Table of Contents

What Is Amazon API Gateway ................................................................. 1
Architecture of API Gateway ..................................................................... 1
Features of API Gateway ........................................................................ 2
API Gateway Use Cases ............................................................................ 3
  Use API Gateway to Create REST APIs ....................................................... 3
  Use API Gateway to Create WebSocket APIs .............................................. 3
Who Uses API Gateway? ......................................................................... 4
Accessing API Gateway ............................................................................ 4
Part of AWS Serverless Infrastructure ....................................................... 5
How to Get Started with Amazon API Gateway ........................................ 5
API Gateway Concepts ............................................................................. 5
API Gateway Pricing ................................................................................. 8
API Gateway Compliance .......................................................................... 9
  PCI DSS ................................................................................................... 9
  HIPAA ................................................................................................... 9
Prerequisites: Get Ready to Build an API in API Gateway ...................... 10
  Sign Up for an AWS Account ................................................................. 10
  Create an IAM Administrator User ......................................................... 10
Create a REST API with Lambda Integrations ......................................... 11
  Step 1: Create a Lambda Function in the Lambda Console ..................... 11
  Step 2: Create a REST API in the API Gateway Console ......................... 11
  Step 3: Deploy Your REST API in the API Gateway Console .................. 14
  Step 4: Create a Second Lambda Function in the Lambda Console .......... 14
  Step 5: Add a Resource, Method, and Parameter to the REST API in the API Gateway Console 15
  Next Steps .......................................................................................... 17
Create a REST API with a Mock Integration ........................................... 18
  Step 1: Create the API ........................................................................ 18
  Step 2: Create the Mock Integration ..................................................... 20
  Step 3: Define the Successful Response ................................................ 21
  Step 4: Add an HTTP 500 Status Code and Error Message .................... 21
  Step 5: Test the Mock Integration ......................................................... 22
  Next Steps ........................................................................................ 24
Amazon API Gateway Videos .................................................................. 25
  Amazon API Gateway Videos from Twitch Build On AWS Event Series .... 25
  Other Amazon API Gateway Videos ..................................................... 25
Tutorials ................................................................................................... 26
  Build an API with Lambda Integration ..................................................... 26
    TUTORIAL: Hello World API with Lambda Proxy Integration .................. 26
    TUTORIAL: Build an API with Cross-Account Lambda Proxy Integration .... 31
    TUTORIAL: Build an API with Lambda Non-Proxy Integration ................ 33
  TUTORIAL: Create a REST API by Importing an Example ....................... 42
  Build an API with HTTP Integration ..................................................... 50
    TUTORIAL: Build an API with HTTP Proxy Integration ........................ 51
    TUTORIAL: Build an API with HTTP Non-Proxy Integration .................. 56
  TUTORIAL: Build an API with Private Integration ................................. 85
  TUTORIAL: Build an API with AWS Integration ..................................... 87
    Prerequisites ....................................................................................... 88
    Step 1: Create the Resource ............................................................... 88
    Step 2: Create the GET Method ........................................................... 89
    Step 3: Create the AWS Service Proxy Execution Role ......................... 89
    Step 4: Specify Method Settings and Test the Method .......................... 90
    Step 5: Deploy the API ..................................................................... 91
    Step 6: Test the API ......................................................................... 91
What Is Amazon API Gateway?

Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services as well as data stored in the AWS Cloud. As an API Gateway API developer, you can create APIs for use in your own client applications (apps). Or you can make your APIs available to third-party app developers. For more information, see the section called “Who Uses API Gateway?” (p. 4).

API Gateway creates REST APIs that:

- Are HTTP-based.
- Adhere to the REST protocol, which enables stateless client-server communication.
- Implement standard HTTP methods such as GET, POST, PUT, PATCH and DELETE.

For more information about API Gateway REST APIs, see the section called “Use API Gateway to Create REST APIs” (p. 3) and the section called “Creating a REST API” (p. 177).

API Gateway creates WebSocket APIs that:

- Adhere to the WebSocket protocol, which enables stateful, full-duplex communication between client and server.
- Route incoming messages and based on message content.

For more information about API Gateway WebSocket APIs, see the section called “Use API Gateway to Create WebSocket APIs” (p. 3) and the section called “About WebSocket APIs” (p. 597).

Topics

- Architecture of API Gateway (p. 1)
- Features of API Gateway (p. 2)
- API Gateway Use Cases (p. 3)
- Accessing API Gateway (p. 4)
- Part of AWS Serverless Infrastructure (p. 5)
- How to Get Started with Amazon API Gateway (p. 5)
- Amazon API Gateway Concepts (p. 5)
- API Gateway Pricing (p. 8)
- API Gateway Compliance (p. 9)

Architecture of API Gateway

The following diagram shows API Gateway architecture.
This diagram illustrates how the APIs you build in Amazon API Gateway provide you or your developer customers with an integrated and consistent developer experience for building AWS serverless applications. API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. API Gateway acts as a "front door" for applications to access data, business logic, or functionality from your backend services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications.

Features of API Gateway

Amazon API Gateway offers features such as the following:

- Support for stateful (WebSocket (p. 597)) and stateless (REST (p. 177)) APIs.
- Powerful, flexible authentication (p. 346) mechanisms, such as AWS Identity and Access Management policies, Lambda authorizer functions, and Amazon Cognito user pools.
- Developer portal (p. 630) for publishing your APIs.
- Canary release deployments (p. 666) for safely rolling out changes.
- CloudTrail (p. 568) logging and monitoring of API usage and API changes.
- CloudWatch access logging and execution logging, including the ability to set alarms. For more information, see the section called “Monitor API Execution with Amazon CloudWatch” (p. 569) and the section called “Monitor WebSocket API Execution with CloudWatch” (p. 617).
- Ability to use AWS CloudFormation templates to enable API creation. For more information, see Amazon API Gateway Resource Types Reference and Amazon API Gateway V2 Resource Types Reference.
- Support for custom domain names (p. 641).
- Integration with AWS WAF (p. 430) for protecting your APIs against common web exploits.
- Integration with AWS X-Ray (p. 558) for understanding and triaging performance latencies.

For a complete list of API Gateway feature releases, see Document History (p. 696).
API Gateway Use Cases

Topics

- Use API Gateway to Create REST APIs (p. 3)
- Use API Gateway to Create WebSocket APIs (p. 3)
- Who Uses API Gateway? (p. 4)

Use API Gateway to Create REST APIs

An API Gateway REST API is made up of resources and methods. A resource is a logical entity that an app can access through a resource path. A method corresponds to a REST API request that is submitted by the user of your API and the response returned to the user.

For example, `/incomes` could be the path of a resource representing the income of the app user. A resource can have one or more operations that are defined by appropriate HTTP verbs such as GET, POST, PUT, PATCH, and DELETE. A combination of a resource path and an operation identifies a method of the API. For example, a POST `/incomes` method could add an income earned by the caller, and a GET `/expenses` method could query the reported expenses incurred by the caller.

The app does not need to know where the requested data is stored and fetched from on the backend. In API Gateway REST APIs, the frontend is encapsulated by method requests and method responses. The API interfaces with the backend by means of integration requests and integration responses.

For example, with DynamoDB as the backend, the API developer sets up the integration request to forward the incoming method request to the chosen backend. The setup includes specifications of an appropriate DynamoDB action, required IAM role and policies, and required input data transformation. The backend returns the result to API Gateway as an integration response. To route the integration response to an appropriate method response (of a given HTTP status code) to the client, you can configure the integration response to map required response parameters from integration to method. You then translate the output data format of the backend to that of the frontend, if necessary. API Gateway enables you to define a schema or model for the payload to facilitate setting up the body mapping template.

API Gateway provides REST API management functionality such as:

- Support for generating SDKs and creating API documentation using API Gateway extensions to OpenAPI
- Throttling of HTTP requests

Use API Gateway to Create WebSocket APIs

In a WebSocket API, the client and the server can both send messages to each other at any time. Backend servers can easily push data to connected users and devices, avoiding the need to implement complex polling mechanisms.

For example, you could build a serverless application using an API Gateway WebSocket API and AWS Lambda to send and receive messages to and from individual users or groups of users in a chat room. Or you could invoke backend services such as AWS Lambda, Amazon Kinesis, or an HTTP endpoint based on message content.

You can use API Gateway WebSocket APIs to build secure, real-time communication applications without having to provision or manage any servers to manage connections or large-scale data exchanges. Targeted use cases include real-time applications such as:
Chat applications
Real-time dashboards such as stock tickers
Real-time alerts and notifications

API Gateway provides WebSocket API management functionality such as:

- Monitoring and throttling of connections and messages
- Using AWS X-Ray to trace messages as they travel through the APIs to backend services
- Easy integration with HTTP/HTTPS endpoints

Who Uses API Gateway?

There are two kinds of developers who use API Gateway: API developers and app developers.

An API developer creates and deploys an API to enable the required functionality in API Gateway. The API developer must be an IAM user in the AWS account that owns the API.

An app developer builds a functioning application to call AWS services by invoking a WebSocket or REST API created by an API developer in API Gateway.

The app developer is the customer of the API developer. The app developer does not need to have an AWS account, provided that the API either does not require IAM permissions or supports authorization of users through third-party federated identity providers supported by Amazon Cognito user pool identity federation. Such identity providers include Amazon, Amazon Cognito User Pools, Facebook, and Google.

Creating and Managing an API Gateway API

An API developer works with the API Gateway service component for API management, named apigateway, to create, configure, and deploy an API. Each API includes a set of resources and methods. A resource is a logical entity that an app can access through a resource path.

As an API developer, you can create and manage an API by using the API Gateway console, described in Getting Started with Amazon API Gateway (p. 10), or by calling the API Gateway V1 and V2 API References (p. 686). There are several ways to call this API. They include using the AWS Command-Line Interface (CLI), or by using an AWS SDK. In addition, you can enable API creation with AWS CloudFormation templates or (in the case of REST APIs) API Gateway Extensions to OpenAPI (p. 575). For a list of regions where API Gateway is available, as well as the associated control service endpoints, see Regions and Endpoints.

Calling an API Gateway API

An app developer works with the API Gateway service component for API execution, named execute-api, to invoke an API that was created or deployed in API Gateway. The underlying programming entities are exposed by the created API. There are several ways to call such an API. You can use the API Gateway console to test invoking the API. For REST APIs, you can use a REST API client, such as cURL or POSTMAN, or an SDK generated by API Gateway for the API to invoke the API.

Accessing API Gateway

You can access Amazon API Gateway in the following ways:

- **AWS Management Console** – The procedures throughout this guide explain how to use the AWS Management Console to perform tasks.
• **AWS SDKs** – If you’re using a programming language that AWS provides an SDK for, you can use an SDK to access API Gateway. SDKs simplify authentication, integrate easily with your development environment, and provide access to API Gateway commands. For more information, see Tools for Amazon Web Services.

• **API Gateway V1 and V2 APIs** – If you’re using a programming language that an SDK isn’t available for, see the Amazon API Gateway Version 1 API Reference and Amazon API Gateway Version 2 API Reference.

• **AWS Command Line Interface** – For more information, see Getting Set Up with the AWS Command Line Interface in the AWS Command Line Interface User Guide.

• **AWS Tools for Windows PowerShell** – For more information, see Setting up the AWS Tools for Windows PowerShell in the AWS Tools for Windows PowerShell User Guide.

### Part of AWS Serverless Infrastructure

Together with AWS Lambda, API Gateway forms the app-facing part of the AWS serverless infrastructure. For an app to call publicly available AWS services, you can use Lambda to interact with required services and expose Lambda functions through API methods in API Gateway. AWS Lambda runs your code on a highly available computing infrastructure. It performs the necessary execution and administration of computing resources. To enable serverless applications, API Gateway supports streamlined proxy integrations (p. 215) with AWS Lambda and HTTP endpoints.

### How to Get Started with Amazon API Gateway

For a quick introduction to Amazon API Gateway, see the following topics:

- **Getting Started with API Gateway** (p. 10), which provides walkthroughs and videos that tell how to create APIs using Amazon API Gateway.
- **Announcing WebSocket APIs in Amazon API Gateway**, which tells how to create a WebSocket API.

### Amazon API Gateway Concepts

**API Gateway**

API Gateway is an AWS service that supports the following:

- Creating, deploying, and managing a REST application programming interface (API) to expose backend HTTP endpoints, AWS Lambda functions, or other AWS services.
- Creating, deploying, and managing a WebSocket API to expose AWS Lambda functions or other AWS services.
- Invoking exposed API methods through the frontend HTTP and WebSocket endpoints.

**API Gateway REST API**

A collection of HTTP resources and methods that are integrated with backend HTTP endpoints, Lambda functions, or other AWS services. This collection can be deployed in one or more stages. Typically, API resources are organized in a resource tree according to the application logic. Each API resource can expose one or more API methods that have unique HTTP verbs supported by API Gateway.

**API Gateway WebSocket API**

A collection of WebSocket routes and route keys that are integrated with backend HTTP endpoints, Lambda functions, or other AWS services. The collection can be deployed in one or more stages.
API methods are invoked through frontend WebSocket connections that you can associate with a registered custom domain name.

API deployment

A point-in-time snapshot of your API Gateway API. To be available for clients to use, the deployment must be associated with one or more API stages.

API developer

Your AWS account that owns an API Gateway deployment (for example, a service provider that also supports programmatic access.)

API endpoint

A hostname for an API in API Gateway that is deployed to a specific region. The hostname is of the form `{api-id}.execute-api.{region}.amazonaws.com`. The following types of API endpoints are supported:

- Edge-optimized API endpoint (p. 6)
- Private API endpoint (p. 7)
- Regional API endpoint (p. 8)

API key

An alphanumeric string that API Gateway uses to identify an app developer who uses your REST or WebSocket API. API Gateway can generate API keys on your behalf, or you can import them from a CSV file. You can use API keys together with Lambda authorizers (p. 380) or usage plans (p. 432) to control access to your APIs.

See API endpoints (p. 6).

API owner

See API developer (p. 6).

API stage

A logical reference to a lifecycle state of your REST or WebSocket API (for example, ‘dev’, ‘prod’, ‘beta’, ‘v2’). API stages are identified by API ID and stage name.

App developer

An app creator who may or may not have an AWS account and interacts with the API that you, the API developer, have deployed. App developers are your customers. An app developer is typically identified by an API key (p. 6).

Callback URL

When a new client is connected to via a WebSocket connection, you can call an integration in API Gateway to store the client's callback URL. You can then use that callback URL to send messages to the client from the backend system.

Developer portal

An application that allows your customers to register, discover, and subscribe to your API products (API Gateway usage plans), manage their API keys, and view their usage metrics for your APIs.

Edge-optimized API endpoint

The default host name of an API Gateway API that is deployed to the specified region while using a CloudFront distribution to facilitate client access typically from across AWS regions. API requests are routed to the nearest CloudFront Point of Presence (POP), which typically improves connection time for geographically diverse clients.

See API endpoints (p. 6).
Integration request

The internal interface of a WebSocket API route or REST API method in API Gateway, in which you map the body of a route request or the parameters and body of a method request to the formats required by the backend.

Integration response

The internal interface of a WebSocket API route or REST API method in API Gateway, in which you map the status codes, headers, and payload that are received from the backend to the response format that is returned to a client app.

Mapping template

A scripts in Velocity Template Language (VTL) that transforms a request body from the frontend data format to the backend data format, or that transforms a response body from the backend data format to the frontend data format. Mapping templates can be specified in the integration request or in the integration response. They can reference data made available at run time as context and stage variables. The mapping can be as simple as an identity transform that passes the headers or body through the integration as-is from the client to the backend for a request. The same is true for a response, in which the payload is passed from the backend to the client.

Method request

The public interface of a REST API method in API Gateway that defines the parameters and body that an app developer must send in requests to access the backend through the API.

Method response

The public interface of a REST API that defines the status codes, headers, and body models that an app developer should expect in responses from the API.

Mock integration

In a mock integration, API responses are generated from API Gateway directly, without the need for an integration backend. As an API developer, you decide how API Gateway responds to a mock integration request. For this, you configure the method's integration request and integration response to associate a response with a given status code.

Model

A data schema specifying the data structure of a request or response payload. A model is required for generating a strongly typed SDK of an API. It is also used to validate payloads. A model is convenient for generating a sample mapping template to initiate creation of a production mapping template. Although useful, a model is not required for creating a mapping template.

Private API

See Private API endpoint (p. 7).

Private API endpoint

An API endpoint that is exposed through interface VPC endpoints and allows a client to securely access private API resources inside a VPC. Private APIs are isolated from the public internet, and they can only be accessed using VPC endpoints for API Gateway that have been granted access.

Private integration

An API Gateway integration type for a client to access resources inside a customer's VPC through a private REST API endpoint without exposing the resources to the public internet.

Proxy integration

A simplified API Gateway integration configuration for a REST or WebSocket API. You can set up a proxy integration as an HTTP proxy integration or a Lambda proxy integration. For HTTP proxy integration, API Gateway passes the entire request and response between the frontend and an HTTP backend. For Lambda proxy integration, API Gateway sends the entire request as input to a backend
Lambda function. API Gateway then transforms the Lambda function output to a frontend HTTP response. In REST APIs, proxy integration is most commonly used with a proxy resource, which is represented by a greedy path variable (e.g., `{proxy+}`) combined with a catch-all ANY method.

