String,
) -> Result<(), anyhow::Error> {
    let invoke = manager.invoke(Increment(opt.inc)).await?;
    log_invoke_output(&invoke, "Invoked function configured as increment");

    let update_code = manager
        .update_function_code(code_path("arithmetic"), code_location.clone())
        .await?;

    let code_sha256 = update_code.code_sha256().unwrap_or("Unknown SHA");
    info!(?code_sha256, "Updated function code with arithmetic.zip");

    let arithmetic_args = Arithmetic(opt.operation, opt.num_a, opt.num_b);
    let invoke = manager.invoke(arithmetic_args).await?;
    log_invoke_output(&invoke, "Invoked function configured as arithmetic");

    let update = manager
        .update_function_configuration(
            Environment::builder()
                .set_variables(Some(HashMap::from([(
                    "RUST_LOG".to_string(),
                    "trace".to_string(),
                )])))
                .build(),
        )
        .await?;
    let updated_environment = update.environment();
    info!(?updated_environment, "Updated function configuration");

    let invoke = manager
        .invoke(Arithmetic(opt.operation, opt.num_a, opt.num_b))
```

```
        .await?;
    log_invoke_output(
        &invoke,
        "Invoked function configured as arithmetic with increased logging",
    );

    let invoke = manager
        .invoke(Arithmetic(Operation::DividedBy, opt.num_a, 0))
        .await?;
    log_invoke_output(
        &invoke,
        "Invoked function configured as arithmetic with divide by zero",
    );

    Ok::<(), anyhow::Error>(())
}

#[tokio::main]
async fn main() {
    tracing_subscriber::fmt()
        .without_time()
        .with_file(true)
        .with_line_number(true)
        .with_env_filter(EnvFilter::from_default_env())
        .init();

    let opt = Opt::parse();
    let manager = LambdaManager::load_from_env(opt.lambda_name.clone(),
 opt.bucket.clone()).await;

    let key = match manager.create_function(code_path("increment")).await {
        Ok(init) => {
            info!(?init, "Created function, initially with increment.zip");
            let run_block = main_block(&opt, &manager, init.clone()).await;
            info!(?run_block, "Finished running example, cleaning up");
            Some(init)
        }
        Err(err) => {
            warn!(?err, "Error happened when initializing function");
            None
        }
    };

    if Some(false) == opt.cleanup || Some(true) == opt.no_cleanup {
```

```
        info!("Skipping cleanup")
    } else {
        let delete = manager.cleanup(key).await;
        info!(?delete, "Deleted function & cleaned up resources");
    }
}
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zu AWS -SDK für Rust.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

SAP ABAP

SDK für SAP ABAP

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

```
   TRY.
       "Create an AWS Identity and Access Management (IAM) role that grants AWS
Lambda permission to write to logs."
       DATA(lv_policy_document) = `{` &&
           `"Version":"2012-10-17",` &&
                 `"Statement": [` &&
                   `{` &&
                     `"Effect": "Allow",` &&
                     `"Action": [` &&
```

```
                      `"sts:AssumeRole"` &&
                    `],` &&
                    `"Principal": {` &&
                      `"Service": [` &&
                        `"lambda.amazonaws.com"` &&
                      `]` &&
                    `}` &&
                  `}` &&
                `]` &&
              `}`.
        TRY.
            DATA(lo_create_role_output) =  lo_iam->createrole(
                    iv_rolename = iv_role_name
                    iv_assumerolepolicydocument = lv_policy_document
                    iv_description = 'Grant lambda permission to write to logs'
                ).
            MESSAGE 'IAM role created.' TYPE 'I'.
            WAIT UP TO 10 SECONDS.            " Make sure that the IAM role is
 ready for use. "
          CATCH /aws1/cx_iamentityalrdyexex.
            MESSAGE 'IAM role already exists.' TYPE 'E'.
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iammalformedplydocex.
            MESSAGE 'Policy document in the request is malformed.' TYPE 'E'.
        ENDTRY.

        TRY.
            lo_iam->attachrolepolicy(
                iv_rolename  = iv_role_name
                iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole'
            ).
            MESSAGE 'Attached policy to the IAM role.' TYPE 'I'.
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
          CATCH /aws1/cx_iamplynotattachableex.
            MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
 modifiable.' TYPE 'E'.
```

```
        ENDTRY.

        " Create a Lambda function and upload handler code. "
        " Lambda function performs 'increment' action on a number. "
        TRY.
            lo_lmd->createfunction(
                 iv_functionname = iv_function_name
                 iv_runtime = `python3.9`
                 iv_role = lo_create_role_output->get_role( )->get_arn( )
                 iv_handler = iv_handler
                 io_code = io_initial_zip_file
                 iv_description = 'AWS Lambda code example'
             ).
            MESSAGE 'Lambda function created.' TYPE 'I'.
          CATCH /aws1/cx_lmdcodestorageexcdex.
            MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        " Verify the function is in Active state "
        WHILE lo_lmd->getfunction( iv_functionname = iv_function_name )-
>get_configuration( )->ask_state( ) <> 'Active'.
          IF sy-index = 10.
            EXIT.               " Maximum 10 seconds. "
          ENDIF.
          WAIT UP TO 1 SECONDS.
        ENDWHILE.

        "Invoke the function with a single parameter and get results."
        TRY.
            DATA(lv_json) = /aws1/cl_rt_util=>string_to_xstring(
              `{`  &&
                `"action": "increment",`  &&
                `"number": 10` &&
              `}`
            ).
            DATA(lo_initial_invoke_output) =  lo_lmd->invoke(
                       iv_functionname = iv_function_name
                       iv_payload = lv_json
                  ).
```

```
            ov_initial_invoke_payload = lo_initial_invoke_output->get_payload( ).
           " ov_initial_invoke_payload is returned for testing purposes. "
            DATA(lo_writer_json) = cl_sxml_string_writer=>create( type =
 if_sxml=>co_xt_json ).
            CALL TRANSFORMATION id SOURCE XML ov_initial_invoke_payload RESULT
 XML lo_writer_json.
            DATA(lv_result) = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
            MESSAGE 'Lambda function invoked.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvrequestcontex.
            MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
          CATCH /aws1/cx_lmdunsuppedmediatyp00.
            MESSAGE 'Invoke request body does not have JSON as its content type.'
 TYPE 'E'.
        ENDTRY.

        " Update the function code and configure its Lambda environment with an
 environment variable. "
        " Lambda function is updated to perform 'decrement' action also. "
        TRY.
            lo_lmd->updatefunctioncode(
                  iv_functionname = iv_function_name
                  iv_zipfile = io_updated_zip_file
              ).
            WAIT UP TO 10 SECONDS.            " Make sure that the update is
 completed. "
            MESSAGE 'Lambda function code updated.' TYPE 'I'.
          CATCH /aws1/cx_lmdcodestorageexcdex.
            MESSAGE 'Maximum total code size per account exceeded.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        TRY.
            DATA lt_variables TYPE /aws1/
cl_lmdenvironmentvaria00=>tt_environmentvariables.
            DATA ls_variable LIKE LINE OF lt_variables.
            ls_variable-key = 'LOG_LEVEL'.
```

```
            ls_variable-value = NEW /aws1/cl_lmdenvironmentvaria00( iv_value =
 'info' ).
            INSERT ls_variable INTO TABLE lt_variables.

            lo_lmd->updatefunctionconfiguration(
                  iv_functionname = iv_function_name
                  io_environment = NEW /aws1/cl_lmdenvironment( it_variables =
 lt_variables )
              ).
            WAIT UP TO 10 SECONDS.            " Make sure that the update is
 completed. "
            MESSAGE 'Lambda function configuration/settings updated.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourceconflictex.
            MESSAGE 'Resource already exists or another operation is in
 progress.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        "Invoke the function with new parameters and get results. Display the
 execution log that's returned from the invocation."
        TRY.
            lv_json = /aws1/cl_rt_util=>string_to_xstring(
              `{`  &&
                `"action": "decrement",`  &&
                `"number": 10` &&
              `}`
            ).
            DATA(lo_updated_invoke_output) =  lo_lmd->invoke(
                       iv_functionname = iv_function_name
                       iv_payload = lv_json
                  ).
            ov_updated_invoke_payload = lo_updated_invoke_output->get_payload( ).
           " ov_updated_invoke_payload is returned for testing purposes. "
            lo_writer_json = cl_sxml_string_writer=>create( type =
 if_sxml=>co_xt_json ).
            CALL TRANSFORMATION id SOURCE XML ov_updated_invoke_payload RESULT
 XML lo_writer_json.
            lv_result = cl_abap_codepage=>convert_from( lo_writer_json-
>get_output( ) ).
            MESSAGE 'Lambda function invoked.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
```

```
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdinvrequestcontex.
            MESSAGE 'Unable to parse request body as JSON.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
          CATCH /aws1/cx_lmdunsuppedmediatyp00.
            MESSAGE 'Invoke request body does not have JSON as its content type.'
 TYPE 'E'.
        ENDTRY.

        " List the functions for your account. "
        TRY.
            DATA(lo_list_output) = lo_lmd->listfunctions( ).
            DATA(lt_functions) = lo_list_output->get_functions( ).
            MESSAGE 'Retrieved list of Lambda functions.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
        ENDTRY.

        " Delete the Lambda function. "
        TRY.
            lo_lmd->deletefunction( iv_functionname = iv_function_name ).
            MESSAGE 'Lambda function deleted.' TYPE 'I'.
          CATCH /aws1/cx_lmdinvparamvalueex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_lmdresourcenotfoundex.
            MESSAGE 'The requested resource does not exist.' TYPE 'E'.
        ENDTRY.

        " Detach role policy. "
        TRY.
            lo_iam->detachrolepolicy(
                iv_rolename  = iv_role_name
                iv_policyarn = 'arn:aws:iam::aws:policy/service-role/
AWSLambdaBasicExecutionRole'
            ).
            MESSAGE 'Detached policy from the IAM role.' TYPE 'I'.
          CATCH /aws1/cx_iaminvalidinputex.
            MESSAGE 'The request contains a non-valid parameter.' TYPE 'E'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
          CATCH /aws1/cx_iamplynotattachableex.
            MESSAGE 'Service role policies can only be attached to the service-
linked role for their service.' TYPE 'E'.
```

```
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
modifiable.' TYPE 'E'.
        ENDTRY.

        " Delete the IAM role. "
        TRY.
            lo_iam->deleterole( iv_rolename = iv_role_name ).
            MESSAGE 'IAM role deleted.' TYPE 'I'.
          CATCH /aws1/cx_iamnosuchentityex.
            MESSAGE 'The requested resource entity does not exist.' TYPE 'E'.
          CATCH /aws1/cx_iamunmodableentityex.
            MESSAGE 'Service that depends on the service-linked role is not
modifiable.' TYPE 'E'.
        ENDTRY.

      CATCH /aws1/cx_rt_service_generic INTO lo_exception.
        DATA(lv_error) = lo_exception->get_longtext( ).
        MESSAGE lv_error TYPE 'E'.
    ENDTRY.
```

- Weitere API-Informationen finden Sie in den folgenden Themen der API-Referenz zum AWS SDK für SAP ABAP.
  - CreateFunction
  - DeleteFunction
  - GetFunction
  - Aufrufen
  - ListFunctions
  - UpdateFunctionKode
  - UpdateFunctionKonfiguration

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Schreiben Sie benutzerdefinierte Aktivitätsdaten mit einer Lambda-Funktion nach der Amazon Cognito Cognito-Benutzerauthentifizierung mithilfe eines SDK AWS

Das folgende Codebeispiel zeigt, wie benutzerdefinierte Aktivitätsdaten mit einer Lambda-Funktion nach der Amazon Cognito Cognito-Benutzerauthentifizierung geschrieben werden.

- Verwenden Sie Administratorfunktionen, um einen Benutzer zu einem Benutzerpool hinzuzufügen.
- Konfigurieren Sie einen Benutzerpool, um eine Lambda-Funktion für den `PostAuthentication` Trigger aufzurufen.
- Melden Sie den neuen Benutzer bei Amazon Cognito an.
- Die Lambda-Funktion schreibt benutzerdefinierte Informationen in CloudWatch Logs und in eine DynamoDB-Tabelle.
- Rufen Sie benutzerdefinierte Daten aus der DynamoDB-Tabelle ab, zeigen Sie sie an und bereinigen Sie anschließend die Ressourcen.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Sie sehen das vollständige Beispiel und erfahren, wie Sie das AWS -Code-Beispiel-Repository einrichten und ausführen.

Führen Sie ein interaktives Szenario an einer Eingabeaufforderung aus.

```
// ActivityLog separates the steps of this scenario into individual functions so
 that
// they are simpler to read and understand.
type ActivityLog struct {
 helper       IScenarioHelper
 questioner   demotools.IQuestioner
 resources    Resources
 cognitoActor *actions.CognitoActions
}
```

```
// NewActivityLog constructs a new activity log runner.
func NewActivityLog(sdkConfig aws.Config, questioner demotools.IQuestioner,
 helper IScenarioHelper) ActivityLog {
 scenario := ActivityLog{
  helper:       helper,
  questioner:   questioner,
  resources:    Resources{},
  cognitoActor: &actions.CognitoActions{CognitoClient:
 cognitoidentityprovider.NewFromConfig(sdkConfig)},
 }
 scenario.resources.init(scenario.cognitoActor, questioner)
 return scenario
}

// AddUserToPool selects a user from the known users table and uses administrator
 credentials to add the user to the user pool.
func (runner *ActivityLog) AddUserToPool(userPoolId string, tableName string)
 (string, string) {
 log.Println("To facilitate this example, let's add a user to the user pool using
 administrator privileges.")
 users, err := runner.helper.GetKnownUsers(tableName)
 if err != nil {
  panic(err)
 }
 user := users.Users[0]
 log.Printf("Adding known user %v to the user pool.\n", user.UserName)
 err = runner.cognitoActor.AdminCreateUser(userPoolId, user.UserName,
 user.UserEmail)
 if err != nil {
  panic(err)
 }
 pwSet := false
 password := runner.questioner.AskPassword("\nEnter a password that has at least
 eight characters, uppercase, lowercase, numbers and symbols.\n"+
  "(the password will not display as you type):", 8)
 for !pwSet {
  log.Printf("\nSetting password for user '%v'.\n", user.UserName)
  err = runner.cognitoActor.AdminSetUserPassword(userPoolId, user.UserName,
 password)
  if err != nil {
   var invalidPassword *types.InvalidPasswordException
   if errors.As(err, &invalidPassword) {
    password = runner.questioner.AskPassword("\nEnter another password:", 8)
```

```
   } else {
    panic(err)
   }
  } else {
   pwSet = true
  }
 }

 log.Println(strings.Repeat("-", 88))

 return user.UserName, password
}

// AddActivityLogTrigger adds a Lambda handler as an invocation target for the
 PostAuthentication trigger.
func (runner *ActivityLog) AddActivityLogTrigger(userPoolId string,
 activityLogArn string) {
 log.Println("Let's add a Lambda function to handle the PostAuthentication
 trigger from Cognito.\n" +
  "This trigger happens after a user is authenticated, and lets your function
 take action, such as logging\n" +
  "the outcome.")
 err := runner.cognitoActor.UpdateTriggers(
  userPoolId,
  actions.TriggerInfo{Trigger: actions.PostAuthentication, HandlerArn:
 aws.String(activityLogArn)})
 if err != nil {
  panic(err)
 }
 runner.resources.triggers = append(runner.resources.triggers,
 actions.PostAuthentication)
 log.Printf("Lambda function %v added to user pool %v to handle
 PostAuthentication Cognito trigger.\n",
  activityLogArn, userPoolId)

 log.Println(strings.Repeat("-", 88))
}

// SignInUser signs in as the specified user.
func (runner *ActivityLog) SignInUser(clientId string, userName string, password
 string) {
 log.Printf("Now we'll sign in user %v and check the results in the logs and the
 DynamoDB table.", userName)
 runner.questioner.Ask("Press Enter when you're ready.")
```

```
 authResult, err := runner.cognitoActor.SignIn(clientId, userName, password)
 if err != nil {
  panic(err)
 }
 log.Println("Sign in successful.",
  "The PostAuthentication Lambda handler writes custom information to CloudWatch
 Logs.")

 runner.resources.userAccessTokens = append(runner.resources.userAccessTokens,
 *authResult.AccessToken)
}

// GetKnownUserLastLogin gets the login info for a user from the Amazon DynamoDB
 table and displays it.
func (runner *ActivityLog) GetKnownUserLastLogin(tableName string, userName
 string) {
 log.Println("The PostAuthentication handler also writes login data to the
 DynamoDB table.")
 runner.questioner.Ask("Press Enter when you're ready to continue.")
 users, err := runner.helper.GetKnownUsers(tableName)
 if err != nil {
  panic(err)
 }
 for _, user := range users.Users {
  if user.UserName == userName {
   log.Println("The last login info for the user in the known users table is:")
   log.Printf("\t%+v", *user.LastLogin)
  }
 }
 log.Println(strings.Repeat("-", 88))
}

// Run runs the scenario.
func (runner *ActivityLog) Run(stackName string) {
 defer func() {
  if r := recover(); r != nil {
   log.Println("Something went wrong with the demo.")
   runner.resources.Cleanup()
  }
 }()

 log.Println(strings.Repeat("-", 88))
 log.Printf("Welcome\n")
```

```
 log.Println(strings.Repeat("-", 88))

 stackOutputs, err := runner.helper.GetStackOutputs(stackName)
 if err != nil {
  panic(err)
 }
 runner.resources.userPoolId = stackOutputs["UserPoolId"]
 runner.helper.PopulateUserTable(stackOutputs["TableName"])
 userName, password := runner.AddUserToPool(stackOutputs["UserPoolId"],
 stackOutputs["TableName"])

 runner.AddActivityLogTrigger(stackOutputs["UserPoolId"],
 stackOutputs["ActivityLogFunctionArn"])
 runner.SignInUser(stackOutputs["UserPoolClientId"], userName, password)
 runner.helper.ListRecentLogEvents(stackOutputs["ActivityLogFunction"])
 runner.GetKnownUserLastLogin(stackOutputs["TableName"], userName)

 runner.resources.Cleanup()

 log.Println(strings.Repeat("-", 88))
 log.Println("Thanks for watching!")
 log.Println(strings.Repeat("-", 88))
}
```

Behandeln Sie den `PostAuthentication` Trigger mit einer Lambda-Funktion.

```
const TABLE_NAME = "TABLE_NAME"

// LoginInfo defines structured login data that can be marshalled to a DynamoDB
 format.
type LoginInfo struct {
 UserPoolId string `dynamodbav:"UserPoolId"`
 ClientId   string `dynamodbav:"ClientId"`
 Time       string `dynamodbav:"Time"`
}

// UserInfo defines structured user data that can be marshalled to a DynamoDB
 format.
type UserInfo struct {
 UserName  string    `dynamodbav:"UserName"`
```

```
 UserEmail string    `dynamodbav:"UserEmail"`
 LastLogin LoginInfo `dynamodbav:"LastLogin"`
}

// GetKey marshals the user email value to a DynamoDB key format.
func (user UserInfo) GetKey() map[string]dynamodbtypes.AttributeValue {
 userEmail, err := attributevalue.Marshal(user.UserEmail)
 if err != nil {
  panic(err)
 }
 return map[string]dynamodbtypes.AttributeValue{"UserEmail": userEmail}
}

type handler struct {
 dynamoClient *dynamodb.Client
}

// HandleRequest handles the PostAuthentication event by writing custom data to
 the logs and
// to an Amazon DynamoDB table.
func (h *handler) HandleRequest(ctx context.Context,
 event events.CognitoEventUserPoolsPostAuthentication)
 (events.CognitoEventUserPoolsPostAuthentication, error) {
 log.Printf("Received post authentication trigger from %v for user '%v'",
 event.TriggerSource, event.UserName)
 tableName := os.Getenv(TABLE_NAME)
 user := UserInfo{
  UserName:  event.UserName,
  UserEmail: event.Request.UserAttributes["email"],
  LastLogin: LoginInfo{
   UserPoolId: event.UserPoolID,
   ClientId:   event.CallerContext.ClientID,
   Time:       time.Now().Format(time.UnixDate),
  },
 }
 // Write to CloudWatch Logs.
 fmt.Printf("%#v", user)

 // Also write to an external system. This examples uses DynamoDB to demonstrate.
 userMap, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshal to DynamoDB map. Here's why: %v\n", err)
 } else if len(userMap) == 0 {
  log.Printf("User info marshaled to an empty map.")
```

```
 } else {
  _, err := h.dynamoClient.PutItem(ctx, &dynamodb.PutItemInput{
   Item:      userMap,
   TableName: aws.String(tableName),
  })
  if err != nil {
   log.Printf("Couldn't write to DynamoDB. Here's why: %v\n", err)
  } else {
   log.Printf("Wrote user info to DynamoDB table %v.\n", tableName)
  }
 }

 return event, nil
}

func main() {
 sdkConfig, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  log.Panicln(err)
 }
 h := handler{
  dynamoClient: dynamodb.NewFromConfig(sdkConfig),
 }
 lambda.Start(h.HandleRequest)
}
```