**Regional API endpoint**

The host name of an API that is deployed to the specified region and intended to serve clients, such as EC2 instances, in the same AWS region. API requests are targeted directly to the region-specific API Gateway without going through any CloudFront distribution. For in-region requests, a regional endpoint bypasses the unnecessary round trip to a CloudFront distribution. In addition, you can apply latency-based routing on regional endpoints to deploy an API to multiple regions using the same regional API endpoint configuration, set the same custom domain name for each deployed API, and configure latency-based DNS records in Route 53 to route client requests to the region that has the lowest latency.

See API endpoints (p. 6).

**Route**

A WebSocket route in API Gateway is used to direct incoming messages to a specific integration, such as an AWS Lambda function, based on the content of the message. When you define your WebSocket API, you specify a route key and an integration backend. The route key is an attribute in the message body. When the route key is matched in an incoming message, the integration backend is invoked. A default route can also be set for non-matching route keys or to specify a proxy model that passes the message through as-is to backend components that perform the routing and process the request.

**Route request**

The public interface of a WebSocket API method in API Gateway that defines the body that an app developer must send in the requests to access the backend through the API.

**Route response**

The public interface of a WebSocket API that defines the status codes, headers, and body models that an app developer should expect from API Gateway.

**Usage plan**

A usage plan (p. 432) provides selected API clients with access to one or more deployed REST or WebSocket APIs. You can use a usage plan to configure throttling and quota limits, which are enforced on individual client API keys.

**WebSocket connection**

API Gateway maintains a persistent connection between clients and API Gateway itself. There is no persistent connection between API Gateway and backend integrations such as Lambda functions; backend services are invoked as needed, based on the content of messages received from clients.

---

**API Gateway Pricing**

For general API Gateway region-specific pricing information, see Amazon API Gateway Pricing.

The following lists the exceptions to the general pricing scheme:

- API caching in Amazon API Gateway is not eligible for the AWS Free Tier.
- Calling methods with the authorization type of AWS_IAM, CUSTOM, and COGNITO_USER_POOLS are not charged for authorization and authentication failures.
- Calls to methods that require API keys are not charged when API keys are missing or invalid.
- API Gateway-throttled requests are not charged when the request rate or burst rate exceeds the preconfigured limits.
• Usage plan-throttled requests are not charged when rate limits or quota exceed the preconfigured limits.

API Gateway Compliance

For information about API Gateway compliance with various security compliance regulations and audits standards, see the following pages:

• AWS Cloud Compliance
• AWS Services in Scope by Compliance Program

In addition, see the following for details about how API Gateway is compliant with the PCI DSS and HIPAA standards.

PCI DSS

API Gateway supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS). For more information about PCI DSS, including how to request a copy of the AWS PCI Compliance Package, see PCI DSS Level 1.

HIPAA

This is a HIPAA Eligible Service. For more information about AWS, U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), and using AWS services to process, store, and transmit protected health information (PHI), see HIPAA Overview.
Getting Started with Amazon API Gateway

To help you get started using Amazon API Gateway, go through the following hands-on walkthroughs and other resources:

- **Prerequisites: Get Ready to Build an API in API Gateway** discusses how to create an AWS account and set up an IAM administrator user.
- **Create a REST API with Lambda Integrations** shows how to create REST APIs with Lambda functions on the backend. Both proxy and non-proxy integration techniques are included.
- **Create a REST API with a Mock Integration** shows how to create a REST API without an actual backend.
- **TUTORIAL: Create a REST API by Importing an Example** shows how to create an example API by importing an OpenAPI 2.0 file.
- **Create a WebSocket API** shows how to create a WebSocket API in API Gateway.
- **Amazon API Gateway Videos** provides links to videos that discuss getting started with API Gateway.

Prerequisites: Get Ready to Build an API in API Gateway

**Topics**

- **Sign Up for an AWS Account** (p. 10)
- **Create an IAM Administrator User** (p. 10)

Before using Amazon API Gateway for the first time, you must have an AWS account.

In many of the tutorials in Getting Started with API Gateway (p. 10) and Tutorials (p. 26), the necessary IAM policies are created for you. However, when you begin creating your own API, you'll need to study the information below and in the section called “Use IAM Permissions” (p. 362).

**Sign Up for an AWS Account**

To use Amazon API Gateway, AWS Lambda, and other AWS services, you need an AWS account. If you don't have an account, visit aws.amazon.com and choose Create an AWS Account. For detailed instructions, see Create and Activate an AWS Account.

**Create an IAM Administrator User**

As a best practice, you should also create an AWS Identity and Access Management (IAM) user with administrator permissions. Use that for all work that does not require root credentials. Create a password for console access, and access keys to use command line tools. For instructions, see Creating Your First IAM Admin User and Group in the IAM User Guide.
Create a REST API with Lambda Integrations in Amazon API Gateway

You can use this walkthrough to create and deploy a REST API with a Lambda proxy integration and a Lambda non-proxy integration in Amazon API Gateway.

In a Lambda integration, the HTTP method request from the client is mapped to a backend Lambda function invocation.

In a **Lambda proxy integration**, the entire client request is sent to the backend Lambda function as is, except that the order of the request parameters isn't preserved. API Gateway maps the entire client request to the input `event` parameter of the backend Lambda function. The Lambda function's output, including status code, headers, and body, is returned to the client as is. For many use cases, this is the preferred integration type. For more information, see the section called “Set up Lambda Proxy Integrations” (p. 219).

In a **Lambda non-proxy integration** (also called a "custom integration"), you configure the way the parameters, headers, and body of the client's request are translated into the format that your backend Lambda function requires. And you configure the way the Lambda function output is translated back to the format that's required by the client. For more information, see the section called “Set up Lambda Custom Integrations” (p. 231).

Depending on your use case, you may choose to use Lambda proxy integration, Lambda non-proxy integration, or both in your API Gateway API.

**Topics**
- Step 1: Create a Lambda Function in the Lambda Console (p. 11)
- Step 2: Create a REST API in the API Gateway Console (p. 11)
- Step 3: Deploy Your REST API in the API Gateway Console (p. 14)
- Step 4: Create a Second Lambda Function in the Lambda Console (p. 14)
- Step 5: Add a Resource, Method, and Parameter to the REST API in the API Gateway Console (p. 15)
- Next Steps (p. 17)

**Step 1: Create a Lambda Function in the Lambda Console**

In this step, you use the AWS Lambda console to create a simple Lambda function. You'll use this function in the following steps.

1. If you haven't already done so, complete the steps in the section called “Prerequisites: Get Ready to Build an API in API Gateway” (p. 10).
2. Complete the steps in To create a Lambda function in the AWS Lambda Developer Guide.

**Step 2: Create a REST API in the API Gateway Console**

In this step, you create a simple REST API in the API Gateway console and attach your Lambda function to it as a backend.

1. From the Services menu, choose API Gateway to go to the API Gateway console.
2. If this is your first time using API Gateway, you see a page that introduces you to the features of the service. Choose Get Started. When the Create Example API popup appears, choose OK.

If this isn't your first time using API Gateway, choose Create API.

3. Under Choose the protocol, choose REST.
4. Under Create new API, choose New API.
5. Under Settings:
   - For API name, enter my-api.
   - If desired, enter a description in the Description field; otherwise, leave it empty.
   - Leave Endpoint Type set to Regional.
6. Choose Create API.
7. Under Resources, you'll see nothing but / . This is the root-level resource, which corresponds to the base path URL for your API (https://b123abcde4.execute-api.us-west-2.amazonaws.com/{stage-name}).

   From the Actions dropdown menu, choose Create Method.
8. Under the resource name (/), you'll see a dropdown menu. Choose GET and then choose the checkmark icon to save your choice.
10. Choose Use Lambda proxy integration.
11. For Lambda Region, choose the Region where you created your Lambda function.
12. In the Lambda Function field, type any character and then choose my-function (or whatever name you gave the function that you created in the previous step) from the dropdown menu. (If the dropdown menu doesn't appear, delete the character you just typed to make the dropdown menu appear.) Leave Use Default Timeout checked. Choose Save to save your choice.
13. When the Add Permission to Lambda Function popup appears (saying "You are about to give API Gateway permission to invoke your Lambda function..."), choose OK to grant API Gateway that permission.

Now you'll see a / – GET – Method Execution pane:
The **Method Execution** pane contains these items, in clockwise order:

- **Client**: This box represents the client (browser or app) that calls your API's GET method. If you choose the Test link and then choose Test, this simulates a GET request from a client.

- **Method Request**: This box represents the client's GET request as it's received by API Gateway. If you choose Method Request, you'll see settings for things like authorization and modifying the method request before it's passed through to the backend as an integration request. For this step, leave everything set to the default values.

- **Integration Request**: This box represents the GET request as it's passed to the backend. Here the settings depend on the Integration Type that's selected. The URL Path Parameters, URL Query String Parameters, HTTP Headers, and Mapping Templates settings are for modifying the method request as needed by the specific backend. Leave the Integration Type set to Lambda function, and leave the other settings set to the default values.

- **Lambda my-function**: This box represents the backend Lambda function you created in Step 1. If you choose my-function, that opens the my-function Lambda function in the Lambda console.

- **Integration Response**: This box represents the response from the backend, before it's passed to the client as a method response. For a Lambda proxy integration, this entire box is grayed out, because a proxy integration returns the Lambda function's output as is. For a Lambda non-proxy integration, you can configure the integration response to transform the Lambda function's output into a form that's appropriate for the client application. You'll learn how to do that later in this walkthrough.

For this Getting Started procedure, leave everything set to the default values.

- **Method Response**: This box represents the method response that's returned to the client as an HTTP status code, an optional response header, and an optional response body. By default, the response body that's returned by your Lambda function is passed through as is as a JSON document, so the response body default setting is application/json with an empty model (indicating that the body is passed through as is). Here, too, leave everything set to the default values.
Step 3: Deploy Your REST API in the API Gateway Console

Once you complete Step 2, you've created an API, but you can't actually use it yet. This is because it needs to be deployed.

1. From the Actions dropdown menu, choose Deploy API.
2. From the Deployment stage dropdown menu, choose [New Stage].
3. For Stage name, enter prod.
5. In the prod Stage Editor, note the Invoke URL at the top. It should be in this format: (https://b123abcde4.execute-api.us-west-2.amazonaws.com/prod). If you choose the Invoke URL, it will open a new browser tab with that URL. If you refresh the new browser tab, you'll see the message body ("Hello from Lambda!") returned.

For actual API testing, you would use a tool such as cURL or POSTMAN to test your API. For example, if you have cURL installed on your computer, you can test your API as follows:

1. Open a terminal window.
2. Copy the following cURL command and paste it into the terminal window, replacing b123abcde4 with your API's API ID and us-west-2 with the Region where your API is deployed.

   **Linux or Macintosh**
   
   ```
   curl -X GET 'https://b123abcde4.execute-api.us-west-2.amazonaws.com/prod'
   ```

   **Windows**
   
   ```
   curl -X GET "https://b123abcde4.execute-api.us-west-2.amazonaws.com/prod"
   ```

   This command returns the following output: "Hello from Lambda!".

Step 4: Create a Second Lambda Function in the Lambda Console

In this step, you'll create a second backend Lambda function. This one takes an input parameter. In Step 5 you'll create a child resource in your API that has its own GET method, which you'll configure to pass a parameter value to this new function.

1. Choose Lambda from the Services menu to go to the Lambda console.
2. Choose Create function.
3. Choose Author from scratch.
4. For Function name, enter my-function2.
5. Under Runtime, choose Node.js 8.10 or Python 3.7.
6. Under Permissions, expand Choose or create an execution role. From the Execution role dropdown list, choose Use an existing role. From Existing role, choose the role from your previous Lambda function. The role's name will be in the form service-role/my-function-a1b23c4d. Or choose Create a new role with basic Lambda permissions.
7. Choose **Create function**.

8. In the **Function code** pane, you'll see the default "Hello from Lambda!" function. Replace the entire function with the following:

Node.js 8.10

```javascript
exports.handler = async (event) => {
  let myParam = event.myParam;
  const response = {
    statusCode: 200,
    body: JSON.stringify(myParam)
  };
  return response;
};
```

Python 3.7

```python
import json
def lambda_handler(event, context):
  myParam = event['myParam']
  return {
    'statusCode': 200,
    'body': json.dumps(myParam)
  }
```

9. Choose **Save**.

---

**Step 5: Add a Resource, Method, and Parameter to the REST API in the API Gateway Console**

Resources and methods are the nouns and verbs of your REST API. In this step, you'll create a child resource for the API and add a **GET** method to the resource. You'll add a query string parameter to the new method to match the input parameter for the Lambda function you created in Step 4. You'll integrate the new function with the method to illustrate how to get user input (a simple "Hello from API Gateway!" text string) and map it to the Lambda function's input (also a simple string).

1. Choose **API Gateway** from the **Services** menu to go to the API Gateway console.
2. From the **APIs** list, choose **my-api**.
4. From the **Actions** dropdown menu, choose **Create Resource**.
5. For **Resource Name**, enter **my-resource**. Notice that the **Resource Path** field is populated automatically with the resource name.
6. Choose **Create Resource**.
7. From the **Actions** dropdown menu, choose **Create Method**.
8. Under the resource name (**my-resource**), you'll see a dropdown menu. Choose **GET** and then choose the checkmark icon to save your choice.
9. In the `/my-resource – GET – Setup` pane, for **Integration type**, choose **Lambda Function**.
10. For **Lambda Region**, choose the Region where you created your Lambda function.
11. In the **Lambda Function** box, type any character and then choose **my-function2** from the dropdown menu. (If the dropdown menu doesn't appear, delete the character you just typed to make the dropdown menu appear.) Choose **Save** to save your choice.
12. When the **Add Permission to Lambda Function** popup appears (saying "You are about to give API Gateway permission to invoke your Lambda function..."), choose OK to grant API Gateway that permission.

13. You'll now see a **/my-resource – GET – Method Execution** pane. Notice that this time the **Integration Response** box is not grayed out.

Choose **Integration Request**.

**/my-resource - GET - Method Execution**

14. Expand **Mapping Templates**.

15. Set **Request body passthrough** to **When there are no templates defined**.

16. Choose **Add mapping template**.

17. For **Content-Type**, enter `application/json` and choose the checkmark icon to save your choice.

18. If a **Change passthrough behavior** popup appears, choose **Yes, secure this integration**. This ensures that your integration only allows requests that match the **Content-Type** you just defined.

19. In the template window, enter the following:

```
{
    "myParam": "$input.params('myParam')"
}
```

This is the JSON document that will be passed to your Lambda function in the body of the input event object. The right-hand side tells API Gateway what to look for in your input query string. The left-hand side stores it into the parameter that you're about to add to your Lambda function.

20. Choose **Save**.

21. From the **Actions** dropdown menu, choose **Deploy API**.

22. From the **Deployment stage** dropdown menu, choose **prod**.

23. Choose **Deploy**.

Test your API as follows:

1. Open a terminal window.
2. Copy the following cURL command and paste it into the terminal window, replacing `b123abcde4` with your API's API ID and `us-west-2` with the Region where your API is deployed.

Linux or Macintosh

```bash
curl -X GET 'https://b123abcde4.execute-api.us-west-2.amazonaws.com/prod'
```

Windows

```bash
curl -X GET "https://b123abcde4.execute-api.us-west-2.amazonaws.com/prod"
```

This will invoke your API, and you'll see "Hello from Lambda!" returned. This is because your new Lambda function, `my-function2`, isn't attached to the root resource `/`. It's attached to the new resource you created, `my-resource`. So the Lambda function you just invoked is the "Hello from Lambda!" function you created earlier, `my-function`.

3. In the cURL command line, after `prod`, type `/my-resource?myParam=Hello%20from%20API%20Gateway!`. The complete command should look like this:

Linux or Macintosh

```bash
```

Windows

```bash
```

You should now see the correct response returned: `{"statusCode": 200, "body": "Hello from API Gateway!"}`.

Next Steps

Explore any or all of the following topics to continue getting familiar with Amazon API Gateway.

<table>
<thead>
<tr>
<th>To Learn More About</th>
<th>Go To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing input to a backend Lambda function</td>
<td>the section called “Input Format of a Lambda Function for Proxy Integration” (p. 227)</td>
</tr>
<tr>
<td>Returning output from a backend Lambda function</td>
<td>the section called “Output Format of a Lambda Function for Proxy Integration” (p. 230)</td>
</tr>
<tr>
<td>Setting up a custom domain name for your API</td>
<td>the section called “Set up an API Custom Domain Name” (p. 641)</td>
</tr>
<tr>
<td>Adding a Lambda authorizer function to your API</td>
<td>the section called “Use Lambda Authorizers” (p. 380)</td>
</tr>
<tr>
<td>Adding a Amazon Cognito user pool authorizer to your API</td>
<td>the section called “Use Cognito User Pool as Authorizer for a REST API” (p. 397)</td>
</tr>
</tbody>
</table>
Create a REST API with a Mock Integration in Amazon API Gateway

You can use this walkthrough to create and deploy an API with a mock integration in Amazon API Gateway. A *mock integration* enables your API to return a response for a request directly, without ever sending the request to a backend. This enables you to develop your API independently from your backend.