Erstellen Sie eine Struktur, die allgemeine Aufgaben ausführt.

```
// IScenarioHelper defines common functions used by the workflows in this
 example.
type IScenarioHelper interface {
 Pause(secs int)
 GetStackOutputs(stackName string) (actions.StackOutputs, error)
 PopulateUserTable(tableName string)
 GetKnownUsers(tableName string) (actions.UserList, error)
 AddKnownUser(tableName string, user actions.User)
 ListRecentLogEvents(functionName string)
}
```

```
// ScenarioHelper contains AWS wrapper structs used by the workflows in this
 example.
type ScenarioHelper struct {
 questioner  demotools.IQuestioner
 dynamoActor *actions.DynamoActions
 cfnActor    *actions.CloudFormationActions
 cwlActor    *actions.CloudWatchLogsActions
 isTestRun   bool
}

// NewScenarioHelper constructs a new scenario helper.
func NewScenarioHelper(sdkConfig aws.Config, questioner demotools.IQuestioner)
 ScenarioHelper {
 scenario := ScenarioHelper{
  questioner:  questioner,
  dynamoActor: &actions.DynamoActions{DynamoClient:
 dynamodb.NewFromConfig(sdkConfig)},
  cfnActor:    &actions.CloudFormationActions{CfnClient:
 cloudformation.NewFromConfig(sdkConfig)},
  cwlActor:    &actions.CloudWatchLogsActions{CwlClient:
 cloudwatchlogs.NewFromConfig(sdkConfig)},
 }
 return scenario
}

// Pause waits for the specified number of seconds.
func (helper ScenarioHelper) Pause(secs int) {
 if !helper.isTestRun {
  time.Sleep(time.Duration(secs) * time.Second)
 }
}

// GetStackOutputs gets the outputs from the specified CloudFormation stack in a
 structured format.
func (helper ScenarioHelper) GetStackOutputs(stackName string)
 (actions.StackOutputs, error) {
 return helper.cfnActor.GetOutputs(stackName), nil
}

// PopulateUserTable fills the known user table with example data.
func (helper ScenarioHelper) PopulateUserTable(tableName string) {
 log.Printf("First, let's add some users to the DynamoDB %v table we'll use for
 this example.\n", tableName)
 err := helper.dynamoActor.PopulateTable(tableName)
```

```
 if err != nil {
  panic(err)
 }
}

// GetKnownUsers gets the users from the known users table in a structured
 format.
func (helper ScenarioHelper) GetKnownUsers(tableName string) (actions.UserList,
 error) {
 knownUsers, err := helper.dynamoActor.Scan(tableName)
 if err != nil {
  log.Printf("Couldn't get known users from table %v. Here's why: %v\n",
 tableName, err)
 }
 return knownUsers, err
}

// AddKnownUser adds a user to the known users table.
func (helper ScenarioHelper) AddKnownUser(tableName string, user actions.User) {
 log.Printf("Adding user '%v' with email '%v' to the DynamoDB known users
 table...\n",
  user.UserName, user.UserEmail)
 err := helper.dynamoActor.AddUser(tableName, user)
 if err != nil {
  panic(err)
 }
}

// ListRecentLogEvents gets the most recent log stream and events for the
 specified Lambda function and displays them.
func (helper ScenarioHelper) ListRecentLogEvents(functionName string) {
 log.Println("Waiting a few seconds to let Lambda write to CloudWatch Logs...")
 helper.Pause(10)
 log.Println("Okay, let's check the logs to find what's happened recently with
 your Lambda function.")
 logStream, err := helper.cwlActor.GetLatestLogStream(functionName)
 if err != nil {
  panic(err)
 }
 log.Printf("Getting some recent events from log stream %v\n",
 *logStream.LogStreamName)
 events, err := helper.cwlActor.GetLogEvents(functionName,
 *logStream.LogStreamName, 10)
 if err != nil {
```

```
  panic(err)
 }
 for _, event := range events {
  log.Printf("\t%v", *event.Message)
 }
 log.Println(strings.Repeat("-", 88))
}
```

Erstellen Sie eine Struktur, die Amazon Cognito Cognito-Aktionen umschließt.

```
type CognitoActions struct {
 CognitoClient *cognitoidentityprovider.Client
}



// Trigger and TriggerInfo define typed data for updating an Amazon Cognito
 trigger.
type Trigger int

const (
 PreSignUp Trigger = iota
 UserMigration
 PostAuthentication
)

type TriggerInfo struct {
 Trigger    Trigger
 HandlerArn *string
}

// UpdateTriggers adds or removes Lambda triggers for a user pool. When a trigger
 is specified with a `nil` value,
// it is removed from the user pool.
func (actor CognitoActions) UpdateTriggers(userPoolId string,
 triggers ...TriggerInfo) error {
 output, err := actor.CognitoClient.DescribeUserPool(context.TODO(),
 &cognitoidentityprovider.DescribeUserPoolInput{
  UserPoolId: aws.String(userPoolId),
```

```
 })
 if err != nil {
  log.Printf("Couldn't get info about user pool %v. Here's why: %v\n",
 userPoolId, err)
  return err
 }
 lambdaConfig := output.UserPool.LambdaConfig
 for _, trigger := range triggers {
  switch trigger.Trigger {
  case PreSignUp:
   lambdaConfig.PreSignUp = trigger.HandlerArn
  case UserMigration:
   lambdaConfig.UserMigration = trigger.HandlerArn
  case PostAuthentication:
   lambdaConfig.PostAuthentication = trigger.HandlerArn
  }
 }
 _, err = actor.CognitoClient.UpdateUserPool(context.TODO(),
 &cognitoidentityprovider.UpdateUserPoolInput{
  UserPoolId:   aws.String(userPoolId),
  LambdaConfig: lambdaConfig,
 })
 if err != nil {
  log.Printf("Couldn't update user pool %v. Here's why: %v\n", userPoolId, err)
 }
 return err
}



// SignUp signs up a user with Amazon Cognito.
func (actor CognitoActions) SignUp(clientId string, userName string, password
 string, userEmail string) (bool, error) {
 confirmed := false
 output, err := actor.CognitoClient.SignUp(context.TODO(),
 &cognitoidentityprovider.SignUpInput{
  ClientId: aws.String(clientId),
  Password: aws.String(password),
  Username: aws.String(userName),
  UserAttributes: []types.AttributeType{
   {Name: aws.String("email"), Value: aws.String(userEmail)},
  },
 })
 if err != nil {
```

```
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't sign up user %v. Here's why: %v\n", userName, err)
  }
 } else {
  confirmed = output.UserConfirmed
 }
 return confirmed, err
}



// SignIn signs in a user to Amazon Cognito using a username and password
 authentication flow.
func (actor CognitoActions) SignIn(clientId string, userName string, password
 string) (*types.AuthenticationResultType, error) {
 var authResult *types.AuthenticationResultType
 output, err := actor.CognitoClient.InitiateAuth(context.TODO(),
 &cognitoidentityprovider.InitiateAuthInput{
  AuthFlow:       "USER_PASSWORD_AUTH",
  ClientId:       aws.String(clientId),
  AuthParameters: map[string]string{"USERNAME": userName, "PASSWORD": password},
 })
 if err != nil {
  var resetRequired *types.PasswordResetRequiredException
  if errors.As(err, &resetRequired) {
   log.Println(*resetRequired.Message)
  } else {
   log.Printf("Couldn't sign in user %v. Here's why: %v\n", userName, err)
  }
 } else {
  authResult = output.AuthenticationResult
 }
 return authResult, err
}



// ForgotPassword starts a password recovery flow for a user. This flow typically
 sends a confirmation code
// to the user's configured notification destination, such as email.
```

```
func (actor CognitoActions) ForgotPassword(clientId string, userName string)
 (*types.CodeDeliveryDetailsType, error) {
 output, err := actor.CognitoClient.ForgotPassword(context.TODO(),
 &cognitoidentityprovider.ForgotPasswordInput{
  ClientId: aws.String(clientId),
  Username: aws.String(userName),
 })
 if err != nil {
  log.Printf("Couldn't start password reset for user '%v'. Here;s why: %v\n",
 userName, err)
 }
 return output.CodeDeliveryDetails, err
}



// ConfirmForgotPassword confirms a user with a confirmation code and a new
 password.
func (actor CognitoActions) ConfirmForgotPassword(clientId string, code string,
 userName string, password string) error {
 _, err := actor.CognitoClient.ConfirmForgotPassword(context.TODO(),
 &cognitoidentityprovider.ConfirmForgotPasswordInput{
  ClientId:         aws.String(clientId),
  ConfirmationCode: aws.String(code),
  Password:         aws.String(password),
  Username:         aws.String(userName),
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't confirm user %v. Here's why: %v", userName, err)
  }
 }
 return err
}



// DeleteUser removes a user from the user pool.
func (actor CognitoActions) DeleteUser(userAccessToken string) error {
 _, err := actor.CognitoClient.DeleteUser(context.TODO(),
 &cognitoidentityprovider.DeleteUserInput{
```

```
  AccessToken: aws.String(userAccessToken),
 })
 if err != nil {
  log.Printf("Couldn't delete user. Here's why: %v\n", err)
 }
 return err
}



// AdminCreateUser uses administrator credentials to add a user to a user pool.
 This method leaves the user
// in a state that requires they enter a new password next time they sign in.
func (actor CognitoActions) AdminCreateUser(userPoolId string, userName string,
 userEmail string) error {
 _, err := actor.CognitoClient.AdminCreateUser(context.TODO(),
 &cognitoidentityprovider.AdminCreateUserInput{
  UserPoolId:     aws.String(userPoolId),
  Username:       aws.String(userName),
  MessageAction:  types.MessageActionTypeSuppress,
  UserAttributes: []types.AttributeType{{Name: aws.String("email"), Value:
 aws.String(userEmail)}},
 })
 if err != nil {
  var userExists *types.UsernameExistsException
  if errors.As(err, &userExists) {
   log.Printf("User %v already exists in the user pool.", userName)
   err = nil
  } else {
   log.Printf("Couldn't create user %v. Here's why: %v\n", userName, err)
  }
 }
 return err
}



// AdminSetUserPassword uses administrator credentials to set a password for a
 user without requiring a
// temporary password.
func (actor CognitoActions) AdminSetUserPassword(userPoolId string, userName
 string, password string) error {
 _, err := actor.CognitoClient.AdminSetUserPassword(context.TODO(),
 &cognitoidentityprovider.AdminSetUserPasswordInput{
```

```
  Password:   aws.String(password),
  UserPoolId: aws.String(userPoolId),
  Username:   aws.String(userName),
  Permanent:  true,
 })
 if err != nil {
  var invalidPassword *types.InvalidPasswordException
  if errors.As(err, &invalidPassword) {
   log.Println(*invalidPassword.Message)
  } else {
   log.Printf("Couldn't set password for user %v. Here's why: %v\n", userName,
 err)
  }
 }
 return err
}
```

Erstellen Sie eine Struktur, die DynamoDB-Aktionen umschließt.

```
// DynamoActions encapsulates the Amazon Simple Notification Service (Amazon SNS)
 actions
// used in the examples.
type DynamoActions struct {
 DynamoClient *dynamodb.Client
}

// User defines structured user data.
type User struct {
 UserName  string
 UserEmail string
 LastLogin *LoginInfo `dynamodbav:",omitempty"`
}

// LoginInfo defines structured custom login data.
type LoginInfo struct {
 UserPoolId string
 ClientId   string
 Time       string
}
```

```
// UserList defines a list of users.
type UserList struct {
 Users []User
}

// UserNameList returns the usernames contained in a UserList as a list of
 strings.
func (users *UserList) UserNameList() []string {
 names := make([]string, len(users.Users))
 for i := 0; i < len(users.Users); i++ {
  names[i] = users.Users[i].UserName
 }
 return names
}

// PopulateTable adds a set of test users to the table.
func (actor DynamoActions) PopulateTable(tableName string) error {
 var err error
 var item map[string]types.AttributeValue
 var writeReqs []types.WriteRequest
 for i := 1; i < 4; i++ {
  item, err = attributevalue.MarshalMap(User{UserName: fmt.Sprintf("test_user_
%v", i), UserEmail: fmt.Sprintf("test_email_%v@example.com", i)})
  if err != nil {
   log.Printf("Couldn't marshall user into DynamoDB format. Here's why: %v\n",
 err)
   return err
  }
  writeReqs = append(writeReqs, types.WriteRequest{PutRequest:
 &types.PutRequest{Item: item}})
 }
 _, err = actor.DynamoClient.BatchWriteItem(context.TODO(),
 &dynamodb.BatchWriteItemInput{
  RequestItems: map[string][]types.WriteRequest{tableName: writeReqs},
 })
 if err != nil {
  log.Printf("Couldn't populate table %v with users. Here's why: %v\n",
 tableName, err)
 }
 return err
}

// Scan scans the table for all items.
func (actor DynamoActions) Scan(tableName string) (UserList, error) {
```

```
 var userList UserList
 output, err := actor.DynamoClient.Scan(context.TODO(), &dynamodb.ScanInput{
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't scan table %v for items. Here's why: %v\n", tableName,
 err)
 } else {
  err = attributevalue.UnmarshalListOfMaps(output.Items, &userList.Users)
  if err != nil {
   log.Printf("Couldn't unmarshal items into users. Here's why: %v\n", err)
  }
 }
 return userList, err
}

// AddUser adds a user item to a table.
func (actor DynamoActions) AddUser(tableName string, user User) error {
 userItem, err := attributevalue.MarshalMap(user)
 if err != nil {
  log.Printf("Couldn't marshall user to item. Here's why: %v\n", err)
 }
 _, err = actor.DynamoClient.PutItem(context.TODO(), &dynamodb.PutItemInput{
  Item:      userItem,
  TableName: aws.String(tableName),
 })
 if err != nil {
  log.Printf("Couldn't put item in table %v. Here's why: %v", tableName, err)
 }
 return err
}
```

Erstellen Sie eine Struktur, die Logs-Aktionen umschließt CloudWatch .

```
type CloudWatchLogsActions struct {
 CwlClient *cloudwatchlogs.Client
}

// GetLatestLogStream gets the most recent log stream for a Lambda function.
```

```
func (actor CloudWatchLogsActions) GetLatestLogStream(functionName string)
 (types.LogStream, error) {
 var logStream types.LogStream
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.DescribeLogStreams(context.TODO(),
 &cloudwatchlogs.DescribeLogStreamsInput{
  Descending:   aws.Bool(true),
  Limit:        aws.Int32(1),
  LogGroupName: aws.String(logGroupName),
  OrderBy:      types.OrderByLastEventTime,
 })
 if err != nil {
  log.Printf("Couldn't get log streams for log group %v. Here's why: %v\n",
 logGroupName, err)
 } else {
  logStream = output.LogStreams[0]
 }
 return logStream, err
}

// GetLogEvents gets the most recent eventCount events from the specified log
 stream.
func (actor CloudWatchLogsActions) GetLogEvents(functionName string,
 logStreamName string, eventCount int32) (
 []types.OutputLogEvent, error) {
 var events []types.OutputLogEvent
 logGroupName := fmt.Sprintf("/aws/lambda/%s", functionName)
 output, err := actor.CwlClient.GetLogEvents(context.TODO(),
 &cloudwatchlogs.GetLogEventsInput{
  LogStreamName: aws.String(logStreamName),
  Limit:         aws.Int32(eventCount),
  LogGroupName:  aws.String(logGroupName),
 })
 if err != nil {
  log.Printf("Couldn't get log event for log stream %v. Here's why: %v\n",
 logStreamName, err)
 } else {
  events = output.Events
 }
 return events, err
}
```

Erstellen Sie eine Struktur, die Aktionen umschließt. AWS CloudFormation

```
// StackOutputs defines a map of outputs from a specific stack.
type StackOutputs map[string]string

type CloudFormationActions struct {
 CfnClient *cloudformation.Client
}

// GetOutputs gets the outputs from a CloudFormation stack and puts them into a
 structured format.
func (actor CloudFormationActions) GetOutputs(stackName string) StackOutputs {
 output, err := actor.CfnClient.DescribeStacks(context.TODO(),
 &cloudformation.DescribeStacksInput{
  StackName: aws.String(stackName),
 })
 if err != nil || len(output.Stacks) == 0 {
  log.Panicf("Couldn't find a CloudFormation stack named %v. Here's why: %v\n",
 stackName, err)
 }
 stackOutputs := StackOutputs{}
 for _, out := range output.Stacks[0].Outputs {
  stackOutputs[*out.OutputKey] = *out.OutputValue
 }
 return stackOutputs
}
```

Ressourcen bereinigen.

```
// Resources keeps track of AWS resources created during an example and handles
// cleanup when the example finishes.
type Resources struct {
 userPoolId       string
 userAccessTokens []string
 triggers         []actions.Trigger

 cognitoActor *actions.CognitoActions
 questioner   demotools.IQuestioner
}
```

```
func (resources *Resources) init(cognitoActor *actions.CognitoActions, questioner
 demotools.IQuestioner) {
 resources.userAccessTokens = []string{}
 resources.triggers = []actions.Trigger{}
 resources.cognitoActor = cognitoActor
 resources.questioner = questioner
}

// Cleanup deletes all AWS resources created during an example.
func (resources *Resources) Cleanup() {
 defer func() {
  if r := recover(); r != nil {
   log.Printf("Something went wrong during cleanup.\n%v\n", r)
   log.Println("Use the AWS Management Console to remove any remaining resources
 \n" +
    "that were created for this scenario.")
  }
 }()

 wantDelete := resources.questioner.AskBool("Do you want to remove all of the AWS
 resources that were created "+
  "during this demo (y/n)?", "y")
 if wantDelete {
  for _, accessToken := range resources.userAccessTokens {
   err := resources.cognitoActor.DeleteUser(accessToken)
   if err != nil {
    log.Println("Couldn't delete user during cleanup.")
    panic(err)
   }
   log.Println("Deleted user.")
  }
  triggerList := make([]actions.TriggerInfo, len(resources.triggers))
  for i := 0; i < len(resources.triggers); i++ {
   triggerList[i] = actions.TriggerInfo{Trigger: resources.triggers[i],
 HandlerArn: nil}
  }
  err := resources.cognitoActor.UpdateTriggers(resources.userPoolId,
 triggerList...)
  if err != nil {
   log.Println("Couldn't update Cognito triggers during cleanup.")
   panic(err)
  }
  log.Println("Removed Cognito triggers from user pool.")
```

```
 } else {
  log.Println("Be sure to remove resources when you're done with them to avoid
 unexpected charges!")
 }
}
```

- API-Details finden Sie in den folgenden Themen der AWS SDK for Go -API-Referenz.
  - AdminCreateNutzer
  - AdminSetUserPassword
  - DeleteUser
  - InitiateAuth
  - UpdateUserSchwimmbad

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Serverlose Beispiele für Lambda mit SDKs AWS

Die folgenden Codebeispiele zeigen, wie Lambda mit AWS SDKs verwendet wird.

Beispiele

- In einer Lambda-Funktion eine Verbindung zu einer Amazon RDS-Datenbank herstellen
- Aufrufen einer Lambda-Funktion über einen Kinesis-Auslöser
- Rufen Sie eine Lambda-Funktion von einem DynamoDB-Trigger aus auf
- Rufen Sie eine Lambda-Funktion von einem Amazon DocumentDB-Trigger aus auf
- Aufrufen einer Lambda-Funktion über einen Amazon-S3-Auslöser
- Eine Lambda-Funktion über einen Amazon-SNS-Trigger aufrufen
- Aufrufen einer Lambda-Funktion über einen Amazon-SQS-Auslöser
- Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem Kinesis-Auslöser
- Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem DynamoDB-Trigger
- Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem Amazon-SQS-Auslöser

In einer Lambda-Funktion eine Verbindung zu einer Amazon RDS-Datenbank herstellen

Die folgenden Codebeispiele zeigen, wie eine Lambda-Funktion implementiert wird, die eine Verbindung zu einer RDS-Datenbank herstellt. Die Funktion stellt eine einfache Datenbankanfrage und gibt das Ergebnis zurück.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Mit Go eine Verbindung zu einer Amazon RDS-Datenbank in einer Lambda-Funktion herstellen.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Golang v2 code here.
*/

package main

import (
 "context"
 "database/sql"
 "encoding/json"
 "fmt"

 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/feature/rds/auth"
 _ "github.com/go-sql-driver/mysql"
)

type MyEvent struct {
```

```
 Name string `json:"name"`
}

func HandleRequest(event *MyEvent) (map[string]interface{}, error) {

 var dbName string = "DatabaseName"
 var dbUser string = "DatabaseUser"
 var dbHost string = "mysqldb.123456789012.us-east-1.rds.amazonaws.com"
 var dbPort int = 3306
 var dbEndpoint string = fmt.Sprintf("%s:%d", dbHost, dbPort)
 var region string = "us-east-1"

 cfg, err := config.LoadDefaultConfig(context.TODO())
 if err != nil {
  panic("configuration error: " + err.Error())
 }

 authenticationToken, err := auth.BuildAuthToken(
  context.TODO(), dbEndpoint, region, dbUser, cfg.Credentials)
 if err != nil {
  panic("failed to create authentication token: " + err.Error())
 }

 dsn := fmt.Sprintf("%s:%s@tcp(%s)/%s?tls=true&allowCleartextPasswords=true",
  dbUser, authenticationToken, dbEndpoint, dbName,
 )

 db, err := sql.Open("mysql", dsn)
 if err != nil {
  panic(err)
 }

 defer db.Close()

 var sum int
 err = db.QueryRow("SELECT ?+? AS sum", 3, 2).Scan(&sum)
 if err != nil {
  panic(err)
 }
 s := fmt.Sprint(sum)
 message := fmt.Sprintf("The selected sum is: %s", s)

 messageBytes, err := json.Marshal(message)
 if err != nil {
```

```
  return nil, err
 }

 messageString := string(messageBytes)
 return map[string]interface{}{
  "statusCode": 200,
  "headers":    map[string]string{"Content-Type": "application/json"},
  "body":       messageString,
 }, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

JavaScript

SDK für JavaScript (v2)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Herstellen einer Verbindung zu einer Amazon RDS-Datenbank in einer Lambda-Funktion mithilfe von Javascript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
/*
Node.js code here.
*/
// ES6+ example
import { Signer } from "@aws-sdk/rds-signer";
import mysql from 'mysql2/promise';

async function createAuthToken() {
  // Define connection authentication parameters
  const dbinfo = {
```

```
    hostname: process.env.ProxyHostName,
    port: process.env.Port,
    username: process.env.DBUserName,
    region: process.env.AWS_REGION,

  }

  // Create RDS Signer object
  const signer = new Signer(dbinfo);

  // Request authorization token from RDS, specifying the username
  const token = await signer.getAuthToken();
  return token;
}

async function dbOps() {

  // Obtain auth token
  const token = await createAuthToken();
  // Define connection configuration
  let connectionConfig = {
    host: process.env.ProxyHostName,
    user: process.env.DBUserName,
    password: token,
    database: process.env.DBName,
    ssl: 'Amazon RDS'
  }
  // Create the connection to the DB
  const conn = await mysql.createConnection(connectionConfig);
  // Obtain the result of the query
  const [res,] = await conn.execute('select ?+? as sum', [3, 2]);
  return res;

}

export const handler = async (event) => {
  // Execute database flow
  const result = await dbOps();
  // Return result
  return {
    statusCode: 200,
    body: JSON.stringify("The selected sum is: " + result[0].sum)
  }
```

```
};
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Aufrufen einer Lambda-Funktion über einen Kinesis-Auslöser

Die folgenden Codebeispiele veranschaulichen, wie eine Lambda-Funktion implementiert wird, die ein durch den Empfang von Datensätzen aus einem Kinesis-Stream ausgelöstes Ereignis empfängt. Die Funktion ruft die Kinesis-Nutzlast ab, dekodiert von Base64 und protokolliert den Datensatzinhalt.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegrationSampleCode;

public class Function
{
```

```
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task FunctionHandler(KinesisEvent evnt, ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return;
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                throw;
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent) error {
 if len(kinesisEvent.Records) == 0 {
  log.Printf("empty Kinesis event received")
  return nil
 }

 for _, record := range kinesisEvent.Records {
  log.Printf("processed Kinesis event with EventId: %v", record.EventID)
  recordDataBytes := record.Kinesis.Data
  recordDataText := string(recordDataBytes)
  log.Printf("record data: %v", recordDataText)
  // TODO: Do interesting work based on the new data
 }
 log.Printf("successfully processed %v records", len(kinesisEvent.Records))
 return nil
}

func main() {
 lambda.Start(handler)
```

```
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;

public class Handler implements RequestHandler<KinesisEvent, Void> {
    @Override
    public Void handleRequest(final KinesisEvent event, final Context context) {
        LambdaLogger logger = context.getLogger();
        if (event.getRecords().isEmpty()) {
            logger.log("Empty Kinesis Event received");
            return null;
        }
        for (KinesisEvent.KinesisEventRecord record : event.getRecords()) {
            try {
                logger.log("Processed Event with EventId: "+record.getEventID());
                String data = new String(record.getKinesis().getData().array());
                logger.log("Data:"+ data);
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex) {
                logger.log("An error occurred:"+ex.getMessage());
                throw ex;
```

```
            }
        }
        logger.log("Successfully processed:"+event.getRecords().size()+"
 records");
        return null;
    }

}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda unter Verwendung von. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      throw err;
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
```

```
  return data;
}
```

Ein Kinesis-Ereignis mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      throw err;
    }
    logger.info(`Successfully processed ${event.Records.length} records.`);
  }
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
```

```
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda mithilfe von PHP verarbeiten.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Kinesis\KinesisHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends KinesisHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
```

```
     */
    public function handleKinesis(KinesisEvent $event, Context $context): void
    {
        $this->logger->info("Processing records");
        $records = $event->getRecords();
        foreach ($records as $record) {
            $data = $record->getData();
            $this->logger->info(json_encode($data));
            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines Kinesis-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import base64
def lambda_handler(event, context):

    for record in event['Records']:
        try:
            print(f"Processed Kinesis Event - EventID: {record['eventID']}")
```

```
            record_data = base64.b64decode(record['kinesis']
['data']).decode('utf-8')
            print(f"Record Data: {record_data}")
            # TODO: Do interesting work based on the new data
        except Exception as e:
            print(f"An error occurred {e}")
            raise e
    print(f"Successfully processed {len(event['Records'])} records.")
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda unter Verwendung von Ruby verarbeiten.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue => err
      $stderr.puts "An error occurred #{err}"
      raise err
    end
  end
  puts "Successfully processed #{event['Records'].length} records."
end

def get_record_data_async(payload)
```

```
  data = Base64.decode64(payload['data']).force_encoding('UTF-8')
  # Placeholder for actual async work
  # You can use Ruby's asynchronous programming tools like async/await or fibers
 here.
  return data
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein Kinesis-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::kinesis::KinesisEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) -> Result<(), Error>
 {
    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    event.payload.records.iter().for_each(|record| {
        tracing::info!("EventId:
 {}",record.event_id.as_deref().unwrap_or_default());

        let record_data = std::str::from_utf8(&record.kinesis.data);

        match record_data {
            Ok(data) => {
                // log the record data
                tracing::info!("Data: {}", data);
            }
```

```
            Err(e) => {
                tracing::error!("Error: {}", e);
            }
        }
    });

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Rufen Sie eine Lambda-Funktion von einem DynamoDB-Trigger aus auf

Die folgenden Codebeispiele zeigen, wie eine Lambda-Funktion implementiert wird, die ein Ereignis empfängt, das durch den Empfang von Datensätzen aus einem DynamoDB-Stream ausgelöst wird. Die Funktion ruft die DynamoDB-Nutzlast ab und protokolliert den Inhalt des Datensatzes.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von.NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public void FunctionHandler(DynamoDBEvent dynamoEvent, ILambdaContext
 context)
    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");

        foreach (var record in dynamoEvent.Records)
        {
            context.Logger.LogInformation($"Event ID: {record.EventID}");
            context.Logger.LogInformation($"Event Name: {record.EventName}");

            context.Logger.LogInformation(JsonSerializer.Serialize(record));
        }

        context.Logger.LogInformation("Stream processing complete.");
```

```
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-lambda-go/events"
 "fmt"
)

func HandleRequest(ctx context.Context, event events.DynamoDBEvent) (*string,
 error) {
 if len(event.Records) == 0 {
  return nil, fmt.Errorf("received empty event")
 }

 for _, record := range event.Records {
   LogDynamoDBRecord(record)
 }

 message := fmt.Sprintf("Records processed: %d", len(event.Records))
 return &message, nil
}

func main() {
```

```
 lambda.Start(HandleRequest)
}

func LogDynamoDBRecord(record events.DynamoDBEventRecord){
 fmt.Println(record.EventID)
 fmt.Println(record.EventName)
 fmt.Printf("%+v\n", record.Change)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Java.

```
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import
 com.amazonaws.services.lambda.runtime.events.DynamodbEvent.DynamodbStreamRecord;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class example implements RequestHandler<DynamodbEvent, Void> {

    private static final Gson GSON = new
 GsonBuilder().setPrettyPrinting().create();

    @Override
    public Void handleRequest(DynamodbEvent event, Context context) {
        System.out.println(GSON.toJson(event));
        event.getRecords().forEach(this::logDynamoDBRecord);
        return null;
    }

    private void logDynamoDBRecord(DynamodbStreamRecord record) {
```

```
        System.out.println(record.getEventID());
        System.out.println(record.getEventName());
        System.out.println("DynamoDB Record: " +
 GSON.toJson(record.getDynamodb()));
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines DynamoDB-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
};

const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

Konsumieren eines DynamoDB-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event, context) => {
    console.log(JSON.stringify(event, null, 2));
```

```
    event.Records.forEach(record => {
        logDynamoDBRecord(record);
    });
}
const logDynamoDBRecord = (record) => {
    console.log(record.eventID);
    console.log(record.eventName);
    console.log(`DynamoDB Record: ${JSON.stringify(record.dynamodb)}`);
};
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein DynamoDB-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\DynamoDb\DynamoDbHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends DynamoDbHandler
{
    private StderrLogger $logger;

    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
```

```
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleDynamoDb(DynamoDbEvent $event, Context $context): void
    {
        $this->logger->info("Processing DynamoDb table items");
        $records = $event->getRecords();

        foreach ($records as $record) {
            $eventName = $record->getEventName();
            $keys = $record->getKeys();
            $old = $record->getOldImage();
            $new = $record->getNewImage();

            $this->logger->info("Event Name:".$eventName."\n");
            $this->logger->info("Keys:". json_encode($keys)."\n");
            $this->logger->info("Old Image:". json_encode($old)."\n");
            $this->logger->info("New Image:". json_encode($new));

            // TODO: Do interesting work based on the new data

            // Any exception thrown will be logged and the invocation will be
 marked as failed
        }

        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords items");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

import json

def lambda_handler(event, context):
    print(json.dumps(event, indent=2))

    for record in event['Records']:
        log_dynamodb_record(record)

def log_dynamodb_record(record):
    print(record['eventID'])
    print(record['eventName'])
    print(f"DynamoDB Record: {json.dumps(record['dynamodb'])}")
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines DynamoDB-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event:, context:)
    return 'received empty event' if event['Records'].empty?

    event['Records'].each do |record|
      log_dynamodb_record(record)
    end

    "Records processed: #{event['Records'].length}"
  end

  def log_dynamodb_record(record)
    puts record['eventID']
    puts record['eventName']
    puts "DynamoDB Record: #{JSON.generate(record['dynamodb'])}"
  end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein DynamoDB-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

use lambda_runtime::{service_fn, tracing, Error, LambdaEvent};
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord},
   };
```

```
// Built with the following dependencies:
//lambda_runtime = "0.11.1"
//serde_json = "1.0"
//tokio = { version = "1", features = ["macros"] }
//tracing = { version = "0.1", features = ["log"] }
//tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }
//aws_lambda_events = "0.15.0"

async fn function_handler(event: LambdaEvent<Event>) ->Result<(), Error> {

    let records = &event.payload.records;
    tracing::info!("event payload: {:?}",records);
    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(());
    }

    for record in records{
        log_dynamo_dbrecord(record);
    }

    tracing::info!("Dynamo db records processed");

    // Prepare the response
    Ok(())

}

fn log_dynamo_dbrecord(record: &EventRecord)-> Result<(), Error>{
    tracing::info!("EventId: {}", record.event_id);
    tracing::info!("EventName: {}", record.event_name);
    tracing::info!("DynamoDB Record: {:?}", record.change );
    Ok(())

}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
    .with_max_level(tracing::Level::INFO)
    .with_target(false)
    .without_time()
    .init();
```

```
    let func = service_fn(function_handler);
    lambda_runtime::run(func).await?;
    Ok(())

}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Rufen Sie eine Lambda-Funktion von einem Amazon DocumentDB-Trigger aus auf

Die folgenden Codebeispiele zeigen, wie eine Lambda-Funktion implementiert wird, die ein Ereignis empfängt, das durch den Empfang von Datensätzen aus einem DocumentDB-Änderungsstream ausgelöst wird. Die Funktion ruft die DocumentDB-Nutzlast ab und protokolliert den Inhalt des Datensatzes.

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0

package main

import (
 "context"
```

```
 "encoding/json"
 "fmt"

 "github.com/aws/aws-lambda-go/lambda"
)

type Event struct {
 Events []Record `json:"events"`
}

type Record struct {
 Event struct {
  OperationType string `json:"operationType"`
  NS            struct {
   DB   string `json:"db"`
   Coll string `json:"coll"`
  } `json:"ns"`
  FullDocument interface{} `json:"fullDocument"`
 } `json:"event"`
}

func main() {
 lambda.Start(handler)
}

func handler(ctx context.Context, event Event) (string, error) {
 fmt.Println("Loading function")
 for _, record := range event.Events {
  logDocumentDBEvent(record)
 }

 return "OK", nil
}

func logDocumentDBEvent(record Record) {
 fmt.Printf("Operation type: %s\n", record.Event.OperationType)
 fmt.Printf("db: %s\n", record.Event.NS.DB)
 fmt.Printf("collection: %s\n", record.Event.NS.Coll)
 docBytes, _ := json.MarshalIndent(record.Event.FullDocument, "", "  ")
 fmt.Printf("Full document: %s\n", string(docBytes))
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda. JavaScript

```
console.log('Loading function');
exports.handler = async (event, context) => {
    event.events.forEach(record => {
        logDocumentDBEvent(record);
    });
    return 'OK';
};

const logDocumentDBEvent = (record) => {
    console.log('Operation type: ' + record.event.operationType);
    console.log('db: ' + record.event.ns.db);
    console.log('collection: ' + record.event.ns.coll);
    console.log('Full document:', JSON.stringify(record.event.fullDocument, null,
 2));
};
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda mithilfe von Python.

```
import json

def lambda_handler(event, context):
    for record in event.get('events', []):
        log_document_db_event(record)
    return 'OK'

def log_document_db_event(record):
    event_data = record.get('event', {})
    operation_type = event_data.get('operationType', 'Unknown')
    db = event_data.get('ns', {}).get('db', 'Unknown')
    collection = event_data.get('ns', {}).get('coll', 'Unknown')
    full_document = event_data.get('fullDocument', {})

    print(f"Operation type: {operation_type}")
    print(f"db: {db}")
    print(f"collection: {collection}")
    print("Full document:", json.dumps(full_document, indent=2))
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines Amazon DocumentDB DocumentDB-Ereignisses mit Lambda unter Verwendung von Ruby.

```
require 'json'

def lambda_handler(event:, context:)
  event['events'].each do |record|
    log_document_db_event(record)
  end
```

```
  'OK'
end

def log_document_db_event(record)
  event_data = record['event'] || {}
  operation_type = event_data['operationType'] || 'Unknown'
  db = event_data.dig('ns', 'db') || 'Unknown'
  collection = event_data.dig('ns', 'coll') || 'Unknown'
  full_document = event_data['fullDocument'] || {}

  puts "Operation type: #{operation_type}"
  puts "db: #{db}"
  puts "collection: #{collection}"
  puts "Full document: #{JSON.pretty_generate(full_document)}"
end
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Aufrufen einer Lambda-Funktion über einen Amazon-S3-Auslöser

In den folgenden Codebeispiele wird die Implementierung einer Lambda-Funktion gezeigt, die ein Ereignis empfängt, das durch Hochladen eines Objekts in einen S3-Bucket ausgelöst wird. Die Funktion ruft den Namen des S3-Buckets sowie den Objektschlüssel aus dem Ereignisparameter ab und ruft die Amazon-S3-API auf, um den Inhaltstyp des Objekts abzurufen und zu protokollieren.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von .NET

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
```

```
// SPDX-License-Identifier: Apache-2.0
using System.Threading.Tasks;
using Amazon.Lambda.Core;
using Amazon.S3;
using System;
using Amazon.Lambda.S3Events;
using System.Web;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace S3Integration
{
    public class Function
    {
        private static AmazonS3Client _s3Client;
        public Function() : this(null)
        {
        }

        internal Function(AmazonS3Client s3Client)
        {
            _s3Client = s3Client ?? new AmazonS3Client();
        }

        public async Task<string> Handler(S3Event evt, ILambdaContext context)
        {
            try
            {
                if (evt.Records.Count <= 0)
                {
                    context.Logger.LogLine("Empty S3 Event received");
                    return string.Empty;
                }

                var bucket = evt.Records[0].S3.Bucket.Name;
                var key = HttpUtility.UrlDecode(evt.Records[0].S3.Object.Key);

                context.Logger.LogLine($"Request is for {bucket} and {key}");

                var objectResult = await _s3Client.GetObjectAsync(bucket, key);
```

```
                context.Logger.LogLine($"Returning {objectResult.Key}");

                return objectResult.Key;
            }
            catch (Exception e)
            {
                context.Logger.LogLine($"Error processing request -
 {e.Message}");

                return string.Empty;
            }
        }
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Go

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "log"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)

func handler(ctx context.Context, s3Event events.S3Event) error {
```

```
 sdkConfig, err := config.LoadDefaultConfig(ctx)
 if err != nil {
  log.Printf("failed to load default config: %s", err)
  return err
 }
 s3Client := s3.NewFromConfig(sdkConfig)

 for _, record := range s3Event.Records {
  bucket := record.S3.Bucket.Name
  key := record.S3.Object.URLDecodedKey
  headOutput, err := s3Client.HeadObject(ctx, &s3.HeadObjectInput{
   Bucket: &bucket,
   Key:    &key,
  })
  if err != nil {
   log.Printf("error getting head of object %s/%s: %s", bucket, key, err)
   return err
  }
  log.Printf("successfully retrieved %s/%s of type %s", bucket, key,
 *headOutput.ContentType)
 }

 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Java

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import software.amazon.awssdk.services.s3.model.HeadObjectRequest;
import software.amazon.awssdk.services.s3.model.HeadObjectResponse;
import software.amazon.awssdk.services.s3.S3Client;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.S3Event;
import
 com.amazonaws.services.lambda.runtime.events.models.s3.S3EventNotification.S3EventNotifi

import org.slf4j.Logger;
import org.slf4j.LoggerFactory;

public class Handler implements RequestHandler<S3Event, String> {
    private static final Logger logger = LoggerFactory.getLogger(Handler.class);
    @Override
    public String handleRequest(S3Event s3event, Context context) {
        try {
          S3EventNotificationRecord record = s3event.getRecords().get(0);
          String srcBucket = record.getS3().getBucket().getName();
          String srcKey = record.getS3().getObject().getUrlDecodedKey();

          S3Client s3Client = S3Client.builder().build();
          HeadObjectResponse headObject = getHeadObject(s3Client, srcBucket,
 srcKey);

          logger.info("Successfully retrieved " + srcBucket + "/" + srcKey + " of
 type " + headObject.contentType());

          return "Ok";
        } catch (Exception e) {
          throw new RuntimeException(e);
        }
    }

    private HeadObjectResponse getHeadObject(S3Client s3Client, String bucket,
 String key) {
        HeadObjectRequest headObjectRequest = HeadObjectRequest.builder()
                .bucket(bucket)
```

```
                .key(key)
                .build();
        return s3Client.headObject(headObjectRequest);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines S3-Ereignisses mit Lambda unter Verwendung JavaScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Client, HeadObjectCommand } from "@aws-sdk/client-s3";

const client = new S3Client();

exports.handler = async (event, context) => {

    // Get the object from the event and show its content type
    const bucket = event.Records[0].s3.bucket.name;
    const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g,
 ' '));

    try {
        const { ContentType } = await client.send(new HeadObjectCommand({
            Bucket: bucket,
            Key: key,
        }));

        console.log('CONTENT TYPE:', ContentType);
        return ContentType;

    } catch (err) {
        console.log(err);
```

```
        const message = `Error getting object ${key} from bucket ${bucket}. Make
 sure they exist and your bucket is in the same region as this function.`;
        console.log(message);
        throw new Error(message);
    }
};
```

Konsumieren eines S3-Ereignisses mit Lambda unter Verwendung TypeScript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { S3Event } from 'aws-lambda';
import { S3Client, HeadObjectCommand } from '@aws-sdk/client-s3';

const s3 = new S3Client({ region: process.env.AWS_REGION });

export const handler = async (event: S3Event): Promise<string | undefined> => {
  // Get the object from the event and show its content type
  const bucket = event.Records[0].s3.bucket.name;
  const key = decodeURIComponent(event.Records[0].s3.object.key.replace(/\+/g, '
 '));
  const params = {
    Bucket: bucket,
    Key: key,
  };
  try {
    const { ContentType } = await s3.send(new HeadObjectCommand(params));
    console.log('CONTENT TYPE:', ContentType);
    return ContentType;
  } catch (err) {
    console.log(err);
    const message = `Error getting object ${key} from bucket ${bucket}. Make sure
 they exist and your bucket is in the same region as this function.`;
    console.log(message);
    throw new Error(message);
  }
};
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein S3-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\S3\S3Event;
use Bref\Event\S3\S3Handler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';


class Handler extends S3Handler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    public function handleS3(S3Event $event, Context $context) : void
    {
        $this->logger->info("Processing S3 records");

        // Get the object from the event and show its content type
        $records = $event->getRecords();

        foreach ($records as $record)
        {
            $bucket = $record->getBucket()->getName();
            $key = urldecode($record->getObject()->getKey());
```

```
            try {
                $fileSize = urldecode($record->getObject()->getSize());
                echo "File Size: " . $fileSize . "\n";
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                echo $e->getMessage() . "\n";
                echo 'Error getting object ' . $key . ' from bucket ' .
 $bucket . '. Make sure they exist and your bucket is in the same region as this
 function.' . "\n";
                throw $e;
            }
        }
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Python

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
import json
import urllib.parse
import boto3

print('Loading function')

s3 = boto3.client('s3')
```

```
def lambda_handler(event, context):
    #print("Received event: " + json.dumps(event, indent=2))