Topics
- Step 1: Create the API (p. 18)
- Step 2: Create the Mock Integration (p. 20)
- Step 3: Define the Successful Response (p. 21)
- Step 4: Add an HTTP 500 Status Code and Error Message (p. 21)
- Step 5: Test the Mock Integration (p. 22)
- Next Steps (p. 24)

Step 1: Create the API

In this step, you create an API with a GET method and a query parameter in the API Gateway console.

1. If you haven't already done so, complete the steps in the section called “Prerequisites: Get Ready to Build an API in API Gateway” (p. 10).
3. If this is your first time using API Gateway, you see a page that introduces you to the features of the service. Choose Get Started. When the Create Example API popup appears, choose OK.

If it isn't your first time, choose Create API.
4. Under **Choose the protocol**, choose **REST**.

5. Under **Create new API**, choose **New API**.

6. Under **Settings**:
   - For **API name**, enter `my-api`.
   - If desired, enter a description in the **Description** field; otherwise, leave it empty.
   - Leave **Endpoint Type** set to **Regional**.

7. Choose **Create API**.

8. From the **Actions** dropdown menu, choose **Create Method**.

9. Under the resource name (`/`), you'll see a dropdown menu. Choose **GET** and then choose the checkmark icon to save your choice.

10. You'll see a `/ – GET – Setup` pane. For **Integration Type**, choose **Mock**.

11. Choose **Save**. Now you'll see a `/ – GET – Method Execution` pane:
Step 2: Create the Mock Integration

In this step, instead of integrating with a backend, you add a query string parameter to your GET method, and then you specify the response codes and messages your API will return.

First, create the query string parameter:

1. In the / - GET - Method Execution pane, choose Method Request.
2. In the / - GET - Method Request pane, expand URL Query String Parameters.
3. Choose Add query string.
4. Type myParam for the Name and choose the checkmark icon to save your choice.

Next, create a mapping template that maps the query string parameter values to the HTTP status code values to be returned to the client.

1. Choose Method Execution.
2. Choose Integration Request.
3. Expand Mapping Templates.
4. For Request body passthrough, choose When there are no templates defined (recommended).
5. Under Content-Type, choose application/json.
6. Replace the template contents with the following:

```json
{
  #if( $input.params('myParam') == "myValue" )
    "statusCode": 200
  #else
    "statusCode": 500
  #end
}
```
7. Choose Save.

---

**Step 3: Define the Successful Response**

Now you'll create a mapping template that maps the HTTP 200 status code value to a success message to be returned to the client.

1. Choose Method Execution and Integration Response.
2. Expand the 200 response and then expand the Mapping Templates section.
3. Under Content-Type, choose application/json.
4. For the template contents, enter the following:

```json
{
  "statusCode": 200,
  "message": "Hello from API Gateway!"
}
```
5. Choose Save.

**Note**
There are two Save buttons in this pane. Be sure to choose the one in the Mapping Templates section.

---

**Step 4: Add an HTTP 500 Status Code and Error Message**

In this step you add an HTTP 500 status code that the frontend can return to the client, and then you map it to an error message.

First, add the 500 status code:
1. Choose **Method Execution** and **Method Response**.
2. Choose **Add response**.
3. For **HTTP status**, enter 500 and choose the checkmark icon to save the setting.

Now create a mapping template that maps the "returned" 500 status code value to an error message from the frontend to the client:

1. Choose **Method Execution** and **Integration Response**.
2. Choose **Add integration response**.
3. For **HTTP status regex**, enter 5\d{2}.
4. For **Method response status**, choose 500 from the dropdown menu and choose **Save**.
5. Expand the 500 response and then expand the **Mapping Templates** section, if it isn’t already expanded.
6. Under **Content-Type**, choose **Add mapping template**.
7. In the box under **Content-Type**, enter application/json and choose the checkmark icon to save your choice.
8. For the template contents, enter the following:

   ```json
   {
       "statusCode": 500,
       "message": "This is an error message."
   }
   ```

9. Choose **Save**.

   **Note**
   There are two **Save** buttons in this pane. Be sure to choose the one in the **Mapping Templates** section.

### Step 5: Test the Mock Integration

In this step, you test the mock integration.

1. Choose **Method Execution** and then choose **Test**.
2. Under **Query Strings**, enter myParam=myValue.
3. Choose **Test**.

   You should see output like the following:
4. Under **Query Strings**, enter `myParam=""`. Or simply delete everything in the **Query Strings** box.
5. Choose **Test**.

You should see output like the following:

```
Request: /?myParam=myValue
Status: 200
Latency: 5 ms
Response Body
{
    "statusCode": 200,
    "message": "Hello from API Gateway!"
}
Response Headers
{"Content-Type":"application/json"}
Logs
Execution log for request 2083a122-7076-11e9-b3da-c5566e62847c
Tue May 07 03:13:46 UTC 2019 : Starting execution for request 2083a122-7076-11e9-b3da-c5566e62847c
Tue May 07 03:13:46 UTC 2019 : HTTP Method: GET, Resource Pa
```
Next Steps

Explore any or all of the following topics to continue getting familiar with Amazon API Gateway.

<table>
<thead>
<tr>
<th>To Learn More About</th>
<th>Go To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defining method requests and responses</td>
<td>the section called “Set up REST API Methods” (p. 199)</td>
</tr>
<tr>
<td>Defining integration responses</td>
<td>the section called “Set up Integration Response” (p. 218)</td>
</tr>
<tr>
<td>Setting up a custom domain name for your API</td>
<td>the section called “Set up an API Custom Domain Name” (p. 641)</td>
</tr>
<tr>
<td>Enabling CORS for your API</td>
<td>the section called “Enable CORS for a REST API Resource” (p. 405)</td>
</tr>
</tbody>
</table>
To get help with Amazon API Gateway from the community, see the API Gateway Discussion Forum. (When you enter this forum, AWS might require you to sign in.)

To get help with API Gateway directly from AWS, see the support options on the AWS Support page. See also our frequently asked questions (FAQs), or contact us directly.

Amazon API Gateway Videos

This section provides several AWS instructional videos for Amazon API Gateway that can serve as additional getting started resources for you.

Topics
• Amazon API Gateway Videos from Twitch Build On AWS Event Series (p. 25)
• Other Amazon API Gateway Videos (p. 25)

Amazon API Gateway Videos from Twitch Build On AWS Event Series

The following videos are from the Build On AWS event series on Twitch.tv.

Introduction to Building Happy Little APIs (1 minute, YouTube website)

This video briefly introduces the Building Happy Little APIs video series.

Building Happy Little APIs | Episode 1 – I Didn’t Know Amazon API Gateway Did That (60 minutes, YouTube website)

This video is an introduction to Amazon API Gateway and the problems it can solve. It discusses the moving parts of API Gateway and gives examples of possible use cases. This overview aims to give you a solid understanding of why you should use API Gateway and what it can do for you.

Building Happy Little APIs | Episode 2 – No REST for the Weary (55 minutes, YouTube website)

This video shows you how to build a simple application that uses Amazon API Gateway with an AWS Lambda function for a backend. You'll learn how to use the AWS Serverless Application Model (AWS SAM) to model the API and the application behind it. You'll also learn the difference between integrations and proxying and when to use each.

Other Amazon API Gateway Videos

The following videos are available on the AWS Online Tech Talks channel on the YouTube website.

Building APIs with Amazon API Gateway (43 minutes, YouTube website)

This video describes the capabilities of Amazon API Gateway, and shows how you can get started building APIs.

Best Practices for Building Enterprise Grade APIs with Amazon API Gateway (40 minutes, YouTube website)

This video shows you how to use Amazon API Gateway with other AWS services to design and operate enterprise-ready APIs. You'll learn about best practices to help you create, maintain, and secure your enterprise APIs.
Amazon API Gateway Tutorials

The following tutorials provide hands-on exercises to help you learn about API Gateway.

Topics
- Build an API Gateway API with Lambda Integration (p. 26)
- TUTORIAL: Create a REST API by Importing an Example (p. 42)
- Build an API Gateway API with HTTP Integration (p. 50)
- TUTORIAL: Build an API with API Gateway Private Integration (p. 85)
- TUTORIAL: Build an API Gateway API with AWS Integration (p. 87)
- TUTORIAL: Create a Calc REST API with Two AWS Service Integrations and and One Lambda Non-Proxy Integration (p. 92)
- TUTORIAL: Create a REST API as an Amazon S3 Proxy in API Gateway (p. 111)
- TUTORIAL: Create a REST API as an Amazon Kinesis Proxy in API Gateway (p. 137)

Build an API Gateway API with Lambda Integration

To build an API with Lambda integrations, you can use Lambda proxy integration or Lambda non-proxy integration.

In Lambda proxy integration, the input to the integrated Lambda function can be expressed as any combination of request headers, path variables, query string parameters, and body. In addition, the Lambda function can use API configuration settings to influence its execution logic. For an API developer, setting up a Lambda proxy integration is simple. Other than choosing a particular Lambda function in a given region, you have little else to do. API Gateway configures the integration request and integration response for you. Once set up, the integrated API method can evolve with the backend without modifying the existing settings. This is possible because the backend Lambda function developer parses the incoming request data and responds with desired results to the client when nothing goes wrong or responds with error messages when anything goes wrong.

In Lambda non-proxy integration, you must ensure that input to the Lambda function is supplied as the integration request payload. This implies that you, as an API developer, must map any input data the client supplied as request parameters into the proper integration request body. You may also need to translate the client-supplied request body into a format recognized by the Lambda function.

Topics
- TUTORIAL: Build a Hello World API with Lambda Proxy Integration (p. 26)
- TUTORIAL: Build an API Gateway API with Cross-Account Lambda Proxy Integration (p. 31)
- TUTORIAL: Build an API Gateway API with Lambda Non-Proxy Integration (p. 33)

TUTORIAL: Build a Hello World API with Lambda Proxy Integration

Lambda proxy integration (p. 219) is a lightweight, flexible API Gateway API integration type that allows you to integrate an API method – or an entire API – with a Lambda function. The Lambda function can be written in any language that Lambda supports. Because it’s a proxy integration, you can change the Lambda function implementation at any time without needing to redeploy your API.
In this tutorial, you do the following:

- Create a "Hello, World!" Lambda function to be the backend for the API.
- Create and test a "Hello, World!" API with Lambda proxy integration.

**Topics**

- Create a "Hello, World!" Lambda Function (p. 27)
- Create a "Hello, World!" API (p. 28)
- Deploy and Test the API (p. 29)

**Create a "Hello, World!" Lambda Function**

This function returns a greeting to the caller as a JSON object in the following format:

```
{  
    "greeting": "Good {time}, {name} of {city}. [ Happy {day}!]
}
```

**Create a "Hello, World!" Lambda function in the Lambda console**

2. On the AWS navigation bar, choose a region (for example, US East (N. Virginia)).
   **Note**
   Note the region where you create the Lambda function. You'll need it when you create the API.
3. Choose **Functions** in the navigation pane.
4. Choose **Create function**.
5. Choose **Author from scratch**.
6. Under **Basic information**, do the following:
   a. In **Function name**, enter **GetStartedLambdaProxyIntegration**.
   b. From the **Runtime** dropdown list, choose **Node.js 8.10**.
   c. Under **Permissions**, expand **Choose or create an execution role**. From the **Execution role** dropdown list, choose **Create new role from AWS policy templates**.
   d. In **Role name**, enter **GetStartedLambdaBasicExecutionRole**.
   e. Leave the **Policy templates** field blank.
   f. Choose **Create function**.
7. Under **Function code**, in the inline code editor, copy/paste the following code:

```javascript
'use strict';
console.log('Loading hello world function');
exports.handler = async (event) => {
  let name = "you";
  let city = 'World';
  let time = 'day';
  let day = "";
  let responseCode = 200;
  console.log("request: " + JSON.stringify(event));

  if (event.queryStringParameters && event.queryStringParameters.name) {
    console.log("Received name: " + event.queryStringParameters.name);
    name = event.queryStringParameters.name;
  }
```
if (event.queryStringParameters && event.queryStringParameters.city) {
    console.log("Received city: " + event.queryStringParameters.city);
    city = event.queryStringParameters.city;
}

if (event.headers && event.headers['day']) {
    console.log("Received day: " + event.headers.day);
    day = event.headers.day;
}

if (event.body) {
    let body = JSON.parse(event.body)
    if (body.time)
        time = body.time;
}

let greeting = `Good ${time}, ${name} of ${city}.`;
if (day) greeting += ` Happy ${day}!`;

let responseBody = {
    message: greeting,
    input: event
};

// The output from a Lambda proxy integration must be
// in the following JSON object. The 'headers' property
// is for custom response headers in addition to standard
// ones. The 'body' property must be a JSON string. For
// base64-encoded payload, you must also set the 'isBase64Encoded'
// property to 'true'.
let response = {
    statusCode: responseCode,
    headers: {
        "x-custom-header" : "my custom header value"
    },
    body: JSON.stringify(responseBody)
};

console.log("response: " + JSON.stringify(response))
return response;

8. Choose Save.

Create a "Hello, World!" API

Now create an API for your "Hello, World!" Lambda function by using the API Gateway console.

Build a "Hello, World!" API

2. If this is your first time using API Gateway, you see a page that introduces you to the features of the service. Choose Get Started. When the Create Example API popup appears, choose OK.
   
   If this is not your first time using API Gateway, choose Create API.
3. Create an empty API as follows:
   
   a. Under Choose the protocol, choose REST.
   b. Under Create new API, choose New API.
   c. Under Settings:
TUTORIAL: Hello World API with Lambda Proxy Integration

• For API name, enter LambdaSimpleProxy.
  • If desired, enter a description in the Description field; otherwise, leave it empty.
  • Leave Endpoint Type set to Regional.

d. Choose Create API.

4. Create the helloworld resource as follows:
   a. Choose the root resource (/) in the Resources tree.
   b. Choose Create Resource from the Actions dropdown menu.
   c. Leave Configure as proxy resource unchecked.
   d. For Resource Name, enter helloworld.
   e. Leave Resource Path set to /helloworld.
   f. Leave Enable API Gateway CORS unchecked.
   g. Choose Create Resource.

5. In a proxy integration, the entire request is sent to the backend Lambda function as-is, via a catch-all ANY method that represents any HTTP method. The actual HTTP method is specified by the client at run time. The ANY method allows you to use a single API method setup for all of the supported HTTP methods: DELETE, GET, HEAD, OPTIONS, PATCH, POST, and PUT.

To set up the ANY method, do the following:
   a. In the Resources list, choose /helloworld.
   b. In the Actions menu, choose Create method.
   c. Choose ANY from the dropdown menu, and choose the checkmark icon.
   d. Leave the Integration type set to Lambda Function.
   e. Choose Use Lambda Proxy integration.
   f. From the Lambda Region dropdown menu, choose the region where you created the GetStartedLambdaProxyIntegration Lambda function.
   g. In the Lambda Function field, type any character and choose GetStartedLambdaProxyIntegration from the dropdown menu.
   h. Leave Use Default Timeout checked.
   i. Choose Save.
   j. Choose OK when prompted with Add Permission to Lambda Function.

Deploy and Test the API

**Deploy the API in the API Gateway console**

1. Choose Deploy API from the Actions dropdown menu.
2. For Deployment stage, choose [new stage].
3. For Stage name, enter test.
4. If desired, enter a Stage description.
5. If desired, enter a Deployment description.
6. Choose Deploy.
7. Note the API’s Invoke URL.

**Use Browser and cURL to Test an API with Lambda Proxy Integration**

You can use a browser or cURL to test your API.
To test GET requests using only query string parameters, you can type the URL for the API's helloworld resource into a browser address bar. For example: 

```
https://r275xc9bmd.execute-api.us-east-1.amazonaws.com/test/helloworld?name=John&city=Seattle
```

For other methods, you must use more advanced REST API testing utilities, such as POSTMAN or cURL. This tutorial uses cURL. The cURL command examples below assume that cURL is installed on your computer.

To test the deployed API using cURL:

1. Open a terminal window.
2. Copy the following cURL command and paste it into the terminal window, replacing `r275xc9bmd` with your API's API ID and `us-east-1` with the region where your API is deployed.

```
curl -v -X POST \
'https://r275xc9bmd.execute-api.us-east-1.amazonaws.com/test/helloworld?' \ 
-H 'content-type: application/json' \ 
-H 'day: Thursday' \ 
-d '{ "time": "evening" }'
```

*Note*

If you’re running the command on Windows, use this syntax instead:

```
curl -v -X POST "https://r275xc9bmd.execute-api.us-east-1.amazonaws.com/test/helloworld?name=John&city=Seattle" -H "content-type: application/json" -H "day: Thursday" -d "{ "time": "evening" }"
```

You should get a successful response with a payload similar to the following:

```
{
    "message": "Good evening, John of Seattle. Happy Thursday!",
    "input": {
        "resource": "/helloworld",
        "path": "/helloworld",
        "httpMethod": "POST",
        "headers": {
            "Accept": "*/*",
            "content-type": "application/json",
            "day": "Thursday",
            "Host": "r275xc9bmd.execute-api.us-east-1.amazonaws.com",
            "User-Agent": "curl/7.64.0",
            "X-Amzn-Trace-Id": "Root=1-1a2b3c4d-a1b2c3d4e5f6a1b2c3d4e5f64",
            "X-Forwarded-For": "72.21.198.64",
            "X-Forwarded-Port": "443",
            "X-Forwarded-Proto": "https",
            "multiValueHeaders": {
                "Accept": ["*/*"],
                "content-type": ["application/json"],
                "day": ["Thursday"],
                "Host": ["r275xc9bmd.execute-api.us-east-1.amazonaws.com"],
                "User-Agent": ["curl/0.0.0"],
                "X-Amzn-Trace-Id": ["Root=1-1a2b3c4d-a1b2c3d4e5f6a1b2c3d4e5f6"],
                "X-Forwarded-For": ["10.12.34.56"],
                "X-Forwarded-Proto": ["https"],
                "queryStringParameters": {
                    "city": "Seattle",
                    "name": "John"
                },
                "multiValueQueryStringParameters": {
                    "city": ["Seattle"],
                    "name": ["John"]
                }
            }
        }
    }
}
```
If you change `POST` to `PUT` in the preceding method request, you should get the same response.