    # Get the object from the event and show its content type
    bucket = event['Records'][0]['s3']['bucket']['name']
    key = urllib.parse.unquote_plus(event['Records'][0]['s3']['object']['key'],
 encoding='utf-8')
    try:
        response = s3.get_object(Bucket=bucket, Key=key)
        print("CONTENT TYPE: " + response['ContentType'])
        return response['ContentType']
    except Exception as e:
        print(e)
        print('Error getting object {} from bucket {}. Make sure they exist and
 your bucket is in the same region as this function.'.format(key, bucket))
        raise e
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein S3-Ereignis mit Lambda unter Verwendung von Ruby konsumieren.

```
require 'json'
require 'uri'
require 'aws-sdk'

puts 'Loading function'

def lambda_handler(event:, context:)
  s3 = Aws::S3::Client.new(region: 'region') # Your AWS region
  # puts "Received event: #{JSON.dump(event)}"

  # Get the object from the event and show its content type
```

```
  bucket = event['Records'][0]['s3']['bucket']['name']
  key = URI.decode_www_form_component(event['Records'][0]['s3']['object']['key'],
 Encoding::UTF_8)
  begin
    response = s3.get_object(bucket: bucket, key: key)
    puts "CONTENT TYPE: #{response.content_type}"
    return response.content_type
  rescue StandardError => e
    puts e.message
    puts "Error getting object #{key} from bucket #{bucket}. Make sure they exist
 and your bucket is in the same region as this function."
    raise e
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines S3-Ereignisses mit Lambda unter Verwendung von Rust

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::s3::S3Event;
use aws_sdk_s3::{Client};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};


/// Main function
#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
```

```
        .init();

    // Initialize the AWS SDK for Rust
    let config = aws_config::load_from_env().await;
    let s3_client = Client::new(&config);

    let res = run(service_fn(|request: LambdaEvent<S3Event>| {
        function_handler(&s3_client, request)
    })).await;

    res
}

async fn function_handler(
    s3_client: &Client,
    evt: LambdaEvent<S3Event>
) -> Result<(), Error> {
    tracing::info!(records = ?evt.payload.records.len(), "Received request from
 SQS");

    if evt.payload.records.len() == 0 {
        tracing::info!("Empty S3 event received");
    }

    let bucket = evt.payload.records[0].s3.bucket.name.as_ref().expect("Bucket
 name to exist");
    let key = evt.payload.records[0].s3.object.key.as_ref().expect("Object key to
 exist");

    tracing::info!("Request is for {} and object {}", bucket, key);

    let s3_get_object_result = s3_client
        .get_object()
        .bucket(bucket)
        .key(key)
        .send()
        .await;

    match s3_get_object_result {
        Ok(_) => tracing::info!("S3 Get Object success, the s3GetObjectResult
 contains a 'body' property of type ByteStream"),
        Err(_) => tracing::info!("Failure with S3 Get Object request")
    }
```

```
    Ok(())
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Eine Lambda-Funktion über einen Amazon-SNS-Trigger aufrufen

In den folgenden Codebeispiele wird die Implementierung einer Lambda-Funktion veranschaulicht, die ein Ereignis empfängt, das durch das Empfangen von Nachrichten aus einem SNS-Thema ausgelöst wird. Die Funktion ruft die Nachrichten aus dem Ereignisparameter ab und protokolliert den Inhalt jeder Nachricht.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SNSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SnsIntegration;

public class Function
```

```
{
    public async Task FunctionHandler(SNSEvent evnt, ILambdaContext context)
    {
        foreach (var record in evnt.Records)
        {
            await ProcessRecordAsync(record, context);
        }
        context.Logger.LogInformation("done");
    }

    private async Task ProcessRecordAsync(SNSEvent.SNSRecord record,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed record
 {record.Sns.Message}");

            // TODO: Do interesting work based on the new message
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"

 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, snsEvent events.SNSEvent) {
 for _, record := range snsEvent.Records {
  processMessage(record)
 }
 fmt.Println("done")
}

func processMessage(record events.SNSEventRecord) {
 message := record.SNS.Message
 fmt.Printf("Processed message: %s\n", message)
 // TODO: Process your record here
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines SNS-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.LambdaLogger;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SNSEvent;
import com.amazonaws.services.lambda.runtime.events.SNSEvent.SNSRecord;


import java.util.Iterator;
import java.util.List;

public class SNSEventHandler implements RequestHandler<SNSEvent, Boolean> {
    LambdaLogger logger;

    @Override
    public Boolean handleRequest(SNSEvent event, Context context) {
        logger = context.getLogger();
        List<SNSRecord> records = event.getRecords();
        if (!records.isEmpty()) {
            Iterator<SNSRecord> recordsIter = records.iterator();
            while (recordsIter.hasNext()) {
                processRecord(recordsIter.next());
            }
        }
        return Boolean.TRUE;
    }

    public void processRecord(SNSRecord record) {
        try {
            String message = record.getSNS().getMessage();
            logger.log("message: " + message);
        } catch (Exception e) {
            throw new RuntimeException(e);
        }
    }

}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines SNS-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record) {
  try {
    const message = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Konsumieren eines SNS-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SNSEvent, Context, SNSHandler, SNSEventRecord } from "aws-lambda";
```

```
export const functionHandler: SNSHandler = async (
  event: SNSEvent,
  context: Context
): Promise<void> => {
  for (const record of event.Records) {
    await processMessageAsync(record);
  }
  console.info("done");
};

async function processMessageAsync(record: SNSEventRecord): Promise<any> {
  try {
    const message: string = JSON.stringify(record.Sns.Message);
    console.log(`Processed message ${message}`);
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von PHP

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

/*
Since native PHP support for AWS Lambda is not available, we are utilizing Bref's
 PHP functions runtime for AWS Lambda.
```

```
For more information on Bref's PHP runtime for Lambda, refer to: https://bref.sh/
docs/runtimes/function

Another approach would be to create a custom runtime.
A practical example can be found here: https://aws.amazon.com/blogs/apn/aws-
lambda-custom-runtime-for-php-a-practical-example/
*/

// Additional composer packages may be required when using Bref or any other PHP
 functions runtime.
// require __DIR__ . '/vendor/autoload.php';

use Bref\Context\Context;
use Bref\Event\Sns\SnsEvent;
use Bref\Event\Sns\SnsHandler;

class Handler extends SnsHandler
{
    public function handleSns(SnsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $message = $record->getMessage();

            // TODO: Implement your custom processing logic here
            // Any exception thrown will be logged and the invocation will be
 marked as failed

            echo "Processed Message: $message" . PHP_EOL;
        }
    }
}

return new Handler();
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for record in event['Records']:
        process_message(record)
    print("done")

def process_message(record):
    try:
        message = record['Sns']['Message']
        print(f"Processed message {message}")
        # TODO; Process your record here

    except Exception as e:
        print("An error occurred")
        raise e
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Verwenden eines SNS-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].map { |record| process_message(record) }
end

def process_message(record)
  message = record['Sns']['Message']
  puts("Processing message: #{message}")
rescue StandardError => e
  puts("Error processing message: #{e}")
  raise
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SNS-Ereignisses mit Lambda unter Verwendung von Rust

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sns::SnsEvent;
use aws_lambda_events::sns::SnsRecord;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
use tracing::info;

// Built with the following dependencies:
//  aws_lambda_events = { version = "0.10.0", default-features = false, features
 = ["sns"] }
//  lambda_runtime = "0.8.1"
//  tokio = { version = "1", features = ["macros"] }
```

```
//  tracing = { version = "0.1", features = ["log"] }
//  tracing-subscriber = { version = "0.3", default-features = false, features =
 ["fmt"] }

async fn function_handler(event: LambdaEvent<SnsEvent>) -> Result<(), Error> {
    for event in event.payload.records {
        process_record(&event)?;
    }

    Ok(())
}

fn process_record(record: &SnsRecord) -> Result<(), Error> {
    info!("Processing SNS Message: {}", record.sns.message);

    // Implement your record handling code here.

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        .with_target(false)
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Aufrufen einer Lambda-Funktion über einen Amazon-SQS-Auslöser

Die folgenden Codebeispiele zeigen, wie eine Lambda-Funktion implementiert wird, die ein Ereignis empfängt, das durch den Empfang von Nachrichten aus einer SQS-Warteschlange ausgelöst wird. Die Funktion ruft die Nachrichten aus dem Ereignisparameter ab und protokolliert den Inhalt jeder Nachricht.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;


// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace SqsIntegrationSampleCode
{
    public async Task FunctionHandler(SQSEvent evnt, ILambdaContext context)
    {
        foreach (var message in evnt.Records)
        {
            await ProcessMessageAsync(message, context);
        }

        context.Logger.LogInformation("done");
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        try
        {
            context.Logger.LogInformation($"Processed message {message.Body}");

            // TODO: Do interesting work based on the new message
```

```
            await Task.CompletedTask;
        }
        catch (Exception e)
        {
            //You can use Dead Letter Queue to handle failures. By configuring a
 Lambda DLQ.
            context.Logger.LogError($"An error occurred");
            throw;
        }

    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package integration_sqs_to_lambda

import (
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(event events.SQSEvent) error {
 for _, record := range event.Records {
  err := processMessage(record)
  if err != nil {
   return err
  }
```

```
 }
 fmt.Println("done")
 return nil
}

func processMessage(record events.SQSMessage) error {
 fmt.Printf("Processed message %s\n", record.Body)
 // TODO: Do interesting work based on the new message
 return nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSEvent.SQSMessage;

public class Function implements RequestHandler<SQSEvent, Void> {
    @Override
    public Void handleRequest(SQSEvent sqsEvent, Context context) {
        for (SQSMessage msg : sqsEvent.getRecords()) {
            processMessage(msg, context);
        }
        context.getLogger().log("done");
```

```
        return null;
    }

    private void processMessage(SQSMessage msg, Context context) {
        try {
            context.getLogger().log("Processed message " + msg.getBody());

            // TODO: Do interesting work based on the new message

        } catch (Exception e) {
            context.getLogger().log("An error occurred");
            throw e;
        }

    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Konsumieren eines SQS-Ereignisses mit Lambda unter Verwendung. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message) {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
```

```
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

Konsumieren eines SQS-Ereignisses mit Lambda unter Verwendung. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, Context, SQSHandler, SQSRecord } from "aws-lambda";

export const functionHandler: SQSHandler = async (
  event: SQSEvent,
  context: Context
): Promise<void> => {
  for (const message of event.Records) {
    await processMessageAsync(message);
  }
  console.info("done");
};

async function processMessageAsync(message: SQSRecord): Promise<any> {
  try {
    console.log(`Processed message ${message.body}`);
    // TODO: Do interesting work based on the new message
    await Promise.resolve(1); //Placeholder for actual async work
  } catch (err) {
    console.error("An error occurred");
    throw err;
  }
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein SQS-Ereignis mit Lambda mithilfe von PHP konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\InvalidLambdaEvent;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
        foreach ($event->getRecords() as $record) {
            $body = $record->getBody();
            // TODO: Do interesting work based on the new message
        }
```

```
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event, context):
    for message in event['Records']:
        process_message(message)
    print("done")

def process_message(message):
    try:
        print(f"Processed message {message['body']}")
        # TODO: Do interesting work based on the new message
    except Exception as err:
        print("An error occurred")
        raise err
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Nutzen eines SQS-Ereignisses mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
  event['Records'].each do |message|
    process_message(message)
  end
  puts "done"
end

def process_message(message)
  begin
    puts "Processed message #{message['body']}"
    # TODO: Do interesting work based on the new message
  rescue StandardError => err
    puts "An error occurred"
    raise err
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Ein SQS-Ereignis mit Lambda mithilfe von Rust konsumieren.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::event::sqs::SqsEvent;
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<SqsEvent>) -> Result<(), Error> {
    event.payload.records.iter().for_each(|record| {
        // process the record
        tracing::info!("Message body: {}",
 record.body.as_deref().unwrap_or_default())
    });

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem Kinesis-Auslöser

Die folgenden Codebeispiele zeigen, wie eine teilweise Batch-Antwort für Lambda-Funktionen implementiert wird, die Ereignisse von einem Kinesis-Stream empfangen. Die Funktion meldet die

Batch-Elementfehler in der Antwort und signalisiert Lambda, diese Nachrichten später erneut zu versuchen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text;
using System.Text.Json.Serialization;
using Amazon.Lambda.Core;
using Amazon.Lambda.KinesisEvents;
using AWS.Lambda.Powertools.Logging;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace KinesisIntegration;

public class Function
{
    // Powertools Logger requires an environment variables against your function
    // POWERTOOLS_SERVICE_NAME
    [Logging(LogEvent = true)]
    public async Task<StreamsEventResponse> FunctionHandler(KinesisEvent evnt,
 ILambdaContext context)
    {
        if (evnt.Records.Count == 0)
        {
            Logger.LogInformation("Empty Kinesis Event received");
            return new StreamsEventResponse();
```

```
        }

        foreach (var record in evnt.Records)
        {
            try
            {
                Logger.LogInformation($"Processed Event with EventId:
 {record.EventId}");
                string data = await GetRecordDataAsync(record.Kinesis, context);
                Logger.LogInformation($"Data: {data}");
                // TODO: Do interesting work based on the new data
            }
            catch (Exception ex)
            {
                Logger.LogError($"An error occurred {ex.Message}");
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                return new StreamsEventResponse
                {
                    BatchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>
                    {
                        new StreamsEventResponse.BatchItemFailure
 { ItemIdentifier = record.Kinesis.SequenceNumber }
                    }
                };
            }
        }
        Logger.LogInformation($"Successfully processed {evnt.Records.Count}
 records.");
        return new StreamsEventResponse();
    }

    private async Task<string> GetRecordDataAsync(KinesisEvent.Record record,
 ILambdaContext context)
    {
        byte[] bytes = record.Data.ToArray();
        string data = Encoding.UTF8.GetString(bytes);
        await Task.CompletedTask; //Placeholder for actual async work
        return data;
    }
}
```

```
public class StreamsEventResponse
{
    [JsonPropertyName("batchItemFailures")]
    public IList<BatchItemFailure> BatchItemFailures { get; set; }
    public class BatchItemFailure
    {
        [JsonPropertyName("itemIdentifier")]
        public string ItemIdentifier { get; set; }
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Artikeln mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

func handler(ctx context.Context, kinesisEvent events.KinesisEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, record := range kinesisEvent.Records {
  curRecordSequenceNumber := ""
```

```
  // Process your record
  if /* Your record processing condition here */ {
   curRecordSequenceNumber = record.Kinesis.SequenceNumber
  }

  // Add a condition to check if the record processing failed
  if curRecordSequenceNumber != "" {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": curRecordSequenceNumber})
  }
 }

 kinesisBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return kinesisBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.KinesisEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
```

```
import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessKinesisRecords implements RequestHandler<KinesisEvent,
 StreamsEventResponse> {

    @Override
    public StreamsEventResponse handleRequest(KinesisEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (KinesisEvent.KinesisEventRecord kinesisEventRecord :
 input.getRecords()) {
            try {
                //Process your record
                KinesisEvent.Record kinesisRecord =
 kinesisEventRecord.getKinesis();
                curRecordSequenceNumber = kinesisRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse(batchItemFailures);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Javascript.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
exports.handler = async (event, context) => {
  for (const record of event.Records) {
    try {
      console.log(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      console.log(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      console.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
  console.log(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(payload) {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import {
  KinesisStreamEvent,
  Context,
  KinesisStreamHandler,
  KinesisStreamRecordPayload,
  KinesisStreamBatchResponse,
} from "aws-lambda";
import { Buffer } from "buffer";
import { Logger } from "@aws-lambda-powertools/logger";

const logger = new Logger({
  logLevel: "INFO",
  serviceName: "kinesis-stream-handler-sample",
});

export const functionHandler: KinesisStreamHandler = async (
  event: KinesisStreamEvent,
  context: Context
): Promise<KinesisStreamBatchResponse> => {
  for (const record of event.Records) {
    try {
      logger.info(`Processed Kinesis Event - EventID: ${record.eventID}`);
      const recordData = await getRecordDataAsync(record.kinesis);
      logger.info(`Record Data: ${recordData}`);
      // TODO: Do interesting work based on the new data
    } catch (err) {
      logger.error(`An error occurred ${err}`);
      /* Since we are working with streams, we can return the failed item
 immediately.
           Lambda will immediately begin to retry processing from this failed
 item onwards. */
      return {
        batchItemFailures: [{ itemIdentifier: record.kinesis.sequenceNumber }],
      };
    }
  }
```

```
  logger.info(`Successfully processed ${event.Records.length} records.`);
  return { batchItemFailures: [] };
};

async function getRecordDataAsync(
  payload: KinesisStreamRecordPayload
): Promise<string> {
  var data = Buffer.from(payload.data, "base64").toString("utf-8");
  await Promise.resolve(1); //Placeholder for actual async work
  return data;
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\Kinesis\KinesisEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
```

```
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
    {
        $kinesisEvent = new KinesisEvent($event);
        $this->logger->info("Processing records");
        $records = $kinesisEvent->getRecords();

        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei Kinesis-Batchelementen mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["kinesis"]["sequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'aws-sdk'

def lambda_handler(event:, context:)
  batch_item_failures = []

  event['Records'].each do |record|
    begin
      puts "Processed Kinesis Event - EventID: #{record['eventID']}"
      record_data = get_record_data_async(record['kinesis'])
      puts "Record Data: #{record_data}"
      # TODO: Do interesting work based on the new data
    rescue StandardError => err
      puts "An error occurred #{err}"
      # Since we are working with streams, we can return the failed item
 immediately.
      # Lambda will immediately begin to retry processing from this failed item
 onwards.
      return { batchItemFailures: [{ itemIdentifier: record['kinesis']
['sequenceNumber'] }] }
    end
  end

  puts "Successfully processed #{event['Records'].length} records."
  { batchItemFailures: batch_item_failures }
end

def get_record_data_async(payload)
  data = Base64.decode64(payload['data']).force_encoding('utf-8')
  # Placeholder for actual async work
```

```
  sleep(1)
  data
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern Kinesis Kinesis-Batch-Elementen mit Lambda mithilfe von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::kinesis::KinesisEvent,
    kinesis::KinesisEventRecord,
    streams::{KinesisBatchItemFailure, KinesisEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn function_handler(event: LambdaEvent<KinesisEvent>) ->
 Result<KinesisEventResponse, Error> {
    let mut response = KinesisEventResponse {
        batch_item_failures: vec![],
    };

    if event.payload.records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in &event.payload.records {
        tracing::info!(
            "EventId: {}",
            record.event_id.as_deref().unwrap_or_default()
        );
```

```
        let record_processing_result = process_record(record);

        if record_processing_result.is_err() {
            response.batch_item_failures.push(KinesisBatchItemFailure {
                item_identifier: record.kinesis.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!(
        "Successfully processed {} records",
        event.payload.records.len()
    );

    Ok(response)
}

fn process_record(record: &KinesisEventRecord) -> Result<(), Error> {
    let record_data = std::str::from_utf8(record.kinesis.data.as_slice());

    if let Some(err) = record_data.err() {
        tracing::error!("Error: {}", err);
        return Err(Error::from(err));
    }

    let record_data = record_data.unwrap_or_default();

    // do something interesting with the data
    tracing::info!("Data: {}", record_data);

    Ok(())
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
```

```
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem DynamoDB-Trigger

Die folgenden Codebeispiele zeigen, wie eine partielle Batch-Antwort für Lambda-Funktionen implementiert wird, die Ereignisse aus einem DynamoDB-Stream empfangen. Die Funktion meldet die Batch-Elementfehler in der Antwort und signalisiert Lambda, diese Nachrichten später erneut zu versuchen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von.NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using System.Text.Json;
using System.Text;
using Amazon.Lambda.Core;
using Amazon.Lambda.DynamoDBEvents;
```

```
// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri

namespace AWSLambda_DDB;

public class Function
{
    public StreamsEventResponse FunctionHandler(DynamoDBEvent dynamoEvent,
 ILambdaContext context)

    {
        context.Logger.LogInformation($"Beginning to process
 {dynamoEvent.Records.Count} records...");
        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 List<StreamsEventResponse.BatchItemFailure>();
        StreamsEventResponse streamsEventResponse = new StreamsEventResponse();

        foreach (var record in dynamoEvent.Records)
        {
            try
            {
                var sequenceNumber = record.Dynamodb.SequenceNumber;
                context.Logger.LogInformation(sequenceNumber);
            }
            catch (Exception ex)
            {
                context.Logger.LogError(ex.Message);
                batchItemFailures.Add(new StreamsEventResponse.BatchItemFailure()
 { ItemIdentifier = record.Dynamodb.SequenceNumber });
            }
        }

        if (batchItemFailures.Count > 0)
        {
            streamsEventResponse.BatchItemFailures = batchItemFailures;
        }

        context.Logger.LogInformation("Stream processing complete.");
        return streamsEventResponse;
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)

type BatchItemFailure struct {
 ItemIdentifier string `json:"ItemIdentifier"`
}

type BatchResult struct {
 BatchItemFailures []BatchItemFailure `json:"BatchItemFailures"`
}

func HandleRequest(ctx context.Context, event events.DynamoDBEvent)
 (*BatchResult, error) {
 var batchItemFailures []BatchItemFailure
 curRecordSequenceNumber := ""

 for _, record := range event.Records {
  // Process your record
  curRecordSequenceNumber = record.Change.SequenceNumber
 }

 if curRecordSequenceNumber != "" {
  batchItemFailures = append(batchItemFailures, BatchItemFailure{ItemIdentifier:
 curRecordSequenceNumber})
```

```
 }

 batchResult := BatchResult{
  BatchItemFailures: batchItemFailures,
 }

 return &batchResult, nil
}

func main() {
 lambda.Start(HandleRequest)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.DynamodbEvent;
import com.amazonaws.services.lambda.runtime.events.StreamsEventResponse;
import com.amazonaws.services.lambda.runtime.events.models.dynamodb.StreamRecord;

import java.io.Serializable;
import java.util.ArrayList;
import java.util.List;

public class ProcessDynamodbRecords implements RequestHandler<DynamodbEvent,
 Serializable> {

    @Override
```

```
    public StreamsEventResponse handleRequest(DynamodbEvent input, Context
 context) {

        List<StreamsEventResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<>();
        String curRecordSequenceNumber = "";

        for (DynamodbEvent.DynamodbStreamRecord dynamodbStreamRecord :
 input.getRecords()) {
          try {
                //Process your record
                StreamRecord dynamodbRecord = dynamodbStreamRecord.getDynamodb();
                curRecordSequenceNumber = dynamodbRecord.getSequenceNumber();

            } catch (Exception e) {
                /* Since we are working with streams, we can return the failed
 item immediately.
                   Lambda will immediately begin to retry processing from this
 failed item onwards. */
                batchItemFailures.add(new
 StreamsEventResponse.BatchItemFailure(curRecordSequenceNumber));
                return new StreamsEventResponse(batchItemFailures);
            }
        }

       return new StreamsEventResponse();
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda unter Verwendung von. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event) => {
  const records = event.Records;
  let curRecordSequenceNumber = "";

  for (const record of records) {
    try {
      // Process your record
      curRecordSequenceNumber = record.dynamodb.SequenceNumber;
    } catch (e) {
      // Return failed record's sequence number
      return { batchItemFailures: [{ itemIdentifier:
 curRecordSequenceNumber }] };
    }
  }

  return { batchItemFailures: [] };
};
```

Melden von DynamoDB-Batchelementfehlern mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { DynamoDBBatchItemFailure, DynamoDBStreamEvent } from "aws-lambda";

export const handler = async (event: DynamoDBStreamEvent):
 Promise<DynamoDBBatchItemFailure[]> => {

    const batchItemsFailures: DynamoDBBatchItemFailure[] = []
    let curRecordSequenceNumber

    for(const record of event.Records) {
        curRecordSequenceNumber = record.dynamodb?.SequenceNumber

        if(curRecordSequenceNumber) {
            batchItemsFailures.push({
                itemIdentifier: curRecordSequenceNumber
            })
        }
    }
```

```
    return batchItemsFailures
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von PHP.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
<?php

# using bref/bref and bref/logger for simplicity

use Bref\Context\Context;
use Bref\Event\DynamoDb\DynamoDbEvent;
use Bref\Event\Handler as StdHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler implements StdHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handle(mixed $event, Context $context): array
```

```
    {
        $dynamoDbEvent = new DynamoDbEvent($event);
        $this->logger->info("Processing records");

        $records = $dynamoDbEvent->getRecords();
        $failedRecords = [];
        foreach ($records as $record) {
            try {
                $data = $record->getData();
                $this->logger->info(json_encode($data));
                // TODO: Do interesting work based on the new data
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $failedRecords[] = $record->getSequenceNumber();
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords records");

        // change format for the response
        $failures = array_map(
            fn(string $sequenceNumber) => ['itemIdentifier' => $sequenceNumber],
            $failedRecords
        );

        return [
            'batchItemFailures' => $failures
        ];
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def handler(event, context):
    records = event.get("Records")
    curRecordSequenceNumber = ""

    for record in records:
        try:
            # Process your record
            curRecordSequenceNumber = record["dynamodb"]["SequenceNumber"]
        except Exception as e:
            # Return failed record's sequence number
            return {"batchItemFailures":[{"itemIdentifier":
 curRecordSequenceNumber}]}

    return {"batchItemFailures":[]}
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
def lambda_handler(event:, context:)
    records = event["Records"]
    cur_record_sequence_number = ""

    records.each do |record|
      begin
        # Process your record
        cur_record_sequence_number = record["dynamodb"]["SequenceNumber"]
      rescue StandardError => e
        # Return failed record's sequence number
        return {"batchItemFailures" => [{"itemIdentifier" =>
 cur_record_sequence_number}]}
      end
    end

    {"batchItemFailures" => []}
  end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von DynamoDB-Batchelementfehlern mit Lambda mithilfe von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::dynamodb::{Event, EventRecord, StreamRecord},
    streams::{DynamoDbBatchItemFailure, DynamoDbEventResponse},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};
```

```
/// Process the stream record
fn process_record(record: &EventRecord) -> Result<(), Error> {
    let stream_record: &StreamRecord = &record.change;

    // process your stream record here...
    tracing::info!("Data: {:?}", stream_record);

    Ok(())
}

/// Main Lambda handler here...
async fn function_handler(event: LambdaEvent<Event>) ->
 Result<DynamoDbEventResponse, Error> {
    let mut response = DynamoDbEventResponse {
        batch_item_failures: vec![],
    };

    let records = &event.payload.records;

    if records.is_empty() {
        tracing::info!("No records found. Exiting.");
        return Ok(response);
    }

    for record in records {
        tracing::info!("EventId: {}", record.event_id);

        // Couldn't find a sequence number
        if record.change.sequence_number.is_none() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: Some("".to_string()),
            });
            return Ok(response);
        }

        // Process your record here...
        if process_record(record).is_err() {
            response.batch_item_failures.push(DynamoDbBatchItemFailure {
                item_identifier: record.change.sequence_number.clone(),
            });
            /* Since we are working with streams, we can return the failed item
 immediately.
```

```
            Lambda will immediately begin to retry processing from this failed
 item onwards. */
            return Ok(response);
        }
    }

    tracing::info!("Successfully processed {} record(s)", records.len());

    Ok(response)
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    tracing_subscriber::fmt()
        .with_max_level(tracing::Level::INFO)
        // disable printing the name of the module in every log line.
        .with_target(false)
        // disabling time is handy because CloudWatch will add the ingestion
 time.
        .without_time()
        .init();

    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unter. Lambda mit einem AWS SDK verwenden Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Melden von Batch-Elementfehlern für Lambda-Funktionen mit einem Amazon-SQS-Auslöser

Die folgenden Codebeispiele zeigen, wie eine teilweise Batch-Antwort für Lambda-Funktionen implementiert wird, die Ereignisse aus einer SQS-Warteschlange empfangen. Die Funktion meldet die Batch-Elementfehler in der Antwort und signalisiert Lambda, diese Nachrichten später erneut zu versuchen.

.NET

AWS SDK for .NET

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von SQS-Batchelementfehlern mit Lambda unter Verwendung von .NET.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
using Amazon.Lambda.Core;
using Amazon.Lambda.SQSEvents;

// Assembly attribute to enable the Lambda function's JSON input to be converted
 into a .NET class.
[assembly:
 LambdaSerializer(typeof(Amazon.Lambda.Serialization.SystemTextJson.DefaultLambdaJsonSeri
namespace sqsSample;

public class Function
{
    public async Task<SQSBatchResponse> FunctionHandler(SQSEvent evnt,
 ILambdaContext context)
    {
        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 List<SQSBatchResponse.BatchItemFailure>();
        foreach(var message in evnt.Records)
        {
            try
            {
                //process your message
                await ProcessMessageAsync(message, context);
            }
            catch (System.Exception)
            {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.Add(new
 SQSBatchResponse.BatchItemFailure{ItemIdentifier=message.MessageId});
            }
```

```
        }
        return new SQSBatchResponse(batchItemFailures);
    }

    private async Task ProcessMessageAsync(SQSEvent.SQSMessage message,
 ILambdaContext context)
    {
        if (String.IsNullOrEmpty(message.Body))
        {
            throw new Exception("No Body in SQS Message.");
        }
        context.Logger.LogInformation($"Processed message {message.Body}");
        // TODO: Do interesting work based on the new message
        await Task.CompletedTask;
    }
}
```

Go

SDK für Go V2

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batch-Elementen mit Lambda mithilfe von Go.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
package main

import (
 "context"
 "encoding/json"
 "fmt"
 "github.com/aws/aws-lambda-go/events"
 "github.com/aws/aws-lambda-go/lambda"
)
```

```
func handler(ctx context.Context, sqsEvent events.SQSEvent)
 (map[string]interface{}, error) {
 batchItemFailures := []map[string]interface{}{}

 for _, message := range sqsEvent.Records {

  if /* Your message processing condition here */ {
   batchItemFailures = append(batchItemFailures, map[string]interface{}
{"itemIdentifier": message.MessageId})
  }
 }

 sqsBatchResponse := map[string]interface{}{
  "batchItemFailures": batchItemFailures,
 }
 return sqsBatchResponse, nil
}

func main() {
 lambda.Start(handler)
}
```

Java

SDK für Java 2.x

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Java.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.amazonaws.services.lambda.runtime.events.SQSEvent;
import com.amazonaws.services.lambda.runtime.events.SQSBatchResponse;
```

```
import java.util.ArrayList;
import java.util.List;

public class ProcessSQSMessageBatch implements RequestHandler<SQSEvent,
 SQSBatchResponse> {
    @Override
    public SQSBatchResponse handleRequest(SQSEvent sqsEvent, Context context) {

        List<SQSBatchResponse.BatchItemFailure> batchItemFailures = new
 ArrayList<SQSBatchResponse.BatchItemFailure>();
        String messageId = "";
        for (SQSEvent.SQSMessage message : sqsEvent.getRecords()) {
            try {
                //process your message
                messageId = message.getMessageId();
            } catch (Exception e) {
                //Add failed message identifier to the batchItemFailures list
                batchItemFailures.add(new
 SQSBatchResponse.BatchItemFailure(messageId));
            }
        }
        return new SQSBatchResponse(batchItemFailures);
    }
}
```

JavaScript

SDK für JavaScript (v3)

> **Note**
>
> Es gibt noch mehr dazu GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von SQS-Batch-Elementfehlern mit Lambda unter Verwendung von. JavaScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
export const handler = async (event, context) => {
    const batchItemFailures = [];
```

```
    for (const record of event.Records) {
        try {
            await processMessageAsync(record, context);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }

    return { batchItemFailures };
};

async function processMessageAsync(record, context) {
    if (record.body && record.body.includes("error")) {
        throw new Error("There is an error in the SQS Message.");
    }
    console.log(`Processed message: ${record.body}`);
}
```

Melden von SQS-Batch-Elementfehlern mit Lambda unter Verwendung von. TypeScript

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
import { SQSEvent, SQSBatchResponse, Context, SQSBatchItemFailure, SQSRecord }
 from 'aws-lambda';

export const handler = async (event: SQSEvent, context: Context):
 Promise<SQSBatchResponse> => {
    const batchItemFailures: SQSBatchItemFailure[] = [];

    for (const record of event.Records) {
        try {
            await processMessageAsync(record);
        } catch (error) {
            batchItemFailures.push({ itemIdentifier: record.messageId });
        }
    }

    return {batchItemFailures: batchItemFailures};
};

async function processMessageAsync(record: SQSRecord): Promise<void> {
    if (record.body && record.body.includes("error")) {
        throw new Error('There is an error in the SQS Message.');
```

```
    }
    console.log(`Processed message ${record.body}`);
}
```

PHP

SDK für PHP

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batch-Elementen mit Lambda mithilfe von PHP.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
<?php

use Bref\Context\Context;
use Bref\Event\Sqs\SqsEvent;
use Bref\Event\Sqs\SqsHandler;
use Bref\Logger\StderrLogger;

require __DIR__ . '/vendor/autoload.php';

class Handler extends SqsHandler
{
    private StderrLogger $logger;
    public function __construct(StderrLogger $logger)
    {
        $this->logger = $logger;
    }

    /**
     * @throws JsonException
     * @throws \Bref\Event\InvalidLambdaEvent
     */
    public function handleSqs(SqsEvent $event, Context $context): void
    {
```

```
        $this->logger->info("Processing SQS records");
        $records = $event->getRecords();

        foreach ($records as $record) {
            try {
                // Assuming the SQS message is in JSON format
                $message = json_decode($record->getBody(), true);
                $this->logger->info(json_encode($message));
                // TODO: Implement your custom processing logic here
            } catch (Exception $e) {
                $this->logger->error($e->getMessage());
                // failed processing the record
                $this->markAsFailed($record);
            }
        }
        $totalRecords = count($records);
        $this->logger->info("Successfully processed $totalRecords SQS records");
    }
}

$logger = new StderrLogger();
return new Handler($logger);
```

Python

SDK für Python (Boto3)

> **Note**
>
> Es gibt noch mehr dazu. GitHub Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Python.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0

def lambda_handler(event, context):
    if event:
        batch_item_failures = []
```

```
        sqs_batch_response = {}

        for record in event["Records"]:
            try:
                # process message
            except Exception as e:
                batch_item_failures.append({"itemIdentifier":
 record['messageId']})

        sqs_batch_response["batchItemFailures"] = batch_item_failures
        return sqs_batch_response
```

Ruby

SDK für Ruby

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Ruby.

```
# Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
# SPDX-License-Identifier: Apache-2.0
require 'json'

def lambda_handler(event:, context:)
  if event
    batch_item_failures = []
    sqs_batch_response = {}

    event["Records"].each do |record|
      begin
        # process message
      rescue StandardError => e
        batch_item_failures << {"itemIdentifier" => record['messageId']}
      end
    end

    sqs_batch_response["batchItemFailures"] = batch_item_failures
```

```
    return sqs_batch_response
  end
end
```

Rust

SDK für Rust

> **Note**
>
> Es gibt noch mehr GitHub. Das vollständige Beispiel sowie eine Anleitung zum Einrichten und Ausführen finden Sie im Repository mit Serverless-Beispielen.

Melden von Fehlern bei SQS-Batchelementen mit Lambda unter Verwendung von Rust.

```
// Copyright Amazon.com, Inc. or its affiliates. All Rights Reserved.
// SPDX-License-Identifier: Apache-2.0
use aws_lambda_events::{
    event::sqs::{SqsBatchResponse, SqsEvent},
    sqs::{BatchItemFailure, SqsMessage},
};
use lambda_runtime::{run, service_fn, Error, LambdaEvent};

async fn process_record(_: &SqsMessage) -> Result<(), Error> {
    Err(Error::from("Error processing message"))
}

async fn function_handler(event: LambdaEvent<SqsEvent>) ->
 Result<SqsBatchResponse, Error> {
    let mut batch_item_failures = Vec::new();
    for record in event.payload.records {
        match process_record(&record).await {
            Ok(_) => (),
            Err(_) => batch_item_failures.push(BatchItemFailure {
                item_identifier: record.message_id.unwrap(),
            }),
        }
    }

    Ok(SqsBatchResponse {
```

```
        batch_item_failures,
    })
}

#[tokio::main]
async fn main() -> Result<(), Error> {
    run(service_fn(function_handler)).await
}
```

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Serviceübergreifende Beispiele für Lambda mit SDKs AWS

Die folgenden Beispielanwendungen verwenden AWS SDKs, um Lambda mit anderen zu kombinieren. AWS-Services Jedes Beispiel enthält einen Link zu GitHub, wo Sie Anweisungen zum Einrichten und Ausführen der Anwendung finden.

Beispiele

- Erstellen einer API-Gateway-REST-API zur Verfolgung von COVID-19-Daten
- Leihbibliothek-REST-API erstellen
- Erstellen einer Messenger-Anwendung mit Step Functions
- Eine Anwendung für Foto-Asset-Management erstellen, mit der Benutzer Fotos mithilfe von Labels verwalten können
- Erstellen einer Websocket-Chat-Anwendung mit API Gateway
- Erstellen einer Anwendung, die Kundenfeedback analysiert und Audio generiert
- Aufrufen einer Lambda-Funktion von einem Browser aus
- Transformieren Sie Daten für Ihre Anwendung mit S3 Object Lambda
- Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion
- Verwenden von Step Functions, um Lambda-Funktionen aufzurufen
- Verwendung geplanter Ereignisse zum Aufrufen einer Lambda-Funktion

Erstellen einer API-Gateway-REST-API zur Verfolgung von COVID-19-Daten

Das folgende Codebeispiel zeigt, wie eine REST-API erstellt wird, die ein System zur Verfolgung der täglichen COVID-19-Fälle in den Vereinigten Staaten unter Verwendung fiktiver Daten simuliert.

Python

SDK für Python (Boto3)

Zeigt, wie AWS Chalice mit dem verwendet wird AWS SDK for Python (Boto3) , um eine serverlose REST-API zu erstellen, die Amazon API Gateway und Amazon AWS Lambda DynamoDB verwendet. Die REST-API simuliert ein System, das die täglichen COVID-19-Fälle in den Vereinigten Staaten unter Verwendung fiktiver Daten simuliert. Lernen Sie Folgendes:

- Verwenden Sie AWS Chalice, um Routen in Lambda-Funktionen zu definieren, die aufgerufen werden, um REST-Anfragen zu bearbeiten, die über API Gateway eingehen.
- Verwenden Sie Lambda-Funktionen zum Abrufen und Speichern von Daten in einer DynamoDB-Tabelle, um REST-Anforderungen zu bearbeiten.
- Definieren Sie die Tabellenstruktur und die Ressourcen für Sicherheitsrollen in einer AWS CloudFormation Vorlage.
- Verwenden Sie AWS Chalice und CloudFormation , um alle erforderlichen Ressourcen zu verpacken und bereitzustellen.
- Wird verwendet CloudFormation , um alle erstellten Ressourcen zu bereinigen.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- API Gateway
- AWS CloudFormation
- DynamoDB
- Lambda

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Leihbibliothek-REST-API erstellen

Im folgenden Codebeispiel wird veranschaulicht, wie man eine Leihbibliothek erstellt, in der Kunden Bücher mithilfe einer REST-API ausleihen und zurückgeben können, die von einer Amazon-Aurora-Datenbank unterstützt wird.

Python

SDK für Python (Boto3)

Zeigt, wie die AWS SDK for Python (Boto3) mit der Amazon Relational Database Service (Amazon RDS) API und AWS Chalice verwendet wird, um eine REST-API zu erstellen, die von einer Amazon Aurora Aurora-Datenbank unterstützt wird. Der Webservice ist vollständig Serverless und stellt eine einfache Leihbibliothek dar, in der die Kunden Bücher ausleihen und zurückgeben können. Lernen Sie Folgendes:

- Erstellen und verwalten Sie einen Serverless-Aurora-Datenbank-Cluster.
- Wird AWS Secrets Manager zur Verwaltung von Datenbankanmeldedaten verwendet.
- Implementieren Sie einen Datenspeicher-Layer, der Amazon RDS verwendet, um Daten in die und aus der Datenbank zu verschieben.
- Verwenden Sie AWS Chalice, um eine serverlose REST-API für Amazon API Gateway bereitzustellen und. AWS Lambda
- Verwenden Sie das Anforderungspaket, um Anfragen an den Webservice zu senden.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- API Gateway
- Aurora
- Lambda
- Secrets Manager

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen einer Messenger-Anwendung mit Step Functions

Das folgende Codebeispiel zeigt, wie eine AWS Step Functions Messenger-Anwendung erstellt wird, die Nachrichtendatensätze aus einer Datenbanktabelle abruft.

Python

SDK für Python (Boto3)

Zeigt, wie AWS SDK for Python (Boto3) mit AWS Step Functions dem with eine Messenger-Anwendung erstellt wird, die Nachrichtendatensätze aus einer Amazon DynamoDB-Tabelle abruft und sie mit Amazon Simple Queue Service (Amazon SQS) sendet. Die Zustandsmaschine ist mit einer AWS Lambda Funktion integriert, mit der die Datenbank nach nicht gesendeten Nachrichten durchsucht werden kann.

- Erstellen Sie einen Zustandsautomaten, der Nachrichtendatensätze aus einer Amazon-DynamoDB-Tabelle abruft und aktualisiert.
- Aktualisieren Sie die Definition des Zustandsautomaten, um auch Nachrichten an Amazon Simple Queue Service (Amazon SQS) zu senden.
- Starten und stoppen Sie Ausführungen des Zustandsautomaten.
- Stellen Sie vom Zustandsautomaten aus über Serviceintegrationen eine Verbindung zu Lambda, DynamoDB und Amazon SQS her.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Lambda
- Amazon SQS
- Step Functions

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Eine Anwendung für Foto-Asset-Management erstellen, mit der Benutzer Fotos mithilfe von Labels verwalten können

Die folgenden Codebeispiele zeigen, wie eine Serverless-Anwendung erstellt wird, mit der Benutzer Fotos mithilfe von Labels verwalten können.

.NET

AWS SDK for .NET

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

C++

SDK für C++

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Java

SDK für Java 2.x

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

JavaScript

SDK für JavaScript (v3)

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Kotlin

SDK für Kotlin

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

PHP

SDK für PHP

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon Rekognition
- Amazon S3
- Amazon SNS

Rust

SDK für Rust

Zeigt, wie eine Anwendung zur Verwaltung von Fotobeständen entwickelt wird, die mithilfe von Amazon Rekognition Labels in Bildern erkennt und sie für einen späteren Abruf speichert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Einen tiefen Einblick in den Ursprung dieses Beispiels finden Sie im Beitrag in der AWS - Community.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda

- Amazon Rekognition
- Amazon S3
- Amazon SNS

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen einer Websocket-Chat-Anwendung mit API Gateway

Das folgende Codebeispiel zeigt, wie eine Chat-Anwendung erstellt wird, die von einer auf Amazon API Gateway basierenden Websocket-API bereitgestellt wird.

Python

SDK für Python (Boto3)

Zeigt, wie das AWS SDK for Python (Boto3) mit Amazon API Gateway V2 verwendet wird, um eine Websocket-API zu erstellen, die in Amazon DynamoDB integriert AWS Lambda werden kann.

- Erstellen Sie eine WebSocket-API, die von API Gateway bereitgestellt wird.
- Definieren Sie einen Lambda-Handler, der Verbindungen in DynamoDB speichert und Nachrichten an andere Chat-Teilnehmer sendet.
- Stellen Sie eine Verbindung zur Websocket-Chat-Anwendung her und senden Sie Nachrichten mit dem Websockets-Paket.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Erstellen einer Anwendung, die Kundenfeedback analysiert und Audio generiert

Die folgenden Codebeispiele zeigen, wie Sie eine Anwendung erstellen, die Kundenkommentarkarten analysiert, sie aus ihrer Originalsprache übersetzt, ihre Stimmung ermittelt und aus dem übersetzten Text eine Audiodatei generiert.

.NET

AWS SDK for .NET

Diese Beispielanwendung analysiert und speichert Kundenfeedback-Karten. Sie ist auf die Anforderungen eines fiktiven Hotels in New York City zugeschnitten. Das Hotel erhält Feedback von Gästen in Form von physischen Kommentarkarten in verschiedenen Sprachen. Dieses Feedback wird über einen Webclient in die App hochgeladen. Nachdem ein Bild einer Kommentarkarte hochgeladen wurde, werden folgende Schritte ausgeführt:

- Der Text wird mithilfe von Amazon Textract aus dem Bild extrahiert.
- Amazon Comprehend ermittelt die Stimmung und die Sprache des extrahierten Textes.
- Der extrahierte Text wird mithilfe von Amazon Translate ins Englische übersetzt.
- Amazon Polly generiert auf der Grundlage des extrahierten Texts eine Audiodatei.

Die vollständige App kann mithilfe des AWS CDK bereitgestellt werden. Den Quellcode und Anweisungen zur Bereitstellung finden Sie im Projekt unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Java

SDK für Java 2.x

Diese Beispielanwendung analysiert und speichert Kundenfeedback-Karten. Sie ist auf die Anforderungen eines fiktiven Hotels in New York City zugeschnitten. Das Hotel erhält

Feedback von Gästen in Form von physischen Kommentarkarten in verschiedenen Sprachen. Dieses Feedback wird über einen Webclient in die App hochgeladen. Nachdem ein Bild einer Kommentarkarte hochgeladen wurde, werden folgende Schritte ausgeführt:

- Der Text wird mithilfe von Amazon Textract aus dem Bild extrahiert.
- Amazon Comprehend ermittelt die Stimmung und die Sprache des extrahierten Textes.
- Der extrahierte Text wird mithilfe von Amazon Translate ins Englische übersetzt.
- Amazon Polly generiert auf der Grundlage des extrahierten Texts eine Audiodatei.

Die vollständige App kann mithilfe des AWS CDK bereitgestellt werden. Den Quellcode und Anweisungen zur Bereitstellung finden Sie im Projekt unter GitHub.

In diesem Beispiel verwendete Dienste

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

JavaScript

SDK für JavaScript (v3)

Diese Beispielanwendung analysiert und speichert Kundenfeedback-Karten. Sie ist auf die Anforderungen eines fiktiven Hotels in New York City zugeschnitten. Das Hotel erhält Feedback von Gästen in Form von physischen Kommentarkarten in verschiedenen Sprachen. Dieses Feedback wird über einen Webclient in die App hochgeladen. Nachdem ein Bild einer Kommentarkarte hochgeladen wurde, werden folgende Schritte ausgeführt:

- Der Text wird mithilfe von Amazon Textract aus dem Bild extrahiert.
- Amazon Comprehend ermittelt die Stimmung und die Sprache des extrahierten Textes.
- Der extrahierte Text wird mithilfe von Amazon Translate ins Englische übersetzt.
- Amazon Polly generiert auf der Grundlage des extrahierten Texts eine Audiodatei.

Die vollständige App kann mithilfe des AWS CDK bereitgestellt werden. Den Quellcode und Anweisungen zur Bereitstellung finden Sie im Projekt unter GitHub. Die folgenden Auszüge zeigen, wie der innerhalb von Lambda-Funktionen verwendet AWS SDK for JavaScript wird.