To test the `GET` method, copy the following `cURL` command and paste it into the terminal window, replacing `r275xc9bmd` with your API’s API ID and `us-east-1` with the region where your API is deployed.

```bash
curl -X GET \
'https://r275xc9bmd.execute-api.us-east-1.amazonaws.com/test/helloworld?Seattle?name=John' \
-H 'content-type: application/json' \
-H 'day: Thursday'
```

You should get a response similar to the result from the preceding `POST` request, except that the `GET` request does not have any payload. So the `body` parameter will be `null`.

### TUTORIAL: Build an API Gateway API with Cross-Account Lambda Proxy Integration

You can now use an AWS Lambda function from a different AWS account as your API integration backend. Each account can be in any region where Amazon API Gateway is available. This makes it easy to centrally manage and share Lambda backend functions across multiple APIs.

In this section, we show how to configure cross-account Lambda proxy integration using the Amazon API Gateway console.
First, we create the example API from the section called “TUTORIAL: Create a REST API by Importing an Example” (p. 42) in one account. We then create a Lambda function in another account. Finally, we use cross-account Lambda integration to allow the example API to use the Lambda function we created in the second account.

Create API for API Gateway Cross-Account Lambda Integration

First, you'll create the example API as described in the section called “TUTORIAL: Create a REST API by Importing an Example” (p. 42).

To create the example API

1. Sign in to the API Gateway console.
2. Choose **Create API** from the API Gateway APIs home page:
3. Under **Create new API**, choose **Examples API**.
4. For **Endpoint Type**, choose **Edge optimized**.
5. Choose **Import** to create the example API.

Create Lambda Integration Function in Another Account

Now you'll create a Lambda function in a different account from the one in which you created the example API.

Creating a Lambda function in another account

1. Log in to the Lambda console in a different account from the one where you created your API Gateway API.
2. Choose **Create function**.
3. Choose **Author from scratch**.
4. Under **Author from scratch**, do the following:
   a. In the **Name** input field, type a function name.
   b. From the **Runtime** drop-down list, choose a supported runtime. In this example, we use **Node.js 8.10**.
   c. From the **Role** drop-down list, choose **Choose an existing role, Create new role from template(s)** or **Create a custom role**. Then, follow the ensuing instructions for the choice.
   d. Choose **Create function** to continue.

   For this example, we will skip the **Designer** section and move to the **Function code** section next.
5. Scroll down to the **Function code** pane.
6. Copy-paste the Node.js function implementation from the section called “TUTORIAL: Hello World API with Lambda Proxy Integration” (p. 26).
7. From the **Runtime** dropdown menu, choose **Node.js 8.10**.
8. Choose **Save**.
9. Note the full ARN for your function (in the upper right corner of the Lambda function pane). You'll need it when you create your cross-account Lambda integration.

Configure Cross-Account Lambda Integration

Once you have a Lambda integration function in a different account, you can use the API Gateway console to add it to your API in your first account.
Note
If you are configuring a cross-region, cross-account authorizer, the sourceArn that is added to the target function should use the region of the function, not the region of the API.

Configuring your cross-account Lambda integration

1. In the API Gateway console, choose your API.
2. Choose Resources.
3. In the Resources pane, choose the top-level GET method.
4. In the Method Execution pane, choose Integration Request.
5. For Integration type, choose Lambda Function.
6. Check Use Lambda Proxy integration.
7. Leave Lambda Region set to your account's region.
8. For Lambda Function, copy/paste the full ARN for the Lambda function you created in your second account and choose the checkmark.
9. You'll see a popup that says Add Permission to Lambda Function: You have selected a Lambda function from another account. Please ensure that you have the appropriate Function Policy on this function. You can do this by running the following AWS CLI command from account 123456789012: aws lambda add-permission, followed by an aws lambda add-permission command string.
10. Copy-paste the aws lambda add-permission command string into an AWS CLI window that is configured for your second account. This will grant your first account access to your second account's Lambda function.
11. In the popup from the previous step in the Lambda console, choose OK.
12. To see the updated policy for your function in the Lambda console,
   a. Choose your integration function.
   b. In the Designer pane, choose the key icon.

   In the Function policy pane, you should now see an Allow policy with a Condition clause in which the in the AWS:SourceArn is the ARN for your API’s GET method.

TUTORIAL: Build an API Gateway API with Lambda Non-Proxy Integration

In this walkthrough, we use the API Gateway console to build an API that enables a client to call Lambda functions through the Lambda non-proxy integration (also known as custom integration). For more information about AWS Lambda and Lambda functions, see the AWS Lambda Developer Guide.

To facilitate learning, we chose a simple Lambda function with minimal API setup to walk you through the steps of building an API Gateway API with the Lambda custom integration. When necessary, we describe some of the logic. For a more detailed example of the Lambda custom integration, see TUTORIAL: Create a Calc REST API with Two AWS Service Integrations and One Lambda Non-Proxy Integration (p. 92).

Before creating the API, set up the Lambda backend by creating a Lambda function in AWS Lambda, described next.

Topics
- Create a Lambda Function for Lambda Non-Proxy Integration (p. 34)
- Create an API with Lambda Non-Proxy Integration (p. 37)
- Test Invoking the API Method (p. 39)
Create a Lambda Function for Lambda Non-Proxy Integration

Note
Creating Lambda functions may result in charges to your AWS account.

In this step, you create a "Hello, World!"-like Lambda function for the Lambda custom integration. Throughout this walkthrough, the function is called `GetStartedLambdaIntegration`.

The Node.js implementation of this `GetStartedLambdaIntegration` Lambda function is as follows:

```javascript
'use strict';
var days = ['Sunday', 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', 'Saturday'];
var times = ['morning', 'afternoon', 'evening', 'night', 'day'];

console.log('Loading function');
exports.handler = function(event, context, callback) {
  // Parse the input for the name, city, time and day property values
  let name = event.name === undefined ? 'you' : event.name;
  let city = event.city === undefined ? 'World' : event.city;
  let time = times.indexOf(event.time)<0 ? 'day' : event.time;
  let day = days.indexOf(event.day)<0 ? null : event.day;

  // Generate a greeting
  let greeting = 'Good ' + time + ', ' + name + ' of ' + city + '. '
                 + (day) ? 'Happy ' + day + '!' : ' ';

  // Log the greeting to CloudWatch
  console.log('Hello: ', greeting);

  // Return a greeting to the caller
  callback(null, {
    "greeting": greeting
  });
};
```

For the Lambda custom integration, API Gateway passes the input to the Lambda function from the client as the integration request body. The event object of the Lambda function handler is the input.

Our Lambda function is simple. It parses the input `event` object for the `name`, `city`, `time`, and `day` properties. It then returns a greeting, as a JSON object of {"message":greeting}, to the caller. The message is in the "Good [morning|afternoon|day], [name|you] in [city|World]. Happy day!" pattern. It is assumed that the input to the Lambda function is of the following JSON object:

```javascript
{
  "city": "...",
  "time": "...",
  "day": "...",
  "name": "...
}
```

For more information, see the AWS Lambda Developer Guide.

In addition, the function logs its execution to Amazon CloudWatch by calling `console.log(...)`. This is helpful for tracing calls when debugging the function. To allow the
GetStartedLambdaIntegration function to log the call, set an IAM role with appropriate policies for the Lambda function to create the CloudWatch streams and add log entries to the streams. The Lambda console guides you through to create the required IAM roles and policies.

If you set up the API without using the API Gateway console, such as when importing an API from an OpenAPI file, you must explicitly create, if necessary, and set up an invocation role and policy for API Gateway to invoke the Lambda functions. For more information on how to set up Lambda invocation and execution roles for an API Gateway API, see Control Access to an API with IAM Permissions (p. 362).

Compared to GetStartedLambdaProxyIntegration, the Lambda function for the Lambda proxy integration, the GetStartedLambdaIntegration Lambda function for the Lambda custom integration only takes input from the API Gateway API integration request body. The function can return an output of any JSON object, a string, a number, a Boolean, or even a binary blob. The Lambda function for the Lambda proxy integration, in contrast, can take the input from any request data, but must return an output of a particular JSON object. The GetStartedLambdaIntegration function for the Lambda custom integration can have the API request parameters as input, provided that API Gateway maps the required API request parameters to the integration request body before forwarding the client request to the backend. For this to happen, the API developer must create a mapping template and configure it on the API method when creating the API.

Now, create the GetStartedLambdaIntegration Lambda function.

To create the GetStartedLambdaIntegration Lambda function for Lambda custom integration

1. Open the AWS Lambda console at https://console.aws.amazon.com/lambda/.
2. Do one of the following:
   a. If the welcome page appears, choose Get Started Now and then choose Create a function.
   b. If the Lambda > Functions list page appears, choose Create a function.
3. Choose Author from scratch.
4. In the Author from scratch pane, do the following:
   a. For Name, type GetStartedLambdaIntegration as the Lambda function name.
   b. For Runtime, choose Node.js 8.10.
   c. For Role, choose Create new role from template(s).
   d. For Role name, type a name for your role (for example, GetStartedLambdaIntegrationRole).
   e. For Policy templates, choose Simple Microservice permissions.
   f. Choose Create function.
5. In the Configure function pane, under Function code do the following:
   a. Choose Edit code inline, if it is not already shown, under Content entry type.
   b. Leave Handler set to index.handler.
   c. Set Runtime to Node.js 8.10.
   d. Copy the Lambda function code listed in the beginning of this section and paste it in the inline code editor.
   e. Leave the default choices for all other fields in this section.
   f. Choose Save.
6. To test the newly created function, choose Configure test events from Select a test event....
   a. For Create new event, replace any default code statements with the following, type HelloworldTest for the Event aname, and choose Create.

```
b. Choose Test to invoke the function. The **Execution result: succeeded** section is shown. Expand **Detail** and you see the following output.

```json
{
    "greeting": "Good morning, Jonny of Seattle. Happy Wednesday!"
}
```

The output is also written to CloudWatch Logs.

As a side exercise, you can use the IAM console to view the IAM role (GetStartedLambdaIntegrationRole) that was created as part of the Lambda function creation. Attached to this IAM role are two inline policies. One stipulates the most basic permissions for Lambda execution. It permits calling the CloudWatch CreateLogGroup for any CloudWatch resources of your account in the region where the Lambda function is created. This policy also allows creating the CloudWatch streams and logging events for the HelloWorldForLambdaIntegration Lambda function.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:region:account-id:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:region:account-id:log-group:/aws/lambda/GetStartedLambdaIntegration:*"
            ]
        }
    ]
}
```

The other policy document applies to invoking another AWS service that is not used in this example. You can skip it for now.

Associated with the IAM role is a trusted entity, which is `lambda.amazonaws.com`. Here is the trust relationship:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            }
        }
    ]
}
```
The combination of this trust relationship and the inline policy makes it possible for the Lambda function to invoke a `console.log()` function to log events to CloudWatch Logs.

If you did not use the AWS Management Console to create the Lambda function, you need to follow these examples to create the required IAM role and policies and then manually attach the role to your function.

Create an API with Lambda Non-Proxy Integration

With the Lambda function (`GetStartedLambdaIntegration`) created and tested, you are ready to expose the function through an API Gateway API. For illustration purposes, we expose the Lambda function with a generic HTTP method. We use the request body, a URL path variable, a query string, and a header to receive required input data from the client. We turn on the API Gateway request validator for the API to ensure that all of the required data is properly defined and specified. We configure a mapping template for API Gateway to transform the client-supplied request data into the valid format as required by the backend Lambda function.

To create an API with Lambda custom integration with a Lambda function

1. Launch the API Gateway console.
2. Choose Create new API.
   a. Type `GetStartedLambdaNonProxyIntegration` for API name.
   b. Type a description of the API for Description or leave it blank.
   c. Choose Create API.
3. Choose the root resource (`/`) under Resources. From the Actions menu, choose Create Resource.
   a. Type `city` for Resource Name.
   b. Replace Resource Path with `{city}`). This is an example of the templated path variable used to take input from the client. Later, we show how to map this path variable into the Lambda function input using a mapping template.
   c. Select the Enable API Gateway Cors option.
   d. Choose Create Resource.
4. With the newly created `{city}` resource highlighted, choose Create Method from Actions.
   a. Choose ANY from the HTTP method drop-down menu. The ANY HTTP verb is a placeholder for a valid HTTP method that a client submits at run time. This example shows that ANY method can be used for Lambda custom integration as well as for Lambda proxy integration.
   b. To save the setting, choose the check mark.
5. In Method Execution, for the `{city}` ANY method, do the following:
   a. Choose Lambda Function for Integration type.
   b. Leave the Use Lambda Proxy integration box unchecked.
   c. Choose the region where you created the Lambda function; for example, us-west-2.
   d. Type the name of your Lambda function in Lambda Function; for example, `GetStartedLambdaIntegration`.
   e. Leave the Use Default timeout box checked.
   f. Choose Save.
g. Choose OK in the Add Permission to Lambda Function popup to have API Gateway set up the required access permissions for the API to invoke the integrated Lambda function.

6. In this step you'll configure the following:

- A query string parameter (time)
- A header parameter (day)
- A payload property (callerName)

At run time, the client can use these request parameters and the request body to provide time of the day, the day of the week, and the name of the caller. You already configured the /{city} path variable.

a. In the Method Execution pane, choose Method Request.

b. Expand the URL Query String Parameters section. Choose Add query string. Type time for Name. Select the Required option and choose the check-mark icon to save the setting. Leave Caching cleared to avoid an unnecessary charge for this exercise.

c. Expand the HTTP Request Headers section. Choose Add header. Type day for Name. Select the Required option and choose the check-mark icon to save the setting. Leave Caching cleared to avoid an unnecessary charge for this exercise.

d. To define the method request payload, do the following:

i. To define a model, choose Models under the API from the API Gateway primary navigation pane, and then choose Create.

ii. Type GetStartedLambdaIntegrationUserInput for Model name.

iii. Type application/json for Content type.

iv. Leave the Model description blank.

v. Copy the following schema definition into the Model schema editor:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "GetStartedLambdaIntegrationInputModel",
  "type": "object",
  "properties": {
    "callerName": { "type": "string" }
  }
}
```

vi. Choose Create model to finish defining the input model.

vii. Choose Resources, choose the /{city} ANY method, choose Method Request, and expand Request body. Choose Add model. Type application/json for Content type. Choose GetStartedLambdaIntegrationInput for Model name. Choose the check-mark icon to save the setting.

7. Choose the /{city} ANY method and choose Integration Request to set up a body-mapping template. In this step you'll map the previously configured method request parameter of nameQuery or nameHeader to the JSON payload, as required by the backend Lambda function:

a. Expand the Mapping Templates section. Choose Add mapping template. Type application/json for Content-Type. Choose the check-mark icon to save the setting.

b. In the popup that appears, choose Yes, secure this integration.

c. Check the recommended When there are no templates defined for Request body passthrough.

d. Choose GetStartedLambdaIntegrationUserInput from Generate template to generate an initial mapping template. This option is available because you defined a model schema, without which you would need to write the mapping template from scratch.
**Test Invoking the API Method**

The API Gateway console provides a testing facility for you to test invoking the API before it is deployed. You use the Test feature of the console to test the API by submitting the following request:

```
POST /Seattle?time=morning
day:Wednesday

{    "callerName": "John"
}
```

In this test request, you’ll set ANY to POST, set `{city}` to Seattle, assign Wednesday as the day header value, and assign "John" as the `callerName` value.

**To test-involve the ANY /{city} method**

1. In **Method Execution**, choose **Test**.
2. Choose **POST** from the **Method** drop-down list.
3. In **Path**, type **Seattle**.
4. In **Query Strings**, type `time=morning`.
5. In **Headers**, type `day:Wednesday`.
6. In **Request Body**, type `{ "callerName":"John" }`.
7. Choose **Test**.
8. Verify that the returned response payload is as follows:

```
{    "greeting": "Good morning, John of Seattle. Happy Wednesday!"
}
```

9. You can also view the logs to examine how API Gateway processes the request and response.
The logs show the incoming request before the mapping and the integration request after the mapping. When a test fails, the logs are useful for evaluating whether the original input is correct or the mapping template works correctly.