```
import {
  ComprehendClient,
  DetectDominantLanguageCommand,
  DetectSentimentCommand,
} from "@aws-sdk/client-comprehend";

/**
 * Determine the language and sentiment of the extracted text.
 *
 * @param {{ source_text: string}} extractTextOutput
 */
export const handler = async (extractTextOutput) => {
  const comprehendClient = new ComprehendClient({});

  const detectDominantLanguageCommand = new DetectDominantLanguageCommand({
    Text: extractTextOutput.source_text,
  });

  // The source language is required for sentiment analysis and
  // translation in the next step.
  const { Languages } = await comprehendClient.send(
    detectDominantLanguageCommand,
  );

  const languageCode = Languages[0].LanguageCode;

  const detectSentimentCommand = new DetectSentimentCommand({
    Text: extractTextOutput.source_text,
    LanguageCode: languageCode,
  });

  const { Sentiment } = await comprehendClient.send(detectSentimentCommand);

  return {
    sentiment: Sentiment,
    language_code: languageCode,
  };
};
```

```
import {
  DetectDocumentTextCommand,
  TextractClient,
} from "@aws-sdk/client-textract";
```

```
/**
 * Fetch the S3 object from the event and analyze it using Amazon Textract.
 *
 * @param {import("@types/aws-lambda").EventBridgeEvent<"Object Created">}
 eventBridgeS3Event
 */
export const handler = async (eventBridgeS3Event) => {
  const textractClient = new TextractClient();

  const detectDocumentTextCommand = new DetectDocumentTextCommand({
    Document: {
      S3Object: {
        Bucket: eventBridgeS3Event.bucket,
        Name: eventBridgeS3Event.object,
      },
    },
  });

  // Textract returns a list of blocks. A block can be a line, a page, word, etc.
  // Each block also contains geometry of the detected text.
  // For more information on the Block type, see https://docs.aws.amazon.com/
textract/latest/dg/API_Block.html.
  const { Blocks } = await textractClient.send(detectDocumentTextCommand);

  // For the purpose of this example, we are only interested in words.
  const extractedWords = Blocks.filter((b) => b.BlockType === "WORD").map(
    (b) => b.Text,
  );

  return extractedWords.join(" ");
};
```

```
import { PollyClient, SynthesizeSpeechCommand } from "@aws-sdk/client-polly";
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

/**
 * Synthesize an audio file from text.
 *
 * @param {{ bucket: string, translated_text: string, object: string}}
 sourceDestinationConfig
 */
```

```
export const handler = async (sourceDestinationConfig) => {
  const pollyClient = new PollyClient({});

  const synthesizeSpeechCommand = new SynthesizeSpeechCommand({
    Engine: "neural",
    Text: sourceDestinationConfig.translated_text,
    VoiceId: "Ruth",
    OutputFormat: "mp3",
  });

  const { AudioStream } = await pollyClient.send(synthesizeSpeechCommand);

  const audioKey = `${sourceDestinationConfig.object}.mp3`;

  // Store the audio file in S3.
  const s3Client = new S3Client();
  const upload = new Upload({
    client: s3Client,
    params: {
      Bucket: sourceDestinationConfig.bucket,
      Key: audioKey,
      Body: AudioStream,
      ContentType: "audio/mp3",
    },
  });

  await upload.done();
  return audioKey;
};
```

```
import {
  TranslateClient,
  TranslateTextCommand,
} from "@aws-sdk/client-translate";

/**
 * Translate the extracted text to English.
 *
 * @param {{ extracted_text: string, source_language_code: string}}
 textAndSourceLanguage
 */
export const handler = async (textAndSourceLanguage) => {
  const translateClient = new TranslateClient({});
```

```
  const translateCommand = new TranslateTextCommand({
    SourceLanguageCode: textAndSourceLanguage.source_language_code,
    TargetLanguageCode: "en",
    Text: textAndSourceLanguage.extracted_text,
  });

  const { TranslatedText } = await translateClient.send(translateCommand);