### Deploy the API

The test invocation is a simulation and has limitations. For example, it bypasses any authorization mechanism enacted on the API. To test the API execution in real time, you must deploy the API first. To deploy an API, you create a stage to create a snapshot of the API at that time. The stage name also defines the base path after the API's default host name. The API's root resource is appended after the stage name. When you modify the API, you must redeploy it to a new or existing stage before the changes take effect.

**To deploy the API to a stage**

1. Choose the API from the **APIs** pane or choose a resource or method from the **Resources** pane. Choose **Deploy API** from the **Actions** drop-down menu.
2. For **Deployment stage**, choose **New Stage**.
3. For **Stage name**, type a name; for example, **test**.
   - **Note**
     - The input must be UTF-8 encoded (i.e., unlocalized) text.
4. For **Stage description**, type a description or leave it blank.
5. For **Deployment description**, type a description or leave it blank.
6. Choose **Deploy**. After the API is successfully deployed, you see the API's base URL (the default host name plus the stage name) displayed as **Invoke URL** at the top of the **Stage Editor**. The general pattern of this base URL is https://api-id.region.amazonaws.com/stageName. For example, the base URL of the API (beags1mnid) created in the us-west-2 region and deployed to the test stage is https://beags1mnid.execute-api.us-west-2.amazonaws.com/test.

**Test the API in a Deployment Stage**

There are several ways you can test a deployed API. For GET requests using only URL path variables or query string parameters, you can type the API resource URL in a browser. For other methods, you must use more advanced REST API testing utilities, such as **POSTMAN** or **cURL**.

**To test the API using cURL**

1. Open a terminal window on your local computer connected to the internet.
2. To test **POST /Seattle?time=evening**:

   Copy the following cURL command and paste it into the terminal window.

   ```
   ```

   You should get a successful response with the following payload:

   ```
   {"greeting":"Good evening, John of Seattle. Happy Thursday!"}
   ```

   If you change **POST** to **PUT** in this method request, you get the same response.

3. To test **GET /Boston?time=morning**:

   Copy the following cURL command and paste it into the terminal window.

   ```
   ```

   You get a **400 Bad Request** response with the following error message:

   ```
   {"message": "Invalid request body"}
   ```

   This is because the GET request that you submitted cannot take a payload and fails the request validation.
Clean Up

If you no longer need the Lambda functions you created for this walkthrough, you can delete them now. You can also delete the accompanying IAM resources.

Warning
If you plan to complete the other walkthroughs in this series, do not delete the Lambda execution role or the Lambda invocation role. If you delete a Lambda function that your APIs rely on, those APIs will no longer work. Deleting a Lambda function cannot be undone. If you want to use the Lambda function again, you must re-create the function.

If you delete an IAM resource that a Lambda function relies on, that Lambda function will no longer work, and any APIs that rely on that function will no longer work. Deleting an IAM resource cannot be undone. If you want to use the IAM resource again, you must re-create the resource.

To delete the Lambda functions

1. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/.
2. From the list of functions, choose GetHelloWorld, choose Actions, and then choose Delete function. When prompted, choose Delete again.
3. From the list of functions, choose GetHelloWithName, choose Actions, and then choose Delete function. When prompted, choose Delete again.

To delete the associated IAM resources

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. From Details, choose Roles.
3. From the list of roles, choose APIGatewayLambdaExecRole, choose Role Actions, and then choose Delete Role. When prompted, choose Yes, Delete.
4. From Details, choose Policies.
5. From the list of policies, choose APIGatewayLambdaExecPolicy, choose Policy Actions, and then choose Delete. When prompted, choose Delete.

You have now reached the end of this walkthrough.

TUTORIAL: Create a REST API by Importing an Example

You can use the Amazon API Gateway console to create and test a simple REST API with the HTTP integration for a PetStore website. The API definition is preconfigured as a OpenAPI 2.0 file. After loading the API definition into API Gateway, you can use the API Gateway console to examine the API's basic structure or simply deploy and test the API.

The PetStore example API supports the following methods for a client to access the HTTP backend website of http://petstore-demo-endpoint.execute-api.com/petstore/pets.

- **GET /**: for read access of the API's root resource that is not integrated with any backend endpoint. API Gateway responds with an overview of the PetStore website. This is an example of the MOCK integration type.
• **GET /pets**: for read access to the API's /pets resource that is integrated with the like-named backend /pets resource. The backend returns a page of available pets in the PetStore. This is an example of the HTTP integration type. The URL of the integration endpoint is `http://petstore-demo-endpoint.execute-api.com/petstore/pets`.

• **POST /pets**: for write access to the API's /pets resource that is integrated with the backend /petstore/pets resource. Upon receiving a correct request, the backend adds the specified pet to the PetStore and returns the result to the caller. The integration is also HTTP.

• **GET /pets/{petId}**: for read access to a pet as identified by a `petId` value as specified as a path variable of the incoming request URL. This method also has the HTTP integration type. The backend returns the specified pet found in the PetStore. The URL of the backend HTTP endpoint is `http://petstore-demo-endpoint.execute-api.com/petstore/pets/n`, where `n` is an integer as the identifier of the queried pet.

The API supports CORS access via the OPTIONS methods of the MOCK integration type. API Gateway returns the required headers supporting CORS access.

The following procedure walks you through the steps to create and test an API from an example using the API Gateway Console.

**To import, build, and test the example API**

1. If you haven't already done so, complete the steps in the section called “Prerequisites: Get Ready to Build an API in API Gateway” (p. 10).
3. Do one of the following:
   a. If this is the first API in your account, choose Get Started from the API Gateway console welcome page.
      
      If prompted with hints, choose OK to close them and continue.
   b. If this is not your first API, choose Create API from the API Gateway APIs home page:

4. Under Create new API, choose Example API and then choose Import to create the example API. For your first API, the API Gateway console starts with this option as default.
You can scroll down the OpenAPI definition for details of this example API before choosing Import.

5. The newly created API is shown as follows:

The Resources pane shows the structure of the created API as a tree of nodes. API methods defined on each resource are edges of the tree. When a resource is selected, all of its methods are listed in the Methods pane on the right. Displayed under each method is a brief summary of the method, including its endpoint URL, authorization type, and API Key requirement.

6. To view the details of a method, to modify its set-up, or to test the method invocation, choose the method name from either the method list or the resource tree. Here, we choose the POST /pets method as an illustration:
The resulting Method Execution pane presents a logical view of the chosen (POST /pets) method's structure and behaviors: Method Request and Method Response are the API's interface with the API's frontend (a client), whereas Integration Request and Integration Response are the API's interface with the backend (http://petstore-demo-endpoint.execute-api.com/petstore/pets). A client uses the API to access a backend feature through the Method Request. API Gateway translates the client request, if necessary, into the form acceptable to the backend in Integration Request before forwarding the incoming request to the backend. The transformed request is known as the integration request. Similarly, the backend returns the response to API Gateway in Integration Response. API Gateway then routes it to Method Response before sending it to the client. Again, if necessary, API Gateway can map the backend response data to a form expected by the client.

For the POST method on an API resource, the method request payload can be passed through to the integration request without modification, if the method request's payload is of the same format as the integration request's payload.

The GET / method request uses the MOCK integration type and is not tied to any real backend endpoint. The corresponding Integration Response is set up to return a static HTML page. When the method is called, the API Gateway simply accepts the request and immediately returns the configured integration response to the client by way of Method Response. You can use the mock integration to test an API without requiring a backend endpoint. You can also use it to serve a local response, generated from a response body-mapping template.

As an API developer, you control the behaviors of your API's frontend interactions by configuring the method request and a method response. You control the behaviors of your API's backend interactions by setting up the integration request and integration response. These involve data mappings between a method and its corresponding integration. We cover the method setup in TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56). For now, we focus on testing the API to provide an end-to-end user experience.
7. Choose Test shown on Client (as shown in the previous image) to start testing. For example, to test the POST /pets method, enter the following {"type": "dog","price": 249.99} payload into the Request Body before choosing the Test button.
Method Execution /pets - POST - Method Test

Make a test call to your method with the provided input

Path

No path parameters exist for this resource. You can define path parameters by using the syntax `{myPathParam}` in a resource path.

Query Strings

No query string parameters exist for this method. You can add them via Method Request.

Headers

No header parameters exist for this method. You can add them via Method Request.

Stage Variables

No stage variables exist for this method.

Client Certificate

No client certificates have been generated.

Request Body

```
{
    "type": "dog",
    "price": 249.99
}
```
The input specifies the attributes of the pet that we want to add to the list of pets on the PetStore website.

8. The results display as follows:

Request: /pets
Status: 200
Latency: 566 ms
Response Body

```
{
    "pet": {
        "type": "dog",
        "price": 249.99
    },
    "message": "success"
}
```

Response Headers

```
{"Access-Control-Allow-Origin": "*", "X-Amzn-Trace-Id": "Root=1-59287e14-bd5f1d07c673367bc0739eae, Content-Type": "application/json"}
```

Logs

```
Execution Log for request test-request
Fri May 26 19:12:20 UTC 2017 : Starting execution for request: test-invoke-request
Fri May 26 19:12:20 UTC 2017 : Method request path: {}
Fri May 26 19:12:20 UTC 2017 : Method request query string: {}
Fri May 26 19:12:20 UTC 2017 : Method request headers: {}
Fri May 26 19:12:20 UTC 2017 : Method request body before transformations: {"type": "dog","price": 249.99}
Fri May 26 19:12:20 UTC 2017 : Endpoint request headers: {x-amzn-api-gateway-api-id=9wklk4ojn3, Accept=application/json, User-Agent=AmazonAPIGateway_4wklk4ojn3, X-Amzn-Trace-Id-Root=1-59287e14-bd5f1d07c673367bc0739eae, Content-Type=application/json}
Fri May 26 19:12:20 UTC 2017 : Endpoint request body after transformations: {"type": "dog","price": 249.99}
Fri May 26 19:12:20 UTC 2017 : Endpoint response body before transformations: {
    "pet": {
        "type": "dog",
        "price": 249.99
    },
    "message": "success"
}
 Fri May 26 19:12:20 UTC 2017 : Endpoint response headers: {Connection=keep-alive, Content-Length=81, Date=Fri, 26 May 2017 19:12:20 GMT, Content-Type=application/json; charset=utf-8, X--powered-by=express}
Fri May 26 19:12:20 UTC 2017 : Method response body after transformations: {
    "pet": {
        "type": "dog",
        "price": 249.99
    },
    "message": "success"
}
Fri May 26 19:12:20 UTC 2017 : Method response headers: {Access-Control-Allow-Origin=*, X-Amzn-Trace-Id=Root=1-59287e14-bd5f1d07c673367bc0739eae, Content-Type=application/json}
Fri May 26 19:12:20 UTC 2017 : Successfully completed execution
Fri May 26 19:12:20 UTC 2017 : Method completed with status: 200
```

The Logs entry of the output shows the state changes from the method request to the integration request, and from the integration response to the method response. This can be useful for troubleshooting any mapping errors that cause the request to fail. In this example, no mapping is
applied: the method request payload is passed through the integration request to the backend and, similarly, the backend response is passed through the integration response to the method response.

To test the API using a client other than the API Gateway test-invoke-request feature, you must first deploy the API to a stage.

9. To deploy the sample API, select the PetStore API, and then choose Deploy API from the Actions menu.

In Deploy API, for Deployment stage, choose [New Stage] because this is the first deployment of the API. Type a name (e.g., test) in Stage name and, optionally, type descriptions in Stage description and Deployment description. Choose Deploy.
In the resulting Stage Editor pane, Invoke URL displays the URL to invoke the API’s GET / method request.

10. On Stage Editor, follow the Invoke URL link to submit the GET / method request in a browser. A successful response return the result, generated from the mapping template in the integration response.

11. In the Stages navigation pane, expand the test stage, select GET on /pets/{petId}, and then copy the Invoke URL value of https://api-id.execute-api.region.amazonaws.com/test/pets/{petId}. {petId} stands for a path variable.

Paste the Invoke URL value (obtained in the previous step) into the address bar of a browser, replacing {petId} by, for example, 1, and press Enter to submit the request. A 200 OK response should return with the following JSON payload:

```
{
   "id": 1,
   "type": "dog",
   "price": 249.99
}
```

Invoking the API method as shown is possible because its Authorization type is set to NONE. If the AWS_IAM authorization were used, you would sign the request using the Signature Version 4 (SigV4) protocols. For an example of such a request, see the section called “TUTORIAL: Build an API with HTTP Non-Proxy Integration” (p. 56).

**Build an API Gateway API with HTTP Integration**

To build an API with HTTP integration, you can use either the HTTP proxy integration or the HTTP custom integration. We recommend that you use the HTTP proxy integration, whenever possible, for the
streamlined API set up while providing versatile and powerful features. The HTTP custom integration can be compelling if it is necessary to transform client request data for the backend or transform the backend response data for the client.

**Topics**
- TUTORIAL: Build an API with HTTP Proxy Integration (p. 51)
- TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56)

**TUTORIAL: Build an API with HTTP Proxy Integration**

HTTP proxy integration is a simple, powerful, and versatile mechanism to build an API that allows a web application to access multiple resources or features of the integrated HTTP endpoint, for example the entire website, with a streamlined setup of a single API method. In HTTP proxy integration, API Gateway passes the client-submitted method request to the backend. The request data that is passed through includes the request headers, query string parameters, URL path variables, and payload. The backend HTTP endpoint or the web server parses the incoming request data to determine the response that it returns. HTTP proxy integration makes the client and backend interact directly with no intervention from API Gateway after the API method is set up, except for known issues such as unsupported characters, which are listed in the section called “Important Notes” (p. 692).

With the all-encompassing proxy resource \{proxy+\}, and the catch-all \texttt{ANY} verb for the HTTP method, you can use an HTTP proxy integration to create an API of a single API method. The method exposes the entire set of the publicly accessible HTTP resources and operations of a website. When the backend web server opens more resources for public access, the client can use these new resources with the same API setup. To enable this, the website developer must communicate clearly to the client developer what the new resources are and what operations are applicable for each of them.

As a quick introduction, the following tutorial demonstrates the HTTP proxy integration. In the tutorial, we create an API using the API Gateway console to integrate with the PetStore website through a generic proxy resource \{proxy+\}, and create the HTTP method placeholder of \texttt{ANY}.

**Topics**
- Create an API with HTTP Proxy Integration Using the API Gateway Console (p. 51)
- Test an API with HTTP Proxy Integration (p. 53)

**Create an API with HTTP Proxy Integration Using the API Gateway Console**

The following procedure walks you through the steps to create and test an API with a proxy resource for an HTTP backend using the API Gateway console. The HTTP backend is the PetStore website (http://petstore-demo-endpoint.execute-api.com/petstore/pets) from TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56), in which screenshots are used as visual aids to illustrate the API Gateway UI elements. If you are new to using the API Gateway console to create an API, you may want to follow that section first.

**To build an API with HTTP proxy integration with the PetStore website through a proxy resource**

2. To create an API, choose Create new API (for creating the first API) or Create API (for creating any subsequent API). Next, do the following:
   a. Choose New API.
b. Type a name in **API Name**.

c. Optionally, add a brief description in **Description**.

d. Choose **Create API**.

For this tutorial, use `ProxyResourceForPetStore` for the API name.

3. To create a child resource, choose a parent resource item under the **Resources** tree and then choose **Create Resource** from the **Actions** drop-down menu. Then, do the following in the **New Child Resource** pane.

   a. Select the **Configure as proxy resource** option to create a proxy resource. Otherwise, leave it de-selected.

   b. Type a name in the **Resource Name** input text field.

   c. Type a new name or use the default name in the **Resource Path** input text field.

   d. Choose **Create Resource**.

   e. Select **Enable API Gateway CORS**, if required.

For this tutorial, select **Configure as proxy resource**. For **Resource Name**, use the default, `proxy`. For **Resource Path**, use `/{proxy+}`. Select **Enable API Gateway CORS**.

4. To set up the **ANY** method for integration with the HTTP backend, do the following:

   a. Choose the resource just created and then choose **Create Method** from the **Actions** drop-down menu.

   b. Choose **ANY** from the HTTP method drop-down list and then choose the check mark icon to save the choice.

   c. Choose **HTTP Proxy** for **Integration type**.

   d. Type an HTTP backend resource URL in **Endpoint URL**.

   e. Use default settings for other fields.

   f. Choose **Save** to finish configuring the **ANY** method.

For this tutorial, use `http://petstore-demo-endpoint.execute-api.com/{proxy}` for the **Endpoint URL**.
In the API just created, the API’s proxy resource path of `{proxy+}` becomes the placeholder of any of the backend endpoints under `http://petstore-demo-endpoint.execute-api.com/`. For example, it can be `petstore`, `petstore/pets`, and `petstore/pets/{petId}`. The ANY method serves as a placeholder for any of the supported HTTP verbs at run time.

Test an API with HTTP Proxy Integration

Whether a particular client request succeeds depends on the following:

- If the backend has made the corresponding backend endpoint available and, if so, has granted the required access permissions.
- If the client supplies the correct input.