  return { translated_text: TranslatedText };
};
```

In diesem Beispiel verwendete Dienste

- Amazon Comprehend
- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Ruby

SDK für Ruby

Diese Beispielanwendung analysiert und speichert Kundenfeedback-Karten. Sie ist auf die Anforderungen eines fiktiven Hotels in New York City zugeschnitten. Das Hotel erhält Feedback von Gästen in Form von physischen Kommentarkarten in verschiedenen Sprachen. Dieses Feedback wird über einen Webclient in die App hochgeladen. Nachdem ein Bild einer Kommentarkarte hochgeladen wurde, werden folgende Schritte ausgeführt:

- Der Text wird mithilfe von Amazon Textract aus dem Bild extrahiert.
- Amazon Comprehend ermittelt die Stimmung und die Sprache des extrahierten Textes.
- Der extrahierte Text wird mithilfe von Amazon Translate ins Englische übersetzt.
- Amazon Polly generiert auf der Grundlage des extrahierten Texts eine Audiodatei.

Die vollständige App kann mithilfe des AWS CDK bereitgestellt werden. Quellcode und Anweisungen zur Bereitstellung finden Sie im Projekt unter. GitHub

In diesem Beispiel verwendete Dienste

- Amazon Comprehend

- Lambda
- Amazon Polly
- Amazon Textract
- Amazon Translate

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Aufrufen einer Lambda-Funktion von einem Browser aus

Das folgende Codebeispiel zeigt, wie eine AWS Lambda Funktion von einem Browser aus aufgerufen wird.

JavaScript

SDK für JavaScript (v2)

Sie können eine browserbasierte Anwendung erstellen, die eine AWS Lambda Funktion verwendet, um eine Amazon DynamoDB-Tabelle mit Benutzerauswahlen zu aktualisieren.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter. GitHub

In diesem Beispiel verwendete Dienste

- DynamoDB
- Lambda

SDK für JavaScript (v3)

Sie können eine browserbasierte Anwendung erstellen, die eine AWS Lambda Funktion verwendet, um eine Amazon DynamoDB-Tabelle mit Benutzerauswahlen zu aktualisieren. Diese App verwendet v3. AWS SDK for JavaScript

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB

- Lambda

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Transformieren Sie Daten für Ihre Anwendung mit S3 Object Lambda

Das folgende Codebeispiel zeigt, wie Sie Daten für Ihre Anwendung mit S3 Object Lambda transformieren.

.NET

AWS SDK for .NET

Zeigt, wie benutzerdefinierten Code zu standardmäßigen S3 GET-Anfragen hinzugefügt wird, um das von S3 abgerufene angeforderte Objekt so zu ändern, dass das Objekt den Anforderungen des anfragenden Clients oder der Anwendung entspricht.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- Lambda
- Amazon S3

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwenden von API Gateway zum Aufrufen einer Lambda-Funktion

Die folgenden Codebeispiele zeigen, wie eine von Amazon API Gateway aufgerufene AWS Lambda Funktion erstellt wird.

Java

SDK für Java 2.x

Zeigt, wie eine AWS Lambda Funktion mithilfe der Lambda Java Runtime API erstellt wird. In diesem Beispiel werden verschiedene AWS Dienste aufgerufen, um einen bestimmten Anwendungsfall auszuführen. Dieses Beispiel zeigt, wie man eine Lambda-Funktion erstellt, die von Amazon API Gateway aufgerufen wird und eine Amazon-DynamoDB-Tabelle nach Arbeitsjubiläen durchsucht und Amazon Simple Notification Service (Amazon SNS) verwendet, um eine Textnachricht an Ihre Mitarbeiter zu senden, die ihnen zu ihrem einjährigen Jubiläum gratuliert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon SNS

JavaScript

SDK für JavaScript (v3)

Zeigt, wie eine AWS Lambda Funktion mithilfe der JavaScript Lambda-Laufzeit-API erstellt wird. In diesem Beispiel werden verschiedene AWS Dienste aufgerufen, um einen bestimmten Anwendungsfall auszuführen. Dieses Beispiel zeigt, wie man eine Lambda-Funktion erstellt, die von Amazon API Gateway aufgerufen wird und eine Amazon-DynamoDB-Tabelle nach Arbeitsjubiläen durchsucht und Amazon Simple Notification Service (Amazon SNS) verwendet, um eine Textnachricht an Ihre Mitarbeiter zu senden, die ihnen zu ihrem einjährigen Jubiläum gratuliert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Dieses Beispiel ist auch verfügbar im AWS SDK for JavaScript Entwicklerhandbuch für v3.

In diesem Beispiel verwendete Dienste

- API Gateway
- DynamoDB
- Lambda
- Amazon SNS

Python

SDK für Python (Boto3)

Dieses Beispiel veranschaulicht, wie eine REST-API für Amazon API Gateway erstellt und verwendet wird, die auf eine AWS Lambda -Funktion verweist. Der Lambda-Handler veranschaulicht, wie basierend auf HTTP-Methoden weitergeleitet wird, wie Daten aus der Abfragezeichenfolge, dem Header und dem Text abgerufen werden und wie eine JSON-Antwort zurückgegeben wird.

- Stellen Sie eine Lambda-Funktion bereit.
- REST-API für API Gateway erstellen
- Erstellen Sie eine REST-Ressource, die auf die Lambda-Funktion verweist.
- Erteilen Sie API Gateway die Berechtigung, die Lambda-Funktion aufzurufen.
- Verwenden Sie das Anforderungspaket, um Anforderungen an die REST-API zu senden.
- Bereinigen Sie alle Ressourcen, die während der Demo erstellt wurden.

Dieses Beispiel lässt sich am besten auf ansehen GitHub. Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- API Gateway
- Lambda

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwenden von Step Functions, um Lambda-Funktionen aufzurufen

Die folgenden Codebeispiele zeigen, wie Sie eine AWS Step Functions Zustandsmaschine erstellen, die nacheinander AWS Lambda Funktionen aufruft.

Java

SDK für Java 2.x

Zeigt, wie Sie mithilfe von AWS Step Functions und einen AWS serverlosen Workflow erstellen. AWS SDK for Java 2.x Jeder Workflow-Schritt wird mithilfe einer AWS Lambda Funktion implementiert.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

JavaScript

SDK für JavaScript (v3)

Zeigt, wie Sie einen AWS serverlosen Workflow mithilfe von AWS Step Functions und erstellen. AWS SDK for JavaScript Jeder Workflow-Schritt wird mithilfe einer AWS Lambda Funktion implementiert.

Lambda ist ein Datenverarbeitungsservice, mit dem Sie Code ausführen können, ohne Server bereitstellen oder verwalten zu müssen. Step Functions ist ein Serverless-Orchestrierungsservice, mit dem Sie Lambda-Funktionen und andere kombinieren AWS -Services kombinieren können, um geschäftskritische Anwendungen zu erstellen.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Dieses Beispiel ist auch verfügbar im AWS SDK for JavaScript Entwicklerhandbuch für v3.

In diesem Beispiel verwendete Dienste

- DynamoDB
- Lambda
- Amazon SES
- Step Functions

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Verwendung geplanter Ereignisse zum Aufrufen einer Lambda-Funktion

Die folgenden Codebeispiele zeigen, wie eine AWS Lambda Funktion erstellt wird, die durch ein von Amazon EventBridge geplantes Ereignis aufgerufen wird.

Java

SDK für Java 2.x

Zeigt, wie ein von Amazon EventBridge geplantes Ereignis erstellt wird, das eine AWS Lambda Funktion aufruft. Konfigurieren Sie so EventBridge , dass ein Cron-Ausdruck verwendet wird, um zu planen, wann die Lambda-Funktion aufgerufen wird. In diesem Beispiel erstellen Sie eine Lambda-Funktion mithilfe der Lambda-Java-Laufzeit-API. In diesem Beispiel werden verschiedene AWS Dienste aufgerufen, um einen bestimmten Anwendungsfall auszuführen. Dieses Beispiel zeigt, wie man eine App erstellt, die eine mobile Textnachricht an Ihre Mitarbeiter sendet, um ihnen zum einjährigen Jubiläum zu gratulieren.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

JavaScript

SDK für JavaScript (v3)

Zeigt, wie ein von Amazon EventBridge geplantes Ereignis erstellt wird, das eine AWS Lambda Funktion aufruft. Konfigurieren Sie so EventBridge , dass ein Cron-Ausdruck verwendet wird, um zu planen, wann die Lambda-Funktion aufgerufen wird. In diesem Beispiel erstellen Sie eine Lambda-Funktion mithilfe der JavaScript Lambda-Laufzeit-API. In diesem Beispiel werden verschiedene AWS Dienste aufgerufen, um einen bestimmten Anwendungsfall auszuführen. Dieses Beispiel zeigt, wie man eine App erstellt, die eine mobile Textnachricht an Ihre Mitarbeiter sendet, um ihnen zum einjährigen Jubiläum zu gratulieren.

Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

Dieses Beispiel ist auch verfügbar im AWS SDK for JavaScript Entwicklerhandbuch für v3.

In diesem Beispiel verwendete Dienste

- DynamoDB
- EventBridge
- Lambda
- Amazon SNS

Python

SDK für Python (Boto3)

Dieses Beispiel zeigt, wie eine AWS Lambda Funktion als Ziel einer geplanten EventBridge Amazon-Veranstaltung registriert wird. Der Lambda-Handler schreibt eine freundliche Nachricht und die vollständigen Ereignisdaten für den späteren Abruf in Amazon CloudWatch Logs.

- Stellt eine Lambda-Funktion bereit.
- Erzeugt ein EventBridge geplantes Ereignis und macht die Lambda-Funktion zum Ziel.
- Erteilt die Erlaubnis, die EventBridge Lambda-Funktion aufrufen zu lassen.
- Druckt die neuesten Daten aus CloudWatch Logs, um das Ergebnis der geplanten Aufrufe anzuzeigen.
- Bereinigt alle Ressourcen, die während der Demo erstellt wurden.

Dieses Beispiel lässt sich am besten auf ansehen. GitHub Den vollständigen Quellcode und Anweisungen zur Einrichtung und Ausführung finden Sie im vollständigen Beispiel unter GitHub.

In diesem Beispiel verwendete Dienste

- CloudWatch Logs
- EventBridge
- Lambda

Eine vollständige Liste der AWS SDK-Entwicklerhandbücher und Codebeispiele finden Sie unterLambda mit einem AWS SDK verwenden. Dieses Thema enthält auch Informationen zu den ersten Schritten und Details zu früheren SDK-Versionen.

Lambda-Kontingente

> **Important**
>
> Neue AWS-Konten haben die Parallelität und die Speicherkontingente reduziert. AWS erhöht diese Kontingente automatisch auf der Grundlage Ihrer Nutzung.

Datenverarbeitung und Speicherung

Lambda legt Kontingente für die Menge an Datenverarbeitung und Speicherressourcen, die Sie verwenden können, um Funktionen auszuführen und zu speichern. Kontingente für gleichzeitige Ausführungen und Speicherung gelten pro AWS-Region. Die Elastic-Network-Schnittstelle (ENI)-Kontingente gelten für jede Virtual Private Cloud (VPC), unabhängig von der Region. Die folgenden Kontingente können gegenüber ihren Standardwerten erhöht werden. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ressource	Standardkontingent	Kann erhöht werden bis zu
Gleichzeitige Ausführungen	1.000	Zehntausende
Speicher für hochgeladene Funktionen (.zip-Datei-Archive) und Ebenen. Jede Funktionsversion und Ebenenversion verbraucht Speicher. Bewährte Methoden für die Verwaltung Ihres Codespeichers finden Sie bei Serverless Land unter Monitoring Lambda code storage.	75 GB	Terabytes
Speicher für als Container-Images definierten Funktionen Diese Bilder werden in Amazon ECR gespeichert.	Siehe Amazon-ECR-Service kontingente.	

Ressource	Standardkontingent	Kann erhöht werden bis zu
Elastic Network-Schnittstellen in der Virtual Private Cloud (VPC) **Note** Dieses Kontingent wird mit anderen Services wie Amazon Elastic File System (Amazon EFS) geteilt. Siehe Amazon-VPC-Kontingente.	250	Tausende

Weitere Details zur Gleichzeitigkeit und zur datenverkehrbasierten Skalierung der Funktionsgleichzeitigkeit von Lambda finden Sie unter Die Lambda-Funktionsskalierung verstehen.

Funktionskonfiguration, -bereitstellung und -ausführung

Die folgenden Kontingente gelten für die Konfiguration, Bereitstellung und Ausführung von Funktionen. Sofern nicht anders angegeben, können sie nicht geändert werden.

Note

Die Lambda-Dokumentation, die Protokollmeldungen und die Konsole verwenden die Abkürzung MB (anstelle von MiB), um auf 1 024 KB zu verweisen.

Ressource	Quota
Funktion Speicherzuweisung	128 MB bis 10.240 MB (in Schritten von 1 MB). Hinweis: Lambda weist die CPU-Leistung proportional zur Menge des konfigurierten Arbeitsspeichers zu. Sie können den Arbeitsspeicher und

Ressource	Quota
	die CPU-Leistung, die Ihrer Funktion zugewiesen sind, mit der Einstellung Arbeitsspeicher (MB) erhöhen oder verringern. Bei 1 769 MB hat eine Funktion das Äquivalent von einer vCPU.
Funktion Zeitüberschreitung	900 Sekunden (15 Minuten)
Funktion Umgebungsvariablen	4 KB, für alle Umgebungsvariablen, die mit der Funktion verknüpft sind, im Aggregat
Funktion ressourcenbasierte Richtlinie	20 KB
Funktionsebenen	Fünf Ebenen
Funktion – Limit für Gleichzeitigkeitsskalierung	Für jede Funktion 1 000 Ausführungsumgebungen alle 10 Sekunden
Aufrufnutzlast (Anfrage und Antwort)	Jeweils 6 MB für Anfrage und Antwort (synchron) 20 MB für jede gestreamte Antwort (synchron). Die Payload-Größe für gestreamte Antworten kann gegenüber den Standardwerten erhöht werden. Wenden Sie sich an AWS Support , um weitere Informationen zu erhalten.) 256 KB (asynchron) 1 MB für die kombinierte Gesamtgröße von Anforderungszeilen- und Header-Werten

Ressource	Quota
Bandbreite für gestreamte Antworten	Unbegrenzt für die ersten 6 MB der Antwort Ihrer Funktion Für Antworten, die größer als 6 MB sind, 2 Mbit/s für den Rest der Antwort
Größe des Bereitstellungspakets (ZIP-Dateiarchiv)	50 MB (gezippt, für direkten Upload) 250 MB (entpackt) Dieses Kontingent gilt für alle Dateien, die Sie uploaden, einschließlich Ebenen und benutzerdefinierte Laufzeitumgebungen. 3 MB (Konsoleneditor)
Größe der Container-Image-Einstellungen	16 KB
Codepaketgröße des Container-Images	10 GB (maximale unkomprimierte Image-Größe, einschließlich aller Ebenen)
Testereignisse (Konsoleneditor)	10
`/tmp`-Verzeichnisspeicher	Zwischen 512 MB und 10 240 MB, in 1-MB-Schritten.
Dateibeschreibungen	1,024
Ausführungsprozesse/-Threads	1,024

Lambda-API-Anforderungen

Die folgenden Kontingente sind Lambda-API-Anfragen zugeordnet.

Ressource	Kontingent
Aufrufanfragen pro Funktion pro Region (synchron)	Jede Instance Ihrer Ausführun gsumgebung kann bis zu 10 Anfragen pro Sekunde bearbeiten. Mit anderen Worten, das Gesamtauf ruflimit beträgt das 10-fache Ihres Gleichzeitigkeitslimits. Siehe Die Lambda-Funktionsskalierung verstehen.
Aufrufanfragen pro Funktion pro Region (asynchron)	Jede Instance Ihrer Ausführun gsumgebung kann eine unbegrenz te Anzahl an Anfragen bearbeiten. Mit anderen Worten, das Gesamtlim it für Aufrufe basiert nur auf der für Ihre Funktion verfügbaren Gleichzei tigkeit. Siehe Die Lambda-Fu nktionsskalierung verstehen.
Aufrufanforderungen pro Funktionsversion oder Alias (Anfragen pro Sekunde)	10 x zugewiesene Provisioned Concurrency **Note** Dieses Kontingent gilt nur für Funktionen, die Provisioned Concurrency verwenden.
GetFunction-API-Anforderungen	100 Anfragen pro Sekunde. Kann nicht erhöht werden.
GetPolicy-API-Anforderungen	15 Anfragen pro Sekunde. Kann nicht erhöht werden.
Restliche API-Anfragen der Kontrollebene (ausgenom men Aufrufe und GetPolicy Anfragen) GetFunction	15 Anfragen pro Sekunde über alle APIs hinweg (nicht 15 Anfragen pro

Ressource	Kontingent
	Sekunde pro API). Kann nicht erhöht werden.

Sonstige Services

Kontingente für andere Dienste wie AWS Identity and Access Management (IAM), Amazon CloudFront (Lambda @Edge) und Amazon Virtual Private Cloud (Amazon VPC) können sich auf Ihre Lambda-Funktionen auswirken. Weitere Informationen finden Sie unter AWS-Service -Kontingent im Allgemeine Amazon Web Services-Referenz und Lambda mit Ereignissen aus anderen Diensten aufrufen AWS.

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen am AWS Lambda Entwicklerhandbuch seit Mai 2018 beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Support SnapStart in neuen Regionen	Lambda SnapStartist jetzt in den folgenden Regionen erhältlich: Europa (Spanien) , Europa (Zürich), Asien-Paz ifik (Melbourne), Asien-Pazifik (Hyderabad) und Naher Osten (VAE).	12. Januar 2024
AWS verwaltete Richtlini enaktualisierungen	Service Quotas hat eine bestehende AWS verwaltet e Richtlinie aktualisiert (`AWSLambdaVPCAccess ExecutionRole`).	5. Januar 2024
Python-3.12-Laufzeit	Lambda unterstützt jetzt Python 3.12 als verwaltete Laufzeit und Container-Basis-Image. Weitere Informationen finden Sie unter Python 3.12 Runtime now available AWS Lambda im AWS Compute-B log.	14. Dezember 2023
Java-21-Laufzeit	Lambda unterstützt jetzt Java 21 als Image für die verwaltete Laufzeit und Container-Basis-Image (`java21`).	16. November 2023

Node.js-20.x-Laufzeit	Lambda unterstützt jetzt Node.js 20 als Image für die verwaltete Laufzeit und Container-Basis-Image (`nodejs20.x`). Weitere Informationen finden Sie im AWS LambdaAWS Compute-Blog unter Node.js 20.x-Laufzeit jetzt verfügbar.	14. November 2023
Laufzeit „provided.al2023“	Lambda unterstützt jetzt Amazon Linux 2023 als Image für die verwaltete Laufzeit und Container-Basis-Image. Weitere Informationen finden Sie unter Einführung in die Amazon Linux 2023 Runtime for AWS Lambda im AWS Compute-Blog.	9. November 2023
IPv6-Unterstützung für Dual-Stack-Subnetze	Lambda unterstützt jetzt den ausgehenden IPv6-Datenverkehr zu Dual-Stack-Subnetzen. Weitere Informationen finden Sie unter IPv6-Unterstützung.	12. Oktober 2023

Serverless-Funktionen und Anwendungen testen	Erfahren Sie mehr über Techniken zum Debuggen und Automatisieren von Tests von Serverless-Funktionen in der Cloud. In den Abschnitten zur Python- und Typescript-Sprache gibt es jetzt ein Kapitel zu Tests sowie Ressourcen. Einzelheiten finden Sie unter Serverless-Funktionen und Anwendungen testen.	16. Juni 2023
Ruby 3.2-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für Ruby 3.2. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Ruby.	7. Juni 2023
Antwort-Streaming	Lambda unterstützt jetzt Streaming-Antworten von Funktionen. Weitere Informationen finden Sie unter Konfigurieren einer Lambda-Funktion zum Streamen von Antworten.	06. April 2023
Asynchrone Aufrufmetriken	Lambda veröffentlicht asynchrone Aufrufmetriken. Weitere Informationen finden Sie unter Asynchrone Aufrufmetriken.	9. Februar 2023

Kontrollen der Laufzeitversion	Lambda veröffentlicht neue Laufzeitversionen, die Sicherheitsupdates, Fehlerbehebungen und neue Funktionen enthalten. Sie können jetzt steuern, wann Ihre Funktionen auf die neuen Laufzeitversionen aktualisiert werden sollen. Weitere Informationen finden Sie unter Lambda-Laufzeitaktualisierungen.	23. Januar 2023
Lambda SnapStart	Verwenden Sie Lambda SnapStart , um die Startzeit für Java-Funktionen zu reduzieren, ohne zusätzliche Ressourcen bereitzustellen oder komplexe Leistungsoptimierungen zu implementieren. Weitere Informationen finden Sie unter Verbessern der Startleistung mit Lambda SnapStart.	28. November 2022
Node.js-18-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für Node.js 18. Node.js 18 verwendet Amazon Linux 2. Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	18. November 2022

Lambda: Bedingungsschlüssel SourceFunctionArn	Bei einer AWS Ressource filtert der `lambda:SourceFunctionArn` Bedingungsschlüssel den Zugriff auf die Ressource nach dem ARN einer Lambda-Funktion. Einzelheiten dazu finden Sie unter Arbeiten mit Anmeldeinformationen der Lambda-Ausführungsumgebung.	01. Juli 2022
Node.js-16-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für Node.js 16. Node.js 16 verwendet Amazon Linux 2. Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	11. Mai 2022
Lambda-Funktions-URLs	Lambda unterstützt jetzt Funktions-URLs, die dedizierte HTTP(S)-Endpunkte für Lambda-Funktionen sind. Details dazu finden Sie unter Lambda-Funktions-URLs.	6. April 2022
Gemeinsame Testereignisse in der Konsole AWS Lambda	Lambda unterstützt jetzt das Teilen von Testereignissen mit anderen Benutzern im selben AWS-Konto. Details finden Sie unter Testen von Lambda-Funktionen mit Hilfe der Konsole.	16. März 2022

PrincipalOrgId in ressourcenbasierten Richtlinien	Lambda unterstützt jetzt das Erteilen von Berechtigungen für eine Organisation in AWS Organizations. Details dazu finden Sie unter Verwenden ressourcenbasierter Richtlinien für AWS Lambda.	11. März 2022
.NET-6-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für .NET 6. Weitere Details finden Sie unter Lambda-Laufzeiten.	23. Februar 2022
Ereignisfilterung für Kinesis-, DynamoDB- und Amazon-SQS-Ereignisquellen	Lambda unterstützt jetzt die Ereignisfilterung für Kinesis-, DynamoDB- und Amazon-SQS-Ereignisquellen. Details dazu finden Sie unter Lambda-Ereignisfilterung.	24. November 2021
mTLS-Authentifizierung für Amazon MSK und selbstverwaltete Apache-Kafka-Ereignisquellen	Lambda unterstützt ab sofort die mTLS-Authentifizierung für Amazon MSK und selbstverwaltete Apache-Kafka-Ereignisquellen. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon MSK.	19. November 2021
Lambda auf Graviton2	Lambda unterstützt jetzt Graviton2 für Funktionen, die arm64-Architektur verwenden. Details dazu finden Sie unter .Lambda-Befehlssatz-Architekturenaus.	29. September 2021

Python-3.9-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für Python 3.9. Weitere Details finden Sie unter Lambda-Laufzeiten.	16. August 2021
Neue Laufzeitversionen für Node.js, Python und Java	Neue Laufzeiten sind für Node.js, Python und Java verfügbar. Weitere Details finden Sie unter Lambda-Laufzeiten.	21. Juli 2021
Support für RabbitMQ als Ereignisquelle für Lambda	Lambda bietet jetzt Unterstützung für Amazon MQ für RabbitMQ als Ereignisquelle. Amazon MQ ist ein verwalteter Message-Broker-Service für Apache ActiveMQ und RabbitMQ, der das Einrichten und Betreiben von Message-Brokern in der Cloud vereinfacht. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon MQ.	7. Juli 2021

SASL/PLAIN-Authentifizierung für selbstverwaltete Kafka in Lambda	SASL/PLAIN ist jetzt ein unterstützter Authentifizierungsmechanismus für selbstverwaltete Kafka-Ereignisquellen auf Lambda Kunden, die SASL/PLAIN bereits auf ihrem selbstverwalteten Kafka-Cluster verwenden, können Lambda nun problemlos verwenden, um Verbraucheranwendungen zu erstellen, ohne die Authentifizierungsmethode ändern zu müssen. Details dazu finden Sie unter Verwenden von Lambda mit selbstverwaltetem Apache Kafka.	29. Juni 2021
Lambda-Erweiterungs-API	Allgemeine Verfügbarkeit von Lambda-Erweiterungen. Erweiterungen verwenden, um Ihre Lambda-Funktionen zu erweitern. Sie können Erweiterungen verwenden, die von Lambda-Partnern bereitgestellt werden, oder Sie können Ihre eigenen Lambda-Erweiterungen erstellen. Weitere Details finden Sie unter Lambda-Erweiterungs-API.	24. Mai 2021
Neues Lambda-Konsolenerlebnis	Die Lambda-Konsole wurde überarbeitet, um die Leistung und Konsistenz zu verbessern.	2. März 2021

Node.js-14-Laufzeit	Lambda unterstützt jetzt eine neue Laufzeit für Node.js 14. Node.js 14 verwendet Amazon Linux 2. Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	27. Januar 2021
Lambda-Container-Images	Lambda unterstützt jetzt als Container-Images definiert e Funktionen. Sie können die Flexibilität von Container -Tooling mit der Agilität und der betrieblichen Einfachhe it von Lambda kombinier en, um Anwendungen zu bauen. Weitere Details finden Sie unter Verwenden von Container-Images mit Lambda.	1. Dezember 2020

Codesignatur für Lambda-Funktionen	Lambda unterstützt jetzt Codesignatur. Administratoren können Lambda-Funktionen so konfigurieren, dass sie bei der Bereitstellung nur signierten Code akzeptieren. Lambda überprüft die Signaturen, um sicherzustellen, dass der Code nicht verändert oder manipuliert wird. Zusätzlich sorgt Lambda dafür, dass der Code von vertrauenswürdigen Entwicklern unterzeichnet wurde, bevor die Bereitstellung zugelassen wird. Weitere Details finden Sie unter Konfigurieren von Codesignatur für Lambda.	23. November 2020
Vorschau: Lambda Runtime Logs API	Lambda unterstützt jetzt die Runtime Logs API. Lambda-Erweiterungen können die Logs-API verwenden, um Protokollstreams in der Ausführungsumgebung zu abonnieren. Weitere Details finden Sie unter Lambda Runtime Logs API.	12. November 2020

Neue Ereignisquelle für Amazon MQ	Lambda bietet jetzt Unterstützung für Amazon MQ als Ereignisquelle. Verwenden Sie eine Lambda-Funktion, um Datensätze von Ihrem Amazon-MQ-Message-Broker zu verarbeiten. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon MQ.	5. November 2020
Vorschau: Lambda-Erweiterungs-API	Lambda-Erweiterungen verwenden, um Ihre Lambda-Funktionen zu erweitern. Sie können Erweiterungen verwenden, die von Lambda-Partnern bereitgestellt werden, oder Sie können Ihre eigenen Lambda-Erweiterungen erstellen. Weitere Details finden Sie unter Lambda-Erweiterungs-API.	8. Oktober 2020
Unterstützung für Java 8 und benutzerdefinierte Laufzeiten in AL2	Lambda unterstützt jetzt Java 8 und benutzerdefinierte Laufzeiten unter Amazon Linux 2. Weitere Details finden Sie unter Lambda-Laufzeiten.	12. August 2020

Neue Ereignisquelle für Amazon Managed Streaming for Apache Kafka	Lambda bietet jetzt Unterstützung für Amazon MSK als Ereignisquelle. Verwenden Sie eine Lambda-Funktion mit Amazon MSK, um Datensätze in einem Kafka-Thema zu verarbeiten. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon MSK.	11. August 2020
Verwenden von IAM-Bedingungsschlüsseln für Amazon-VPC-Einstellungen	Sie können nun Lambda-spezifische Bedingungsschlüssel für VPC-Einstellungen verwenden. Sie können beispielsweise festlegen, dass alle Funktionen in Ihrer Organisation mit einer VPC sein müssen. Sie können auch die Subnetze und Sicherheitsgruppen angeben, die die Benutzer der Funktion verwenden können bzw. nicht verwenden können. Weitere Details finden Sie unter Konfigurieren einer VPC für IAM-Funktionen.	10. August 2020

Einstellungen für Parallelbetrieb für Kinesis-HTTP/2-Stream-Konsumenten	Sie können jetzt die folgenden Parallelitätseinstellungen für Kinesis-Verbraucher mit erweitertem Fan-Out (HTTP/2-Streams) verwenden : ParallelizationFactor,, MaximumRetryAttempts, MaximumRecordAgeIn Seconds und. DestinationConfig BisectBatchOnFunctionError Einzelheiten finden Sie unter Verwenden AWS Lambda mit Amazon Kinesis.	7. Juli 2020
Batch-Fenster für Kinesis HTTP/2-Stream-Konsumenten	Sie können jetzt ein Batch-Fenster (MaximumBatchingWindowInSekunden) für HTTP/2-Streams konfigurieren. Lambda liest Datensätze aus dem Stream, bis es einen vollständigen Batch gesammelt hat oder bis das Batchfenster abläuft. Einzelheiten finden Sie unter Verwenden AWS Lambda mit Amazon Kinesis.	18. Juni 2020