For example, the PetStore API used here does not expose the `/petstore` resource. As such, you get a 404 Resource Not Found response containing the error message of Cannot GET /petstore.

In addition, the client must be able to handle the output format of the backend in order to parse the result correctly. API Gateway does not mediate to facilitate interactions between the client and backend.

To test an API integrated with the PetStore website using HTTP proxy integration through the proxy resource

1. To use the API Gateway console to test invoking the API, do the following.
   a. Choose ANY on a proxy resource in the Resources tree.
   b. Choose Test in the Method Execution pane.
   c. From the Method drop-down list, choose an HTTP verb supported by the backend.
   d. Under Path, type a specific path for the proxy resource supporting the chosen operation.
   e. If required, type a supported query expression for the chosen operation under the Query Strings heading.
   f. If required, type one or more supported header expressions for the chosen operation under the Headers heading.
   g. If configured, set the required stage variable values for the chosen operation under the Stage Variables heading.
h. If prompted and required, choose an API Gateway-generated client certificate under the Client Certificate heading to the operation to be authenticated by the back end.

i. If prompted, type an appropriate request body in the text editor under the Request Body heading.

j. Choose Test to test invoking the method.

For this tutorial, use GET for Method in place of ANY, use petstore/pets for Path in place of the proxy resource path (proxy), and type=fish for Query Strings.
Method Execution  /{proxy+} - ANY - Method Test

Make a test call to your method with the provided input

Method
GET

Path
{proxy}
petstore/pets

Query Strings
{proxy}
type=fish

Headers
{proxy}
Use a colon (:) to separate header name and value, and new lines to declare multiple headers. eg. Accept:application/json.

Stage Variables
No stage variables exist for this method.

Client Certificate
No client certificates have been generated.

Request Body
Request Body is not supported for GET methods.
Because the backend website supports the GET /petstore/pets?type=fish request, it returns a successful response similar to the following:

```
[
  {
    "id": 1,
    "type": "fish",
    "price": 249.99
  },
  {
    "id": 2,
    "type": "fish",
    "price": 124.99
  },
  {
    "id": 3,
    "type": "fish",
    "price": 0.99
  }
]
```

If you try to call GET /petstore, you get a 404 response with an error message of Cannot GET /petstore. This is because the backend does not support the specified operation. If you call GET /petstore/pets/1, you get a 200 OK response with the following payload, because the request is supported by the PetStore website.

```
{
  "id": 1,
  "type": "dog",
  "price": 249.99
}
```

2. To use a browser to call a GET method on a specific resource of the API, do the following.

   a. If you have not done so, choose Deploy API from the Actions drop-down menu for the API you created. Follow the instructions to deploy the API to a specific stage. Note the Invoke URL that displays on the resulting Stage Editor page. This is the base URL of the API.

   b. To submit a GET request on a specific resource, append the resource path, including possible query string expressions to the Invoke URL value obtained in the previous step, copy the complete URL into the address bar of a browser, and choose Enter.

   For this tutorial, deploy the API to a test stage and append petstore/pets?type=fish to the API's Invoke URL. This produces a URL of https://4z9gli12c1.execute-api.us-west-2.amazonaws.com/test/petstore/pets?type=fish.

   The result should be the same as returned when you use TestInvoke from the API Gateway console.

**TUTORIAL: Build an API with HTTP Non-Proxy Integration**

In this tutorial, you create an API from scratch using the Amazon API Gateway console. You can think of the console as an API design studio and use it to scope the API features, to experiment with its behaviors, to build the API, and to deploy your API in stages.
Create an API with HTTP Custom Integration

This section walks you through the steps to create resources, expose methods on a resource, configure a method to achieve the desired API behaviors, and to test and deploy the API.

2. To create an API, choose Create new API (for creating the first API) or Create API (for creating any subsequent API). Next, do the following:
   a. Choose New API.
   b. Type a name in API Name.
   c. Optionally, add a brief description in Description.
   d. Choose Create API.

As a result, an empty API is created. The Resources tree shows the root resource (/) without any methods. In this exercise, we will build the API with the HTTP custom integration of the PetStore website (http://petstore-demo-endpoint.execute-api.com/petstore/pets.) For illustration purposes, we will create a /pets resource as a child of the root and expose a GET method on this resource for a client to retrieve a list of available Pets items from the PetStore website.

3. To create the /pets resource, select the root, choose Actions and then choose Create Resource.
   Type Pets in Resource Name, leave the Resource Path value as given, choose Enable API Gateway CORS, and choose Create Resource.

4. To expose a GET method on the /pets resource, choose Actions and then Create Method.
Choose **GET** from the list under the `/pets` resource node and choose the check mark icon to finish creating the method.
Note
Other options for an API method include:

- **POST**, primarily used to create child resources.
- **PUT**, primarily used to update existing resources (and, although not recommended, can be used to create child resources).
- **DELETE**, used to delete resources.
- **PATCH**, used to update resources.
- **HEAD**, primarily used in testing scenarios. It is the same as GET but does not return the resource representation.
- **OPTIONS**, which can be used by callers to get information about available communication options for the target service.

The method created is not yet integrated with the backend. The next step sets this up.

5. In the method's Setup pane, select HTTP for Integration type, select GET from the HTTP method drop-down list, type `http://petstore-demo-endpoint.execute-api.com/petstore/pets` as the Endpoint URL value, leave all other settings as default, and then choose Save.

Note
For the integration request's HTTP method, you must choose one supported by the backend. For HTTP or Mock integration, it makes sense that the method request and the integration request use the same HTTP verb. For other integration types the method request will likely use an HTTP verb different from the integration request. For example, to call a Lambda function, the integration request must use **POST** to invoke the function, whereas the method request may use any HTTP verb depending on the logic of the Lambda function.
When the method setup finishes, you are presented with the **Method Execution** pane, where you can further configure the method request to add query string or custom header parameters. You can also update the integration request to map input data from the method request to the format required by the back end.

The PetStore website allows you to retrieve a list of Pet items by the pet type (e.g., "Dog" or "Cat") on a given page. It uses the type and page query string parameters to accept such input. As such, we must add the query string parameters to the method request and map them into the corresponding query strings of the integration request.

6. In the GET method's **Method Execution** pane, choose **Method Request**, select **AWS_IAM** for **Authorization**, expand the **URL Query String Parameters** section, and choose **Add query string** to create two query string parameters named `type` and `page`. Choose the check mark icon to save each query string parameter as you add it.
The client can now supply a pet type and a page number as query string parameters when submitting a request. These input parameters must be mapped into the integration's query string parameters to forward the input values to our PetStore website in the backend. Because the method uses AWS_IAM, you must sign the request to invoke the method.

7. From the method's Integration Request page, expand the URL Query String Parameters section. By default, the method request query string parameters are mapped to the like-named integration request query string parameters. This default mapping works for our demo API. We will leave them as given. To map a different method request parameter to the corresponding integration request parameter, choose the pencil icon for the parameter to edit the mapping expression, shown in the Mapped from column. To map a method request parameter to a different integration request parameter, first choose the delete icon to remove the existing integration request parameter, choose Add query string to specify a new name and the desired method request parameter mapping expression.
This completes building the simple demo API. It’s time to test the API.

8. To test the API using the API Gateway console, choose Test on the Method Execution pane for the GET /pets method. In the Method Test pane, enter dog and 2 for the type and page query strings, respectively, and then choose Test.
The result is shown as follows. (You may need to scroll down to see the test result.)
Now that the test is successful, we can deploy the API to make it publicly available.

9. To deploy the API, select the API and then choose Deploy API from the Actions drop-down menu.
In the **Deploy API** dialog, choose a stage (or **[New Stage]** for the API's first deployment); enter a name (e.g., "test", "prod", "dev", etc.) in the **Stage name** input field; optionally, provide a description in **Stage description** and/or **Deployment description**; and then choose **Deploy**.

Once deployed, you can obtain the invocation URLs (**Invoke URL**) of the API's endpoints.
If the GET method supported open access, (i.e., if the method's authorization type were set to NONE) you could double-click the Invoke URL link to invoke the method in your default browser. If needed, you could also append necessary query string parameters to the invocation URL. With the AWS IAM authorization type described here, you must sign the request with an access key ID and the corresponding secret key of an IAM user of your AWS account. To do this, you must use a client that supports the Signature Version 4 (SigV4) protocols. An example of such a client is an app that uses one of the AWS SDKs or the Postman application or cURL commands. To call a POST, PUT, or PATCH method that take a payload, you also need to use such a client to handle the payload.

To invoke this API method in the Postman, append the query string parameters to the stage-specific method invocation URL (as shown in the previous image) to create the complete method request URL:


Specify this URL in the address bar of the browser. Choose GET as the HTTP verb. Select AWS Signature for the Type option under the Authorization tab, and then specify the following required properties before sending the request:

- For AccessKey, type the caller's AWS access key, as provisioned from AWS IAM.
- For SecretKey, type the caller's AWS secret key, as provisioned from AWS IAM when the access key was first created.
- For AWS Region, type the API-hosting AWS Region, as specified in the invocation URL.
- For Service Name, type execute-api, for the API Gateway execution service.

If you use an SDK to create a client, you can call the methods exposed by the SDK to sign the request. For implementation details, see the AWS SDK of your choosing.

**Note**

When changes are made to your API, you must redeploy the API to make the new or updated features available before invoking the request URL again.

## Map Request Parameters for an API Gateway API

In this walkthrough, we describe how to map method request parameters to the corresponding integration request parameters for an API Gateway API. We create an example API with the HTTP custom integration and use it to demonstrate how to use API Gateway to map a method request parameter to the corresponding integration request parameter. We then access the following publicly accessible HTTP endpoint:

http://petstore-demo-endpoint.execute-api.com/petstore/pets

If you copy the above URL, paste it into the address bar of a web browser, and press Enter or Return, you get the following JSON-formatted response body:

```json
[
  {
    "id": 1,
    "type": "dog",
    "price": 249.99
  },
  {
    "id": 2,
    "type": "cat",
    "price": 66
  }
]
```
The preceding endpoint can take two query parameters: type and page. For example, change the URL to the following:


You receive the following JSON-formatted response payload, displaying page 2 of only the cats:

[
  {
    "id": 4,
    "type": "cat",
    "price": 999.99
  },
  {
    "id": 5,
    "type": "cat",
    "price": 249.99
  },
  {
    "id": 6,
    "type": "cat",
    "price": 49.97
  }
]

This endpoint also supports the use of an item ID, as expressed by a URL path parameter. For example, browse to the following:

http://petstore-demo-endpoint.execute-api.com/petstore/pets/1

The following JSON-formatted information about the item with an ID of 1 is displayed:

{
  "id": 1,
  "type": "dog",
  "price": 249.99
}

In addition to supporting GET operations, this endpoint takes POST requests with a payload. For example, use Postman to send a POST method request to the following:

http://petstore-demo-endpoint.execute-api.com/petstore/pets

Include the header Content-type: application/json and the following request body:

{
  "type": "dog",
}
You receive the following JSON object in the response body:

```
{
  "pet": {
    "type": "dog",
    "price": 249.99
  },
  "message": "success"
}
```

We now expose these and other features by building an API Gateway API with the HTTP custom integration of this PetStore website. The tasks include the following:

- Enable the API to accept two method request query parameters of `petType` and `petsPage`, map them to the `type` and `page` query parameters of the integration request, respectively, and pass the request to the HTTP endpoint.
- Support a path parameter of `{petId}` on the API's method request URL to specify an item ID, map it to the `{id}` path parameter in the integration request URL, and send the request to the HTTP endpoint.
- Enable the method request to accept the JSON payload of the format defined by the backend website, and pass the payload without modification through the integration request to the backend HTTP endpoint.

**Topics**
- Prerequisites (p. 68)
- Step 1: Create Resources (p. 68)
- Step 2: Create and Test the Methods (p. 69)
- Step 3: Deploy the API (p. 72)
- Step 4: Test the API (p. 72)

**Note**
Pay attention to the casing used in the steps of this walkthrough. Typing a lowercase letter instead of an uppercase letter (or vice versa) can cause errors later in the walkthrough.

**Prerequisites**

Before you begin this walkthrough, you should do the following:

1. Complete the steps in Prerequisites: Get Ready to Build an API in API Gateway (p. 10), including assigning API Gateway access permission to the IAM user.
2. At a minimum, follow the steps in TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56) to create a new API named `MyDemoAPI` in the API Gateway console.

**Step 1: Create Resources**

In this step, you create three resources that enable the API to interact with the HTTP endpoint.
To create the first resource

1. In the Resources pane, select the resource root, as represented by a single forward slash (/), and then choose Create Resource from the Actions drop-down menu.
2. For Resource Name, type petstorewalkthrough.
3. For Resource Path, accept the default of /petstorewalkthrough, and then choose Create Resource.

To create the second resource

1. In the Resources pane, choose /petstorewalkthrough, and then choose Create Resource.
2. For Resource Name, type pets.
3. For Resource Path, accept the default of /petstorewalkthrough/pets, and then choose Create Resource.

To create the third resource

1. In the Resources pane, choose /petstorewalkthrough/pets, and then choose Create Resource.
2. For Resource Name, type petId. This maps to the item ID in the HTTP endpoint.
3. For Resource Path, overwrite petid with {petId}. Use curly braces ({ }) around petId so that /petstorewalkthrough/pets/{petId} is displayed, and then choose Create Resource.

This maps to /petstore/pets/my-item-id in the HTTP endpoint.

Step 2: Create and Test the Methods

In this step, you integrate the methods with the backend HTTP endpoints, map the GET method request parameters to the corresponding integration request parameters, and then test the methods.

To set up and test the first GET method

This procedure demonstrates the following:

- Create and integrate the method request of GET /petstorewalkthrough/pets with the integration request of GET http://petstore-demo-endpoint.execute-api.com/petstore/pets.
- Map the method request query parameters of petType and petsPage to the integration request query string parameters of type and page, respectively.

1. In the Resources pane, choose /petstorewalkthrough/pets, choose Create Method from the Actions menu, and then choose GET under /pets from the drop-down list of the method names.
2. In the /petstorewalkthrough/pets - GET - Setup pane, choose HTTP for Integration type and choose GET for HTTP method.
4. Choose Save.
5. In the Method Execution pane, choose Method Request, and then choose the arrow next to URL Query String Parameters.
6. Choose Add query string.
7. For Name, type petType.

This specifies the petType query parameter in the API's method request.
8. Choose the check mark icon to finish creating the method request URL query string parameter.
9. Choose Add query string again.
10. For Name, type petsPage.

This specifies the petsPage query parameter in the API's method request.
11. Choose the check mark icon to finish creating the method request URL query string parameter.
12. Choose Method Execution, choose Integration Request, and then choose the arrow next to URL Query String Parameters.
13. Delete the petType entry mapped from method.request.querystring.petType and the petsPage entry mapped from method.request.querystring.petsPage. You perform this step because the endpoint requires query string parameters named type and page for the request URL, instead of the default values.
15. For Name, type type. This creates the required query string parameter for the integration request URL.
16. For Mapped from, type method.request.querystring.petType.

This maps the method request's petType query parameter to the integration request's type query parameter.
17. Choose the check mark icon to finish creating the integration request URL query string parameter.
18. Choose Add query string again.
19. For Name, type page. This creates the required query string parameter for the integration request URL.
20. For Mapped from, type method.request.querystring.petsPage.

This maps the method request's petsPage query parameter to the integration request's page query parameter.
21. Choose the check mark icon to finish creating the integration request URL query string parameter.
22. Choose Method Execution. In the Client box, choose TEST. In the Query Strings area, for petType, type cat. For petsPage, type 2.
23. Choose Test. If successful, Response Body displays the following:

```
[
  {
    "id": 4,
    "type": "cat",
    "price": 999.99
  },
  {
    "id": 5,
    "type": "cat",
    "price": 249.99
  },
  {
    "id": 6,
    "type": "cat",
    "price": 49.97
  }
]
```

To set up and test the second GET method

This procedure demonstrates the following:
• Create and integrate the method request of GET /petstorewalkthrough/pets/{petId} with the integration request of GET http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}.

• Map the method request path parameters of petId to the integration request path parameters of id.

1. In the Resources list, choose /petstorewalkthrough/pets/{petId}, choose Create Method from the Actions drop-down menu, and then choose GET as the HTTP verb for the method.
2. In the Setup pane, choose HTTP for Integration type and choose GET for HTTP method.
3. For Endpoint URL, type http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}.
4. Choose Save.
5. In the Method Execution pane, choose Integration Request, and then choose the arrow next to URL Path Parameters.
6. Choose Add path.
7. For Name, type id.
8. For Mapped from, type method.request.path.petId.

   This maps the method request's path parameter of petId to the integration request's path parameter of id.
9. Choose the check mark icon to finish creating the URL path parameter.
10. Choose Method Execution, and in the Client box, choose TEST. In the Path area, for petId, type 1.
11. Choose Test. If successful, Response Body displays the following:

```json
{
   "id": 1,
   "type": "dog",
   "price": 249.99
}
```

To set up and test the POST method

This procedure demonstrates the following:

• Create and integrate the method request of POST /petstorewalkthrough/pets with the integration request of POST http://petstore-demo-endpoint.execute-api.com/petstore/pets.

• Pass the method request JSON payload through to the integration request payload, without modification.