Support für Amazon-EFS-Dateisysteme	Sie können nun ein Amazon-EFS-Dateisystem mit Ihren Lambda-Funktionen für den freigegebenen Netzwerkdateizugriff verbinden. Weitere Details finden Sie unter Konfigurieren des Dateisystemzugriffs für Lambda-Funktionen.	16. Juni 2020

AWS CDK Beispielanwendungen in der Lambda-Konsole	Die Lambda-Konsole enthält jetzt Beispielanwendungen, die das AWS Cloud Development Kit (AWS CDK) for TypeScript verwenden. Das AWS CDK ist ein Framework, mit dem Sie Ihre Anwendungsressourcen in Python TypeScript, Java oder .NET definieren können.	1. Juni 2020
Support für.NET Core 3.1.0 Runtime in AWS Lambda	AWS Lambda unterstützt jetzt die.NET Core 3.1.0-Runtime. Weitere Details finden Sie unter .NET Core CLI.	31. März 2020
Support für API-Gateway-Metriken für HTTP-APIs	Aktualisierte und erweiterte Dokumentation für die Verwendung von Lambda mit API Gateway, einschließlich Unterstützung für HTTP-APIs. Es wurde eine Beispielanwendung hinzugefügt, die eine API erstellt und mit AWS CloudFormation funktioniert. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon API Gateway.	23. März 2020

Ruby 2.7	Für Ruby 2.7 steht eine neue Laufzeit, ruby2.7, zur Verfügung. Dies ist die erste Ruby-Laufzeitumgebung, die Amazon Linux 2 verwendet . Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Ruby.	19. Februar 2020
Gleichzeitigkeitsmetriken	Lambda meldet nun die Metrik `ConcurrentExecutions` für alle Funktionen, Aliase und Versionen. Sie können ein Diagramm für diese Metrik auf der Überwachungsseite für Ihre Funktion anzeigen. Bisher wurde `ConcurrentExecutions` nur auf Kontoebene und für Funktionen gemeldet, die reservierte Gleichzeitigkeit verwenden . Details hierzu finden Sie unter AWS Lambda -Funktionsmetriken.	18. Februar 2020

Aktualisieren auf Funktionszustände	Funktionszustände werden jetzt standardmäßig für alle Funktionen erzwungen. Wenn Sie eine Funktion mit einer VPC verbinden, erstellt Lambda gemeinsame Elastic-Network-Schnittstellen. Dadurch kann Ihre Funktion skaliert werden, ohne zusätzliche Netzwerkschnittstellen erstellen zu müssen. Während dieser Zeit können Sie keine zusätzlichen Operationen für die Funktion ausführen, einschließlich der Aktualisierung der Konfiguration und der Veröffentlichung von Versionen. In einigen Fällen ist der Aufruf ebenfalls betroffen. Details zum aktuellen Status einer Funktion sind über die Lambda-API verfügbar. Diese Aktualisierung wird phasenweise veröffentlicht. Einzelheiten finden Sie im AWS Compute-Blog unter Aktualisierter Lambda-States-Lebenszyklus für VPC-Netzwerke. Weitere Informationen zu Zuständen finden Sie unter AWS Lambda -Funktionszustände.	24. Januar 2020

Aktualisierungen der API-Ausgabe der Funktionskonfiguration	Ursachencodes zu StateReasonCode (InvalidSubnet, InvalidSecurityGroup) und LastUpdateStatusReasonCode (SubnetOutofIPAddresses,, InvalidSecurityGroup) für Funktionen hinzugefügt InvalidSubnet, die eine Verbindung zu einer VPC herstellen. Weitere Informationen zu Zuständen finden Sie unter AWS Lambda -Funktionszustände.	20. Januar 2020
Bereitgestellte Gleichzeitigkeit	Sie haben nun die Möglichkeit, bereitgestellte Gleichzeitigkeit (Provisioned Concurrency) für eine Funktionsversion oder einen Alias zuzuweisen. Mit der bereitgestellten Gleichzeitigkeit kann eine Funktion ohne Schwankungen der Latenz skalieren. Weitere Details finden Sie unter Verwalten von Gleichzeitigkeit für eine Lambda-Funktion.	03. Dezember 2019

Erstellen eines Datenbank-Proxys	Sie können nun mit der Lambda-Konsole einen Datenbank-Proxy für eine Lambda-Funktion erstellen . Ein Datenbank-Proxy ermöglicht es einer Funktion, hohe Gleichzeitigkeitsstufen ohne überlastende Datenbank verbindungen zu erreichen . Weitere Details finden Sie unter Konfigurieren des Datenbankzugriffs für eine Lambda-Funktion.	03. Dezember 2019
Perzentilunterstützung für die Dauer-Metrik	Sie können nun die Dauer-Metrik basierend auf Perzentil en filtern. Weitere Details finden Sie unter AWS Lambda -Metriken.	26. November 2019
Höhere Gleichzeitigkeit für Stream-Ereignisquellen	Eine neue Option für das DynamoDB-Stream- und Kinesis-Stream-Ereignis quellen-Mapping ermöglich t es Ihnen, von jedem Shard mehrere Batches gleichzeitig zu verarbeiten. Wenn Sie die Anzahl gleichzeitiger Stapel pro Shard erhöhen, kann die Gleichzeitigkeit der Funktion bis zu zehnmal so hoch sein wie die Anzahl der Shards in Ihrem Stream. Weitere Details finden Sie unter Lambda-Er eignisquellen-Zuweisung.	25. November 2019

Funktionszustände	Wenn Sie eine Funktion erstellen oder aktualisieren, wechselt diese in einen ausstehenden Zustand, während Lambda Ressourcen zur Unterstützung bereitstellt. Wenn Sie Ihre Funktion mit einer VPC verbinden, kann Lambda sofort eine gemeinsame Elastic-Network-Schnittstelle erstellen, anstatt Netzwerkschnittstellen zu erstellen, wenn Ihre Funktion aufgerufen wird. Dies verbessert die Leistung von mit der VPC verbundenen Funktionen, erfordert aber möglicherweise eine Aktualisierung Ihrer Automatisierung. Details hierzu finden Sie unter AWS Lambda -Funktionszustände.	25. November 2019
Fehlerbehandlungsoptionen für den asynchronen Aufruf	Für den asynchronen Aufruf stehen neue Konfigurationsoptionen zur Verfügung. Sie können Lambda so konfigurieren, dass Wiederholversuche begrenzt und ein maximales Ereignisalter festgelegt werden. Weitere Details finden Sie unter Konfigurieren der Fehlerbehandlung für den asynchronen Aufruf.	25. November 2019

Fehlerbehandlung für Stream-Ereignisquellen	Es sind neue Konfigurationsoptionen für Ereignisquellen-Zuweisungen verfügbar, die aus Streams gelesen werden. Sie können DynamoDB-Stream- und Kinesis-Stream-Ereignisquellen-Zuweisung konfigurieren, um Wiederholversuche zu begrenzen und ein maximales Datensatzalter festzulegen. Wenn Fehler auftreten, können Sie das Ereignisquellen-Mapping so konfigurieren, dass Batches vor dem erneuten Versuch aufgeteilt und Aufrufdatensätze für fehlgeschlagene Batches an eine Warteschlange oder an ein Thema gesendet werden. Weitere Details finden Sie unter Lambda-Ereignisquellen-Mapping.	25. November 2019

Ziele für den asynchronen Aufruf	Sie können Lambda jetzt so konfigurieren, dass Datensätze asynchroner Aufrufe an einen anderen Service gesendet werden. Aufrufdatensätze enthalten Details zu Ereignis, Kontext und Antwort der Funktion. Sie können Aufrufdatensätze an eine SQS-Warteschlange, ein SNS-Thema, eine Lambda-Funktion oder einen Ereignisbus senden. EventBridge Weitere Details finden Sie unter Konfigurieren der Ziele für asynchronen Aufruf.	25. November 2019
Neue Laufzeiten für Node.js, Python und Java	Neue Laufzeiten sind für Node.js 12, Python 3.8 und Java 11 verfügbar. Weitere Details finden Sie unter Lambda-Laufzeiten.	18. November 2019
FIFO-Warteschlangenunterstützung für Amazon-SQS-Ereignisquellen	Sie können jetzt ein Ereignisquellen-Mapping erstellen, die aus einer FIFO (First-in-First-out)-Warteschlange liest. Bisher wurden nur Standardwarteschlangen unterstützt. Weitere Details finden Sie unter Verwendung von Lambda mit Amazon SQS.	18. November 2019

Erstellen von Anwendungen in der Lambda-Konsole	Die Anwendungserstellung in der Lambda-Konsole ist jetzt allgemein verfügbar. Anweisungen finden Sie unter Anwendungen in der Lambda-Konsole verwalten.	31. Oktober 2019
Erstellen von Anwendungen in der Lambda-Konsole (Beta)	Sie können nun eine Lambda-Anwendung mit einer integrierten fortlaufenden Bereitstellungs-Pipeline in der Lambda-Konsole erstellen. Die Konsole stellt Beispielanwendungen bereit, die Sie als Ausgangspunkt für Ihr eigenes Projekt verwenden können. Wählen Sie zwischen AWS CodeCommit und GitHub für die Quellcodeverwaltung. Jedes Mal, wenn Sie Änderungen zu Ihrem Repository übertragen, wird die enthaltene Pipeline automatisch erstellt und bereitgestellt. Anweisungen finden Sie unter Anwendungen in der Lambda-Konsole verwalten.	3. Oktober 2019

Leistungsverbesserungen für VPC-verbundene Funktionen	Lambda verwendet jetzt eine neue Art von Elastic-Network-Schnittstelle, die von allen Funktionen in einem Virtual-Private-Cloud-(VPC)-Subnetz gemeinsam genutzt wird. Wenn Sie eine Funktion mit einer VPC verbinden, erstellt Lambda eine Netzwerkschnittstelle für jede Kombination aus Sicherheitsgruppe und Subnetz, die Sie auswählen. Wenn die freigegebenen Netzwerkschnittstellen verfügbar sind, muss die Funktion bei der Skalierung nach oben keine zusätzlichen Netzwerkschnittstellen erstellen. Dies verbessert die Startup-Zeiten erheblich. Weitere Details finden Sie unter Konfigurieren einer Lambda-Funktion für den Zugriff auf Ressourcen in einer VPC.	03. September 2019

Stream-Batch-Einstellungen	Sie können jetzt ein Batch-Fenster für Amazon-DynamoDB- und Amazon-Kinesis-Ereignisquellen-Mappings konfigurieren. Konfigurieren Sie ein Batch-Fenster von bis zu fünf Minuten, um eingehende Datensätze zu puffern, bis ein vollständiger Batch verfügbar ist. Dies reduziert die Anzahl der Aufrufe Ihrer Funktion, wenn der Stream weniger aktiv ist.	29. August 2019
CloudWatch Integration von Logs & Insights	Die Überwachungsseite in der Lambda-Konsole enthält jetzt Berichte von Amazon CloudWatch Logs Insights. Einzelheiten finden Sie unter Überwachungsfunktionen in der AWS Lambda Konsole.	18. Juni 2019
Amazon Linux 2018.03	Die Lambda-Ausführungsumgebung wurde aktualisiert und verwendet jetzt Amazon Linux 2018.03. Weitere Details finden Sie unter Ausführungsumgebung.	21. Mai 2019

Node.js 10	Eine neue Laufzeit ist verfügbar für Node.js 10, nodejs10.x. Diese Laufzeit verwendet Node.js 10.15 und wird regelmäßig mit der neuesten Version von Node.js 10 aktualisiert. Node.js 10 ist auch die erste Laufzeit, die Amazon Linux 2 verwendet . Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	13. Mai 2019
GetLayerVersionByArn API	Verwenden Sie die GetLayerVersionByArn-API, um Layer-Versionsinformationen mit dem Versions-ARN als Eingabe herunterzuladen. Im Vergleich zu GetLayerVersionByArn können Sie den ARN direkt verwenden GetLayerVersion, anstatt ihn zu analysieren, um den Layer-Namen und die Versionsnummer abzurufen.	25. April 2019
Ruby	AWS Lambda unterstützt jetzt Ruby 2.5 mit einer neuen Runtime. Weitere Details finden Sie unter Erstellen von Lambda-Funktionen mit Ruby.	29. November 2018

Ebenen	Mit Lambda-Ebenen können Sie Bibliotheken, benutzerdefinierte Laufzeiten und andere Abhängigkeiten getrennt von Ihrem Funktionscode verpacken und bereitstellen. Geben Sie Ihre Ebenen für andere Konten oder die ganze Welt frei. Weitere Details finden Sie unter Lambda-Ebenen.	29. November 2018
Benutzerdefinierte Laufzeiten	Erstellen Sie eine benutzerdefinierte Laufzeit zur Ausführung von Lambda-Funktionen in Ihrer bevorzugten Programmiersprache. Weitere Details finden Sie unter Benutzerdefinierte Lambda-Laufzeiten.	29. November 2018
Application-Load-Balancer-Auslöser	Elastic Load Balancing unterstützt nun Lambda-Funktionen als Ziel für Application Load Balancers. Details finden Sie unter Verwenden von Lambda mit Application Load Balancern.	29. November 2018

Verwenden von Kinesis-HTTP/2-Stream-Konsumenten als Auslöser	Sie können mit Kinesis HTTP/2-Daten-Stream-Konsumenten Ereignisse an sende AWS Lambda. Stream-Konsumenten haben einen dedizierten Lesedurchsatz aus jedem Shard in Ihrem Daten-Stream und verwenden HTTP/2, um die Latenz zu minimieren. Details finden Sie unter Verwenden von Lambda mit Kinesis.	19. November 2018
Python 3.7	AWS Lambda unterstützt jetzt Python 3.7 mit einer neuen Runtime. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Python.	19. November 2018
Erhöhung des Nutzlastlimits für asynchronen Funktionsaufruf	Die maximale Nutzlastgröße für asynchrone Aufrufe wurde von 128 KB auf 256 KB erhöht, was der maximale Nachrichtengröße eines Amazon-SNS-Auslösers entspricht. Weitere Details finden Sie unter Lambda-Kontingente.	16. November 2018
AWS GovCloud Region (USA-Ost)	AWS Lambda ist jetzt in der Region AWS GovCloud (USA-Ost) verfügbar.	12. November 2018

Die AWS SAM Themen wurden in ein separates Entwicklerhandbuch verschoben	Eine Reihe von Themen befasste sich mit der Entwicklung serverloser Anwendungen mithilfe von AWS Serverless Application Model (AWS SAM). Diese Themen wurden in das AWS Serverless Application Model -Entwicklerhandbuch verschoben.	25. Oktober 2018
Anzeigen von Lambda-Anwendungen in der Konsole	Sie können den Status Ihrer Lambda-Anwendungen auf der Seite Anwendungen in der Lambda-Konsole anzeigen. Auf dieser Seite wird der Status des AWS CloudFormation Stacks angezeigt. Sie enthält Links zu Seiten mit weiteren Informationen zu den Ressourcen im Stack. Sie können auch aggregierte Metriken für die Anwendung anzeigen und benutzerdefinierte Überwachungs-Dashboards erstellen.	11. Oktober 2018
Timeout-Limit für die Funktionsausführung	Für langlaufende Funktionen wurde das maximal konfigurierbare Ausführungs-Timeout von 5 Minuten auf 15 Minuten erhöht. Weitere Details finden Sie unter Lambda-Limits.	10. Oktober 2018

Support für die PowerShell Kernsprache in AWS Lambda	AWS Lambda unterstützt jetzt die PowerShell Core-Sprache. Weitere Informationen finden Sie unter Programmiermodell für die Erstellung von Lambda-Funktionen in. PowerShell	11. September 2018
Support für.NET Core 2.1.0 Runtime in AWS Lambda	AWS Lambda unterstützt jetzt die.NET Core 2.1.0 Runtime. Weitere Informationen finden Sie unter .NET Core-CLI.	9. Juli 2018
Aktualisierungen jetzt über RSS verfügbar	Sie können jetzt einen RSS-Feed abonnieren, um Releases für dieses Handbuch nachzufolgen.	5. Juli 2018
Unterstützung für Amazon SQS als Ereignisquelle	AWS Lambda unterstützt jetzt Amazon Simple Queue Service (Amazon SQS) als Ereignisquelle. Weitere Informationen finden Sie unter Aufrufen von Lambda-Funktionen.	28. Juni 2018
China (Ningxia)-Region	AWS Lambda ist jetzt in der Region China (Ningxia) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	28. Juni 2018

Frühere Updates

In der folgenden Tabelle sind die wichtigen Änderungen in jeder Version des AWS Lambda - Entwicklerhandbuchs vor Juni 2018 beschrieben.

Änderung	Beschreibung	Datum
Laufzeitunterstützung für Node.js-Laufzeitversion 8.10	AWS Lambda unterstützt jetzt die Runtime-Version 8.10 von Node.js. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	2. April 2018
Funktions- und Aliasänderungs-IDs	AWS Lambda unterstützt jetzt Revisions-IDs für Ihre Funktionsversionen und Aliase. Mit diesen IDs können Sie bedingte Aktualisierungen bei der Aktualisierung Ihrer Funktionsversion oder Alias-Ressourcen nachverfolgen und anwenden.	25. Januar 2018
Unterstützung für Go und .NET 2.0 bei Laufzeit	AWS Lambda hat Runtime-Unterstützung für Go und .NET 2.0 hinzugefügt. Weitere Informationen erhalten Sie unter Erstellen von Lambda-Funktionen mit Go und Erstellen von Lambda-Funktionen mit C#.	15. Januar 2018
Umgestaltung der Konsole	AWS Lambda hat eine neue Lambda-Konsole eingeführt, um Ihre Erfahrung zu vereinfachen, und einen Cloud9-Code-Editor hinzugefügt, mit dem Sie Ihren Funktionscode besser debuggen und überarbeiten können. Weitere Informationen finden Sie unter Bearbeiten von Code mit dem Lambda-Konsoleneditor.	30. November 2017
Festlegen von Gleichzeitigkeitslimits für einzelne Funktionen	AWS Lambda unterstützt jetzt das Setzen von Parallelitätslimits für einzelne Funktionen. Weitere Informationen finden Sie unter Reservierte Parallelität für eine Funktion konfigurieren.	30. November 2017
Verschiebung von Datenverkehr mithilfe von Aliassen	AWS Lambda unterstützt jetzt die Verlagerung von Traffic mit Aliasnamen. Weitere Informationen finden Sie unter Erstellen Sie fortlaufende Bereitstellungen für Lambda-Funktionen.	28. November 2017

Änderung	Beschreibung	Datum
Graduelle Code-Bereitstellung	AWS Lambda unterstützt jetzt die sichere Bereitstellung neuer Versionen Ihrer Lambda-Funktion mithilfe von Code Deploy. Weitere Informationen finden Sie unter Graduelle Code-Bereitstellung.	28. November 2017
Region China (Peking)	AWS Lambda ist jetzt in der Region China (Peking) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	9. November 2017
Einführung von SAM Local	AWS Lambda stellt SAM Local (jetzt bekannt als SAM CLI) vor, ein AWS CLI Tool, das Ihnen eine Umgebung bietet, in der Sie Ihre serverlosen Anwendungen lokal entwickeln, testen und analysieren können, bevor Sie sie in die Lambda-Laufzeit hochladen. Weitere Informationen finden Sie unter Testen und Debuggen von Serverless Anwendungen.	11. August 2017
Region Kanada (Zentral)	AWS Lambda ist jetzt in der Region Kanada (Zentral) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	22. Juni 2017
South America (São Paulo) Region	AWS Lambda ist jetzt in der Region Südamerika (São Paulo) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	6. Juni 2017
AWS Lambda Unterstützung für AWS X-Ray.	In Lambda wird die Unterstützung von X-Ray eingeführt; damit können Sie Leistungsprobleme bei Ihren Lambda-Anwendungen erkennen, analysieren und optimieren. Weitere Informationen finden Sie unter Visualisieren Sie Lambda-Funktionsaufrufe mit AWS X-Ray.	19. April 2017

Änderung	Beschreibung	Datum
Region Asien-Pazifik (Mumbai)	AWS Lambda ist jetzt in der Region Asien-Pazifik (Mumbai) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	28. März 2017
AWS Lambda unterstützt jetzt Node.js Runtime v6.10	AWS Lambda Unterstützung für Node.js Runtime v6.10 hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	22. März 2017
Region Europa (London)	AWS Lambda ist jetzt in der Region Europa (London) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	1. Februar 2017
AWS Lambda Unterstützung für.NET-Runtime, Lambda @Edge (Preview), Dead Letter Queues und automatisiertes Deployment serverloser Anwendungen.	AWS Lambda Unterstützung für C# hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit C#. Mit Lambda @Edge können Sie Lambda-Funktionen an den AWS Edge-Standorten als Reaktion auf CloudFront Ereignisse ausführen. Weitere Informationen finden Sie unter Verwenden von AWS Lambda mit CloudFront Lambda@Edge.	3. Dezember 2016
AWS Lambda fügt Amazon Lex als unterstützte Ereignisquelle hinzu.	Mit Lambda und Amazon Lex können Sie Chatbots für verschiedene Services wie Slack und Facebook schnell erstellen. Weitere Informationen finden Sie unter Verwenden von AWS Lambda mit Amazon Lex.	30. November 2016
US West (N. California) Region	AWS Lambda ist jetzt in der Region USA West (Nordkalifornien) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	21. November 2016

Änderung	Beschreibung	Datum
Einführung der Einstellungen AWS SAM für die Erstellung und Bereitstellung von Lambda-basierten Anwendungen und die Verwendung von Umgebungsvariablen für die Konfiguration von Lambda-Funktionen.	AWS SAM: Sie können jetzt den verwenden, AWS SAM um die Syntax für das Ausdrücken von Ressourcen in einer serverlosen Anwendung zu definieren. Sie stellen Ihre Anwendung bereit, indem Sie die benötigten Ressourcen einfach zusammen mit den zugehörigen Berechtigungsrichtlinien als Teil der Anwendung in einer AWS CloudFormation -Vorlagendatei angeben (die in JSON oder YAML geschrieben ist), Ihre Bereitstellungsartefakte paketieren und die Vorlage bereitstellen. Weitere Informationen finden Sie unter AWS Lambda Anwendungen. Umgebungsvariablen: Sie können Umgebungsvariablen verwenden, um Konfigurationseinstellungen für Ihre Lambda-Funktion vorzunehmen, ohne dabei den Code für die Funktion ändern zu müssen. Weitere Informationen finden Sie unter Verwenden Sie Lambda-Umgebungsvariablen, um Werte im Code zu konfigurieren.	18. November 2016
Region Asien-Pazifik (Seoul)	AWS Lambda ist jetzt in der Region Asien-Pazifik (Seoul) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	29. August 2016
Asia Pacific (Sydney) Region	Lambda ist jetzt in der Region Asien-Pazifik (Sydney) verfügbar. Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	23. Juni 2016
Aktualisierungen für die Lambda-Konsole	Die Lambda-Konsole wurde aktualisiert, um das Verfahren für die Erstellung von Rollen zu vereinfachen.	23. Juni 2016
AWS Lambda unterstützt jetzt Node.js Runtime v4.3	AWS Lambda Unterstützung für Node.js Runtime v4.3 hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Node.js.	07. April 2016

Änderung	Beschreibung	Datum
Region Europa (Frankfurt)	Lambda ist jetzt in der Region Europa (Frankfurt) verfügbar . Weitere Informationen zu Lambda-Regionen und -Endpunkten finden Sie unter Regionen und Endpunkte in der Allgemeine AWS-Referenz.	14. März 2016
VPC-Unterstützung	Sie können eine Lambda-Funktion jetzt für den Zugriff auf Ressourcen in Ihrer VPC konfigurieren. Weitere Informationen finden Sie unter Lambda-Funktionen Zugriff auf Ressourcen in einer Amazon VPC gewähren.	11. Februar 2016
Die Lambda-Laufzeitumgebung wurde aktualisiert.	Die Ausführungsumgebung wurde aktualisiert.	4. November 2015

Änderung	Beschreibung	Datum
Unterstützung der Versioning, Python für die Entwicklung von Code für Lambda-Funktionen, geplante Ereignisse und Erhöhung der Ausführungszeit	Sie können den Code für Ihre Lambda-Funktionen jetzt mit Python entwickeln. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Python. Versioning: Sie können eine oder mehrere Versionen einer Lambda-Funktion pflegen. Mit der Versioning können Sie steuern, welche Versionen einer Lambda-Funktion in verschiedenen Umgebungen ausgeführt werden (z. B. in einer Entwicklungs-, Test- oder produktiven Umgebung). Weitere Informationen finden Sie unter Versionen der Lambda-Funktion. Geplante Ereignisse: Außerdem können Sie Lambda mithilfe der Lambda-Konsole so einrichten, dass Ihr Code regelmäßig und nach Plan abgerufen wird. Sie können einen festen Takt für die Ausführung (eine Anzahl von Stunden, Tagen oder Wochen) oder einen Cron-Ausdruck angeben. Weitere Informationen finden Sie unter Verwenden von Lambda mit Amazon EventBridge Scheduler. Erhöhung der Ausführungszeit: Sie können Ihre Lambda-Funktion jetzt so einrichten, dass sie bis zu fünf Minuten lang ausgeführt wird; dadurch werden Funktionen mit längeren Laufzeiten ermöglicht, z. B. Aufträge für die Erfassung oder Verarbeitung großer Datenvolumen.	08. Oktober 2015

Änderung	Beschreibung	Datum
Unterstützung für DynamoDB Streams	DynamoDB Streams ist jetzt allgemein verfügbar; Sie können die Funktion in allen Regionen verwenden, in denen DynamoDB verfügbar ist. Sie können DynamoDB Streams für Ihre Tabelle aktivieren und eine Lambda-Funktion als Auslöser für die Tabelle verwenden. Auslöser sind benutzerdefinierte Aktionen, die als Reaktion auf Aktualisierungen der DynamoDB-Tabelle ausgeführt werden. Ein Beispiel-Walkthrough finden Sie unte Tutorial: Verwendung AWS Lambda mit Amazon DynamoDB DynamoDB-Streams .	14. Juli 2015
Lambda unterstützt jetzt den Aufruf von Lambda-Funktionen mit REST-kompatiblen Clients.	Bisher benötigten Sie die AWS SDKs (z. B. SDK for Java, SDK for Android oder AWS SDK for iOS), um Ihre Lambda-Funktion von Ihrer Web-, Mobil- oder AWS IoT-Anwendung aus aufzurufen. AWS Lambda unterstützt jetzt Aufrufe einer Lambda-Funktion mit REST-kompatiblen Clients über eine benutzerdefinierte API, die Sie mithilfe des Amazon API Gateway erstellen können. Sie können Anfragen an die Endpunkt-URL Ihrer Lambda-Funktion senden. Sie können die Sicherheitseinstellungen an dem Endpunkt für einen offenen Zugriff konfigurieren, den Zugriff mithilfe von AWS Identity and Access Management (IAM) autorisieren oder API-Schlüssel verwenden, um den Zugriff auf Lambda-Funktionen durch andere Benutzer zu erfassen. Ein Beispielübung mit ersten Schritten finden Sie unter Aufrufen einer Lambda-Funktion mithilfe eines Amazon API Gateway Gateway-Endpunkts. Weitere Informationen zum Amazon API Gateway finden Sie unter https://aws.amazon.com/api-gateway/.	09. Juli 2015

Änderung	Beschreibung	Datum
In der Lambda-Konsole werden jetzt Vorlagen bereitgestellt, mit denen Sie Lambda-Funktionen einfach erstellen und testen können.	In der Lambda-Konsole wird eine Reihe von Vorlagen bereitgestellt. Jede Vorlage enthält eine Beispielkonfiguration für eine Ereignisquelle sowie Beispielcode für eine Lambda-Funktion, mit dem Sie Lambda-basierte Anwendungen einfach erstellen können. Die Vorlagen sind jetzt in allen Lambda-Übungen mit ersten Schritten enthalten. Weitere Informationen finden Sie unter Erste Schritte mit Lambda.	09. Juli 2015
Lambda unterstützt jetzt Lambda-Funktionen, die in Java geschrieben wurden.	Sie können Lambda-Code jetzt in Java verfassen. Weitere Informationen finden Sie unter Erstellen von Lambda-Funktionen mit Java.	15. Juni 2015
Lambda unterstützt bei der Erstellung oder Aktualisierung einer Lambda-Funktion jetzt die Angabe eines Amazon-S3-Objekts als ZIP-Datei.	Sie können das Bereitstellungspaket für eine Lambda-Funktion (ZIP-Datei) in einen Amazon-S3-Bucket in derselben Region uploaden, in der Sie die Lambda-Funktion erstellen möchten. Danach können Sie bei der Erstellung oder Aktualisierung der Lambda-Funktion den Bucket-Namen und Objektschlüsselnamen angeben.	28. Mai 2015

Änderung	Beschreibung	Datum
In Lambda wurde die allgemeine Unterstützung von mobilen Backends hinzugefügt.	Lambda ist jetzt allgemein für den produktiven Einsatz verfügbar. In dieser Version werden außerdem neue Funktionen eingeführt, mit denen die Erstellung von Backends für Mobiltelefone, Tablets und das Internet of Things (IoT) vereinfacht wird; diese können mit Lambda automatisch skaliert werden, ohne dass eine Infrastruktur bereitgestellt oder verwaltet werden muss. Lambda unterstützt jetzt sowohl synchrone (in Echtzeit) als auch asynchrone Ereignisse. Es sind zusätzliche Funktionen enthalten, u. a. für eine einfachere Konfiguration und Verwaltung von Ereignisquellen. Das Berechtigungsmodell und das Programmiermodell wurden durch die Einführung von Ressourcenrichtlinien für Lambda-Funktionen vereinfacht. Die Dokumentation wurde entsprechend aktualisiert. Weitere Informationen finden Sie unter den folgenden Themen: Erste Schritte mit Lambda AWS Lambda	9. April 2015
Vorversion	Vorversion des AWS Lambda -Entwicklerhandbuchs.	13. November 2014

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.