1. In the Resources pane, choose /petstorewalkthrough/pets, choose Create Method from the Actions drop-down menu, and then choose POST as the HTTP verb for the method.
2. In the Setup pane, choose HTTP for Integration type and choose POST for HTTP method.
4. Choose Save.
5. In the Method Execution pane, in the Client box, choose TEST. Expand Request Body, and then type the following:

```json
{
}
```
6. Choose Test. If successful, **Response Body** displays the following:

   ```json
   {
     "pet": {
       "type": "dog",
       "price": 249.99
     },
     "message": "success"
   }
   ```

### Step 3: Deploy the API

In this step, you deploy the API so that you can begin calling it outside of the API Gateway console.

**To deploy the API**

1. In the Resources pane, choose **Deploy API**.
2. For **Deployment stage**, choose **test**.

   **Note**
   
   The input must be UTF-8 encoded (i.e., unlocalized) text.

3. For **Deployment description**, type **Calling HTTP endpoint walkthrough**.
4. Choose **Deploy**.

### Step 4: Test the API

In this step, you go outside of the API Gateway console and use your API to access the HTTP endpoint.

1. In the Stage Editor pane, next to **Invoke URL**, copy the URL to the clipboard. It should look something like this:

   ```text
   https://my-api-id.execute-api.region-id.amazonaws.com/test
   ```

2. Paste this URL in the address box of a new browser tab.
3. Append `/petstorewalkthrough/pets` so that it looks like this:

   ```text
   https://my-api-id.execute-api.region-id.amazonaws.com/test/petstorewalkthrough/pets
   ```

   Browse to the URL. The following information should be displayed:

   ```json
   [
     {
       "id": 1,
       "type": "dog",
       "price": 249.99
     },
     {
       "id": 2,
       "type": "cat",
       "price": 124.99
     }
   ]
   ```
4. After `petstorewalkthrough/pets`, type `?petType=cat&petsPage=2` so that it looks like this:

```
```

5. Browse to the URL. The following information should be displayed:

```
[
  {
    "id": 4,
    "type": "cat",
    "price": 999.99
  },
  {
    "id": 5,
    "type": "cat",
    "price": 249.99
  },
  {
    "id": 6,
    "type": "cat",
    "price": 49.97
  }
]
```

6. After `petstorewalkthrough/pets`, replace `?petType=cat&petsPage=2` with `/1` so that it looks like this:

```
https://my-api-id.execute-api.region-id.amazonaws.com/test/petstorewalkthrough/pets/1
```

7. Browse to the URL. The following information should be displayed:

```
{
  "id": 1,
  "type": "dog",
  "price": 249.99
}
```

8. Using a web debugging proxy tool or the cURL command-line tool, send a POST method request to the URL from the previous procedure. Append `/petstorewalkthrough/pets` so that it looks like this:

```
https://my-api-id.execute-api.region-id.amazonaws.com/test/petstorewalkthrough/pets
```

Append the following header:

```
Content-Type: application/json
```

Add the following code to the request body:

```
{
  "type": "dog",
  "price": 249.99
}
```
For example, if you use the cURL command-line tool, run a command similar to the following:

```bash
```

The following information should be returned in the response body:

```json
{
    "pet": {
        "type": "dog",
        "price": 249.99
    },
    "message": "success"
}
```

You have reached the end of this walkthrough.

**Map Response Payload**

In this walkthrough, we show how to use models and mapping templates in API Gateway to transform the output of an API call from one data schema to another. This walkthrough builds on the instructions and concepts in the Getting Started with Amazon API Gateway (p. 10) and the Map Request Parameters for an API Gateway API (p. 66). If you have not yet completed those walkthroughs, we suggest you do them first.

This walkthrough uses API Gateway to get example data from a publicly accessible HTTP endpoint and from an AWS Lambda function you create. Both the HTTP endpoint and the Lambda function return the same example data:

```json
[  
    {  
        "id": 1,
        "type": "dog",
        "price": 249.99
    },
    {  
        "id": 2,
        "type": "cat",
        "price": 124.99
    },
    {  
        "id": 3,
        "type": "fish",
        "price": 0.99
    }
]
```

You will use models and mapping templates to transform this data to one or more output formats. In API Gateway, a model defines the format, also known as the schema or shape, of some data. In API Gateway, a mapping template is used to transform some data from one format to another. For more information, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

The first model and mapping template is used to rename `id` to `number`, `type` to `class`, and `price` to `salesPrice`, as follows:
The second model and mapping template is used to combine id and type into description, and to rename price to askingPrice, as follows:

```json
[
  { "description": "Item 1 is a dog.\n  "askingPrice": 249.99
  },
  { "description": "Item 2 is a cat.\n  "askingPrice": 124.99
  },
  { "description": "Item 3 is a fish.\n  "askingPrice": 0.99
  }
]
```

The third model and mapping template is used to combine id, type, and price into a set of listings, as follows:

```json
{
  "listings": [
    "Item 1 is a dog. The asking price is 249.99.\n    "Item 2 is a cat. The asking price is 124.99.\n    "Item 3 is a fish. The asking price is 0.99."
  ]
}
```

**Topics**

- Step 1: Create Models (p. 76)
- Step 2: Create Resources (p. 77)
- Step 3: Create GET Methods (p. 78)
- Step 4: Create a Lambda Function (p. 79)
- Step 5: Set up and Test the Methods (p. 80)
- Step 6: Deploy the API (p. 83)
- Step 7: Test the API (p. 83)
- Step 8: Clean Up (p. 85)
Step 1: Create Models

In this step, you create four models. The first three models represent the data output formats for use with the HTTP endpoint and the Lambda function. The last model represents the data input schema for use with the Lambda function.

To create the first output model

2. If MyDemoAPI is displayed, choose Models.
3. Choose Create.
4. For Model name, type PetsModelNoFlatten.
5. For Content type, type application/json.
6. For Model description, type Changes id to number, type to class, and price to salesPrice.
7. For Model schema, type the following JSON Schema-compatible definition:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "PetsModelNoFlatten",
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "number": { "type": "integer" },
      "class": { "type": "string" },
      "salesPrice": { "type": "number" }
    }
  }
}
```
8. Choose Create model.

To create the second output model

1. Choose Create.
2. For Model name, type PetsModelFlattenSome.
3. For Content type, type application/json.
4. For Model description, type Combines id and type into description, and changes price to askingPrice.
5. For Model schema, type the following:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "PetsModelFlattenSome",
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "description": { "type": "string" },
      "askingPrice": { "type": "number" }
    }
  }
}
```
6. Choose Create model.
To create the third output model

1. Choose Create.
2. For **Model name**, type `PetsModelFlattenAll`.
3. For **Content type**, type `application/json`.
4. For **Model description**, type *Combines id, type, and price into a set of listings.*
5. For **Model schema**, type the following:

   ```json
   {
     "$schema": "http://json-schema.org/draft-04/schema#",
     "title": "PetsModelFlattenAll",
     "type": "object",
     "properties": {
       "listings": {
         "type": "array",
         "items": {
           "type": "string"
         }
       }
     }
   }
   ```

6. Choose Create model.

To create the input model

1. Choose Create.
2. For **Model name**, type `PetsLambdaModel`.
3. For **Content type**, type `application/json`.
4. For **Model description**, type *GetPetsInfo model.*
5. For **Model schema**, type the following:

   ```json
   {
     "$schema": "http://json-schema.org/draft-04/schema#",
     "title": "PetsLambdaModel",
     "type": "array",
     "items": {
       "type": "object",
       "properties": {
         "id": { "type": "integer" },
         "type": { "type": "string" },
         "price": { "type": "number" }
       }
     }
   }
   ```

6. Choose Create model.

**Step 2: Create Resources**

In this step, you create four resources. The first three resources enable you to get the example data from the HTTP endpoint in the three output formats. The last resource enables you to get the example data from the Lambda function in the output schema that combines `id` and `type` into `description` and renames `price` to `askingPrice`.
To create the first resource

1. In the links list, choose Resources.
2. In the Resources pane, choose /petstore walkthrough, and then choose Create Resource.
3. For Resource Name, type NoFlatten.
4. For Resource Path, accept the default of /petstore walkthrough/noflatten, and then choose Create Resource.

To create the second resource

1. In the Resources pane, choose /petstore walkthrough again, and then choose Create Resource.
2. For Resource Name, type FlattenSome.
3. For Resource Path, accept the default of /petstore walkthrough/flattensome, and then choose Create Resource.

To create the third resource

1. In the Resources pane, choose /petstore walkthrough again, and then choose Create Resource.
2. For Resource Name, type FlattenAll.
3. For Resource Path, accept the default of /petstore walkthrough/flattenall, and then choose Create Resource.

To create the fourth resource

1. In the Resources pane, choose /petstore walkthrough again, and then choose Create Resource.
2. For Resource Name, type LambdaFlattenSome.
3. For Resource Path, accept the default of /petstore walkthrough/lambdaflattensome, and then choose Create Resource.

Step 3: Create GET Methods

In this step, you create a GET method for each of the resources you created in the previous step.

To create the first GET method

1. In the Resources list, choose /petstore walkthrough/flattenall, and then choose Create Method.
2. From the drop-down list, choose GET, and then choose the check mark icon to save your choice.

To create the second GET method

1. In the Resources list, choose /petstore walkthrough/lambdaflattensome, and then choose Create Method.
2. From the drop-down list, choose GET, and then choose the check mark to save your choice.
3. In the Setup pane, choose Lambda Function for the Integration type, choose the region where you have created the GetPetsInfo Lambda function (p. 79) from the Lambda Region drop-down list, choose GetPetsInfo for Lambda Function, and choose Save. Choose OK when prompted to add permission to the Lambda function.
To create the third GET method

1. In the Resources list, choose `/petstorewalkthrough/flattensome`, and then choose Create Method.
2. From the drop-down list, choose GET, and then choose the check mark icon to save your choice.
3. In the Setup pane, choose HTTP for the Integration type and GET for HTTP method, type `http://petstore-demo-endpoint.execute-api.com/petstorepets` in Endpoint URL, and then choose Save.

To create the fourth GET method

1. In the Resources list, choose `/petstorewalkthrough/noflatten`, and then choose Actions, Create Method.
2. From the drop-down list, choose GET, and then choose the check mark icon to save your choice.
3. In the Setup pane, choose HTTP for the Integration type and GET for HTTP method, type `http://petstore-demo-endpoint.execute-api.com/petstorepets` in Endpoint URL, and then choose Save.

Step 4: Create a Lambda Function

In this step, you create a Lambda function that returns the sample data.

To create the Lambda function

2. Do one of the following:
   - If a welcome page appears, choose Get Started Now.
   - If the Lambda: Function list page appears, choose Create a Lambda function.
3. For Name, type GetPetsInfo.
4. For Description, type Gets information about pets.
5. For Code template, choose None.
6. Type the following code:

```javascript
console.log('Loading event');
exports.handler = function(event, context, callback) {
  callback(null,
    [{"id": 1, "type": "dog", "price": 249.99},
     {"id": 2, "type": "cat", "price": 124.99},
     {"id": 3, "type": "fish", "price": 0.99}]); // SUCCESS with message
};
```

Tip
In the preceding code, written in Node.js, `console.log` writes information to an Amazon CloudWatch log. event contains the input to the Lambda function. context contains calling context. callback returns the result. For more information about how to write Lambda function code, see the 'Programming Model' section in AWS Lambda: How it Works and the sample walkthroughs in the AWS Lambda Developer Guide.

7. For Handler name, leave the default of index.handler.
8. For Role, choose the Lambda execution role, APIGatewayLambdaExecRole, you created in the Build an API Gateway API with Lambda Integration (p. 26).
9. Choose Create Lambda function.
10. In the list of functions, choose GetPetsInfo to show the function's details.
11. Make a note of the AWS region where you created this function. You need it later.
12. In the pop-up list, choose Edit or test function.
13. For Sample event, replace any code that appears with the following:

```json
{
}
```

**Tip**
The empty curly braces mean that there are no input values for this Lambda function. This function simply returns the JSON object containing the pets information, so those key-value pairs are not required here.

14. Choose Invoke. Execution result shows `[{"id":1,"type":"dog","price":249.99},
{"id":2,"type":"cat","price":124.99},{"id":3,"type":"fish","price":0.99}]`, which is also written to the CloudWatch Logs log files.

15. Choose Go to function list.

**Step 5: Set up and Test the Methods**

In this step, you configure the method responses, integration requests, and integration responses to specify the input and output data schemas (or models) for the GET methods associated with the HTTP endpoint and the Lambda function. You also learn to test calling these methods using the API Gateway console.

**To set up the integration for the first GET method and then test it**

1. From the API's Resources tree, choose GET under the /petstorewalkthrough/flattenall node.
2. In the Method Execution pane, choose Method Response, and then choose the arrow next to 200.
3. In the Response Models for 200 area, for application/json, choose the pencil icon to start setting up the model for the method output. For Models, choose PetsModelFlattenAll, and then choose the check mark icon to save the setting.
4. Choose Method Execution, choose Integration Response, and then choose the arrow next to 200.
5. Expand the Body Mapping Templates section, choose application/json under Content-Type.
6. For Generate template from model, choose PetsModelFlattenAll to display a mapping template after the PetsModelFlattenAll model as a starting point.
7. Modify the mapping template code as follows:

```bash
#set($inputRoot = $input.path('"\')
{
   "listings" : [
   #foreach($elem in $inputRoot)
   "Item number $elem.id is a $elem.type. The asking price is $elem.price."#if($foreach.hasNext),#end
   #end
   ]
}
```
8. Choose Save.
9. Choose Method Execution, and in the Client box, choose TEST, and then choose Test. If successful, Response Body displays the following:

```json
{
```
To set up integration for the second GET method and then test it

1. From the API's Resources tree, choose GET under the /petstorewalkthrough/lambdaflattensome node.
2. In Method Execution, choose Method Response. And then choose the arrow next to 200 to expand the section.
3. In the Response Models for 200 area, choose the pencil icon on the row for the content type of application/json. Choose PetsModelFlattenSome for Models, and then choose the check mark icon to save the choice.
4. Go back to Method Execution. Choose Integration Response, and then choose the arrow next to 200.
5. In the Body Mapping Templates section, choose application/json under Content-Type.
6. For Generate template, choose PetsModelFlattenSome to display the mapping script template for the output of this method.
7. Modify the code as follows, and then choose Save:

```
#set($inputRoot = $input.path(''))
[
  #foreach($elem in $inputRoot)
    {
      "description" : "Item $elem.id is a $elem.type.",
      "askingPrice" : $elem.price
    }#if($foreach.hasNext),#end
  #end
]
```

8. Choose Method Execution, and in the Client box, choose TEST, and then choose Test. If successful, Response Body displays the following:

```
[
  {
    "description" : "Item 1 is a dog."
    "askingPrice" : 249.99
  },
  {
    "description" : "Item 2 is a cat."
    "askingPrice" : 124.99
  },
  {
    "description" : "Item 3 is a fish."
    "askingPrice" : 0.99
  }
]
```

To set up integration for the third GET method and then test it

1. From the API's Resources tree, choose GET under the /petstorewalkthrough/flattensome node.
2. In the Method Execution pane, choose Method Response.
3. Choose the arrow next to 200.

4. In the Response Models for 200 area, for application/json, choose the pencil icon. For Models, choose PetsModelFlattenSome, and then choose the check-mark icon to save the choice.

5. Go back to Method Execution and choose Integration Response.

6. Choose the arrow next to 200 to expand the section.

7. Expand the Body Mapping Templates area. Choose application/json for Content-Type. For Generate template, choose PetsModelFlattenSome to display a mapping script template for the output of this method.

8. Modify the code as follows:

```java
#set($inputRoot = $input.path('$'))
[
#foreach($elem in $inputRoot)
  {
    "description": "Item $elem.id is a $elem.type.",
    "askingPrice": $elem.price
  }#if($foreach.hasNext),#end
#end
]
```

9. Choose Save.

10. Go back to Method Execution and choose TEST in the Client box. And then choose Test. If successful, Response Body displays the following:

```json
[
  {
    "description": "Item 1 is a dog.",
    "askingPrice": 249.99
  },
  {
    "description": "Item 2 is a cat.",
    "askingPrice": 124.99
  },
  {
    "description": "Item 3 is a fish.",
    "askingPrice": 0.99
  }
]
```

To set up integration for the fourth GET method and then test it

1. From the API's Resources tree, choose GET under the /petstorewalkthrough/noflatten node.

2. In the Method Execution pane, choose Method Response, and then expand the 200 section.

3. In the Response Models for 200 area, for application/json, choose the pencil icon to update the response model for this method.

4. Choose PetsModelNoFlatten as the model for the content type of application/json, and then choose the check-mark icon to save the choice.

5. Choose Method Execution, choose Integration Response, and then choose the arrow next to 200 to expand the section.

6. Expand the Mapping Templates section. Choose application/json for Content-Type. For Generate templates, choose PetsModelNoFlatten to display a mapping script template for the output of this method.

7. Modify the code as follows:
8. Choose Save.
9. Go back to Method Execution, and in the Client box, choose TEST, and then choose Test. If successful, Response Body displays the following:

```json
[
  {
    "number": 1,
    "class": "dog",
    "salesPrice": 249.99
  },
  {
    "number": 2,
    "class": "cat",
    "salesPrice": 124.99
  },
  {
    "number": 3,
    "class": "fish",
    "salesPrice": 0.99
  }
]
```

**Step 6: Deploy the API**

In this step, you deploy the API so that you can begin calling it outside of the API Gateway console.

**To deploy the API**

1. In the Resources pane, choose Deploy API.
2. For Deployment stage, choose test.
3. For Deployment description, type Using models and mapping templates walkthrough.

**Step 7: Test the API**

In this step, you go outside of the API Gateway console to interact with both the HTTP endpoint and the Lambda function.

1. In the Stage Editor pane, next to Invoke URL, copy the URL to the clipboard. It should look something like this:

   `https://my-api-id.execute-api.region-id.amazonaws.com/test`

2. Paste this URL in the address box of a new browser tab.
3. Append /petstorewalkthrough/noflatten so that it looks like this:

```
https://my-api-id.execute-api.region-id.amazonaws.com/test/petstorewalkthrough/noflatten
```

Browse to the URL. The following information should be displayed:

```
[
  {
    "number": 1,
    "class": "dog",
    "salesPrice": 249.99
  },
  {
    "number": 2,
    "class": "cat",
    "salesPrice": 124.99
  },
  {
    "number": 3,
    "class": "fish",
    "salesPrice": 0.99
  }
]
```

4. After petstorewalkthrough/, replace noflatten with flattensome.

5. Browse to the URL. The following information should be displayed:

```
[
  {
    "description": "Item 1 is a dog.",
    "askingPrice": 249.99
  },
  {
    "description": "Item 2 is a cat.",
    "askingPrice": 124.99
  },
  {
    "description": "Item 3 is a fish.",
    "askingPrice": 0.99
  }
]
```

6. After petstorewalkthrough/, replace flattensome with flattenall.

7. Browse to the URL. The following information should be displayed:

```
{
  "listings": [
    "Item number 1 is a dog. The asking price is 249.99.",
    "Item number 2 is a cat. The asking price is 124.99.",
    "Item number 3 is a fish. The asking price is 0.99."
  ]
}
```

8. After petstorewalkthrough/, replace flattenall with lambdaflattensome.

9. Browse to the URL. The following information should be displayed:

```
[
  {"description": "Item 1 is a dog.",
  
```
Step 8: Clean Up

If you no longer need the Lambda function you created for this walkthrough, you can delete it now. You can also delete the accompanying IAM resources.

**Warning**
If you delete a Lambda function your APIs rely on, those APIs will no longer work. Deleting a Lambda function cannot be undone. If you want to use the Lambda function again, you must re-create the function.
If you delete an IAM resource a Lambda function relies on, the Lambda function and any APIs that rely on it will no longer work. Deleting an IAM resource cannot be undone. If you want to use the IAM resource again, you must re-create the resource. If you plan to continue experimenting with the resources you created for this and the other walkthroughs, do not delete the Lambda invocation role or the Lambda execution role.

To delete the Lambda function

1. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/.
2. On the Lambda: Function list page, in the list of functions, choose the button next to GetPetsInfo, and then choose Actions, Delete. When prompted, choose Delete again.

To delete the associated IAM resources

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the Details area, choose Roles.
3. Select APIGatewayLambdaExecRole, and then choose Role Actions, Delete Role. When prompted, choose Yes, Delete.
4. In the Details area, choose Policies.
5. Select APIGatewayLambdaExecPolicy, and then choose Policy Actions, Delete. When prompted, choose Delete.

You have now reached the end of this walkthrough.

**TUTORIAL: Build an API with API Gateway Private Integration**

You can create an API Gateway API with private integration to provide your customers access to HTTP/HTTPS resources within your Amazon Virtual Private Cloud (Amazon VPC). Such VPC resources are HTTP/HTTPS endpoints on an EC2 instance behind a network load balancer in the VPC. The network load balancer encapsulates the VPC resource and routes incoming requests to the targeted resource.
When a client calls the API, API Gateway connects to the network load balancer through the pre-configure VPC link. A VPC link is encapsulated by an API Gateway resource of VpcLink. It is responsible for forwarding API method requests to the VPC resources and returns backend responses to the caller. For an API developer, a VpcLink is functionally equivalent to an integration endpoint.

To create an API with private integration, you must create a new VpcLink, or choose an existing one, that is connected to a network load balancer that targets the desired VPC resources. You must have appropriate permissions (p. 245) to create and manage a VpcLink. You then set up an API method and integrate it with the VpcLink by setting either HTTP or HTTP_PROXY as the integration type, setting VPC_LINK as the integration connection type, and setting the VpcLink identifier on the integration connectionId.

To quickly get started creating an API to access VPC resources, we walk through the essential steps for building an API with the private integration, using the API Gateway console. Before creating the API, do the following:

1. Create a VPC resource, create or choose a network load balancer under your account in the same region, and add the EC2 instance hosting the resource as a target of the network load balancer. For more information, see Set up a Network Load Balancer for API Gateway Private Integrations (p. 244).
2. Grant permissions to create the VPC links for private integrations. For more information, see Grant Permissions to Create a VPC Link (p. 245).

After creating your VPC resource and your network load balancer with your VPC resource configured in its target groups, follow the instructions below to create an API and integrate it with the VPC resource via a VpcLink in a private integration.

**To create an API with private integration using the API Gateway console**

1. Sign in to the API Gateway console and choose a region; for example, us-west-2, on the navigation bar.
2. Create a VPC link, if you have not already done so:
   a. From the primary navigation pane, choose VPC Links and then choose + Create.
   b. Under VPC Link, type a name (for example, my-test-vpc-link) in the Name field.
   c. Optionally, give a description of the VPC link in the Description text area.
   d. Choose a network load balancer from the Target NLB drop-down list.
   e. Choose Create to start creating the VPC link.
   You must have the network load balancer already created in the region you chose for the network load balancer to be present in the list.
3. Choose APIs from the primary navigation pane and then choose + Create API to create a new API of either an edge-optimized or regional endpoint type.
4. For the root resource (/), choose Create Method from the Actions drop-down menu, and then choose GET.
5. In the / GET - Setup pane, initialize the API method integration as follows:
   a. Choose VPC Link for Integration type.
   b. Choose Use Proxy Integration.
   c. From the Method drop-down list, choose GET as the integration method.
d. From the **VPC Link** drop-down list, choose [Use Stage Variables] and type

```
${stageVariables.vpcLinkId}
```

in the text box below.

We will define the `vpcLinkId` stage variable after deploying the API to a stage and set its value to the ID of the VpcLink created in **Step 1**.

e. Type a URL, for example, `http://myApi.example.com`, for **Endpoint URL**.

Here, the host name (for example, `myApi.example.com`) is used to set the `Host` header of the integration request.

**Note**

For the network load balancer (NLB), be sure to use the NLB DNS name as described in

Getting Started with Network Load Balancers.

f. Leave the **Use Default Timeout** selection as-is, unless you want to customize the integration timeouts.

g. Choose **Save** to finish setting up the integration.

With the proxy integration, the API is ready for deployment. Otherwise, you need to proceed to set up appropriate method responses and integration responses.

h. From the **Actions** drop-down menu, choose **Deploy API** and then choose a new or existing stage to deploy the API.

**Note** the resulting **Invoke URL**. You need it to invoke the API. Before doing that, you must set up the `vpcLinkId` stage variable.

i. In the **Stage Editor**, choose the **Stage Variables** tab and choose **Add Stage Variable**.

i. Under the **Name** column, type `vpcLinkId`.

ii. Under the **Value** column, type the ID of `VPC_LINK`, for example, `gix6s7`.

iii. Choose the check-mark icon to save this stage variable.

Using the stage variable, you can easily switch to different VPC links for the API by changing the stage variable value.

This completes creating the API. You can test invoking the API as with other integrations.

---

**TUTORIAL: Build an API Gateway API with AWS Integration**

Both the **TUTORIAL: Build a Hello World API with Lambda Proxy Integration (p. 26)** and **Build an API Gateway API with Lambda Integration (p. 26)** topics describe how to create an API Gateway API to expose the integrated Lambda function. In addition, you can create an API Gateway API to expose other AWS services, such as Amazon SNS, Amazon S3, Amazon Kinesis, and even AWS Lambda. This is made possible by the **AWS** integration. The Lambda integration or the Lambda proxy integration is a special case, where the Lambda function invocation is exposed through the API Gateway API.

All AWS services support dedicated APIs to expose their features. However, the application protocols or programming interfaces are likely to differ from service to service. An API Gateway API with the **AWS** integration has the advantage of providing a consistent application protocol for your client to access different AWS services.

In this walkthrough, we create an API to expose Amazon SNS. For more examples of integrating an API with other AWS services, see **Tutorials (p. 26)**.
Unlike the Lambda proxy integration, there is no corresponding proxy integration for other AWS services. Hence, an API method is integrated with a single AWS action. For more flexibility, similar to the proxy integration, you can set up a Lambda proxy integration. The Lambda function then parses and processes requests for other AWS actions.

API Gateway does not retry when the endpoint times out. The API caller must implement retry logic to handle endpoint timeouts.

This walkthrough builds on the instructions and concepts in Build an API Gateway API with Lambda Integration (p. 26). If you have not yet completed that walkthrough, we suggest that you do it first.

**Topics**
- Prerequisites (p. 88)
- Step 1: Create the Resource (p. 88)
- Step 2: Create the GET Method (p. 89)
- Step 3: Create the AWS Service Proxy Execution Role (p. 89)
- Step 4: Specify Method Settings and Test the Method (p. 90)
- Step 5: Deploy the API (p. 91)
- Step 6: Test the API (p. 91)
- Step 7: Clean Up (p. 92)

**Prerequisites**

Before you begin this walkthrough, do the following:

1. Complete the steps in Prerequisites: Get Ready to Build an API in API Gateway (p. 10).
2. Ensure that the IAM user has access to create policies and roles in IAM. You need to create an IAM policy and role in this walkthrough.
3. Create a new API named `MyDemoAPI`. For more information, see TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).
4. Deploy the API at least once to a stage named `test`. For more information, see Deploy the API (p. 40) in Build an API Gateway API with Lambda Integration (p. 26).
5. Complete the rest of the steps in Build an API Gateway API with Lambda Integration (p. 26).
6. Create at least one topic in Amazon Simple Notification Service (Amazon SNS). You will use the deployed API to get a list of topics in Amazon SNS that are associated with your AWS account. To learn how to create a topic in Amazon SNS, see Create a Topic. (You do not need to copy the topic ARN mentioned in step 5.)

**Step 1: Create the Resource**

In this step, you create a resource that enables the AWS service proxy to interact with the AWS service.

**To create the resource**

2. If `MyDemoAPI` is displayed, choose Resources.
3. In the Resources pane, choose the resource root, represented by a single forward slash (/), and then choose Create Resource.
4. For Resource Name, type `MyDemoAWSProxy`, and then choose Create Resource.
Step 2: Create the GET Method

In this step, you create a GET method that enables the AWS service proxy to interact with the AWS service.

To create the GET method

1. In the Resources pane, choose `/mydemoawsproxy`, and then choose Create Method.
2. For the HTTP method, choose GET, and then save your choice.

Step 3: Create the AWS Service Proxy Execution Role

In this step, you create an IAM role that your AWS service proxy uses to interact with the AWS service. We call this IAM role an AWS service proxy execution role. Without this role, API Gateway cannot interact with the AWS service. In later steps, you specify this role in the settings for the GET method you just created.

To create the AWS service proxy execution role and its policy

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose Policies.
3. Do one of the following:
   • If the Welcome to Managed Policies page appears, choose Get Started, and then choose Create Policy.
   • If a list of policies appears, choose Create Policy.
4. Next to Create Your Own Policy, choose Select.
5. For Policy Name, type a name for the policy (for example, APIGatewayAWSProxyExecPolicy).
6. For Description, type Enables API Gateway to call AWS services.
7. For Policy Document, type the following, and then choose Create Policy.

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

This policy document allows the caller to get a list of the Amazon SNS topics for the AWS account.
8. Choose Roles.
9. Choose Create Role.
10. Choose AWS Service under Select role type and then choose API Gateway.
11. Choose Next: Permissions.
12. Choose Next: Review.
13. For Role Name, type a name for the execution role (for example, APIGatewayAWSProxyExecRole), optionally type a description for this role, and then choose Create role.
14. In the Roles list, choose the role you just created. You may need to scroll down the list.
15. For the selected role, choose Attach policy.
16. Select the check box next to the policy you created earlier (for example, APIGatewayAWSProxyExecPolicy) and choose Attach policy.
17. The role you just created has the following trust relationship that enables API Gateway assume to role for any actions permitted by the attached policies:

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

For Role ARN, note of the Amazon Resource Name (ARN) for the execution role. You need it later. The ARN should look similar to: arn:aws:iam::123456789012:role/APIGatewayAWSProxyExecRole, where 123456789012 is your AWS account ID.

### Step 4: Specify Method Settings and Test the Method

In this step, you specify the settings for the GET method so that it can interact with an AWS service through an AWS service proxy. You then test the method.

**To specify settings for the GET method and then test it**

1. In the API Gateway console, in the Resources pane for the API named MyDemoAPI, in /mydemoawsproxy, choose GET.
2. In the Setup pane, for Integration type, choose Show advanced, and then choose AWS Service Proxy.
3. For AWS Region, choose the name of the AWS Region where you want to get the Amazon SNS topics.
4. For AWS Service, choose SNS.
5. For HTTP method, choose GET.
6. For Action, type ListTopics.
7. For Execution Role, type the ARN for the execution role.
8. Leave Path Override blank.
9. Choose Save.
10. In the Method Execution pane, in the Client box, choose TEST, and then choose Test. If successful, Response Body displays a response similar to the following:

```json
{
```

90
"ListTopicsResponse": {
  "ListTopicsResult": {
    "NextToken": null,
    "Topics": [
      {
        "TopicArn": "arn:aws:sns:us-east-1:80398EXAMPLE:MySNSTopic-1"
      },
      {
        "TopicArn": "arn:aws:sns:us-east-1:80398EXAMPLE:MySNSTopic-2"
      },
      ...
      {
        "TopicArn": "arn:aws:sns:us-east-1:80398EXAMPLE:MySNSTopic-N"
      }
    ],
    "ResponseMetadata": {
      "RequestId": "abc1de23-45fa-6789-b0c1-d2e345fa6b78"
    }
  }
}

**Step 5: Deploy the API**

In this step, you deploy the API so that you can call it from outside of the API Gateway console.

**To deploy the API**

1. In the **Resources** pane, choose **Deploy API**.
2. For **Deployment stage**, choose **test**.
3. For **Deployment description**, type **Calling AWS service proxy walkthrough**.
4. Choose **Deploy**.

**Step 6: Test the API**

In this step, you go outside of the API Gateway console and use your AWS service proxy to interact with the Amazon SNS service.

1. In the **Stage Editor** pane, next to **Invoke URL**, copy the URL to the clipboard. It should look like this:

   https://my-api-id.execute-api.region-id.amazonaws.com/test

2. Paste the URL into the address box of a new browser tab.
3. Append `/mydemoawsproxy` so that it looks like this:

   https://my-api-id.execute-api.region-id.amazonaws.com/test/mydemoawsproxy

Browse to the URL. Information similar to the following should be displayed:

Step 7: Clean Up

You can delete the IAM resources the AWS service proxy needs to work.

**Warning**
If you delete an IAM resource an AWS service proxy relies on, that AWS service proxy and any APIs that rely on it will no longer work. Deleting an IAM resource cannot be undone. If you want to use the IAM resource again, you must re-create it.

To delete the associated IAM resources

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the Details area, choose Roles.
3. Select APIGatewayAWSProxyExecRole, and then choose Role Actions, Delete Role. When prompted, choose Yes, Delete.
4. In the Details area, choose Policies.
5. Select APIGatewayAWSProxyExecPolicy, and then choose Policy Actions, Delete. When prompted, choose Delete.

You have reached the end of this walkthrough. For more detailed discussions about creating API as an AWS service proxy, see TUTORIAL: Create a REST API as an Amazon S3 Proxy in API Gateway (p. 111), TUTORIAL: Create a Calc REST API with Two AWS Service Integrations and and One Lambda Non-Proxy Integration (p. 92), or TUTORIAL: Create a REST API as an Amazon Kinesis Proxy in API Gateway (p. 137).

TUTORIAL: Create a Calc REST API with Two AWS Service Integrations and and One Lambda Non-Proxy Integration

The Getting Started non-proxy integration tutorial (p. 33) uses Lambda Function integration exclusively. Lambda Function integration is a special case of the AWS Service integration type that performs much of the integration setup for you, such as automatically adding the required resource-based permissions for invoking the Lambda function. Here, two of the three integrations use AWS Service integration. In this integration type, you have more control, but you'll need to manually perform tasks like creating and specifying an IAM role containing appropriate permissions.

In this tutorial, you'll create a Calc Lambda function that implements basic arithmetic operations, accepting and returning JSON-formatted input and output. Then you'll create a REST API and integrate it with the Lambda function in the following ways:

1. By exposing a GET method on the /calc resource to invoke the Lambda function, supplying the input as query string parameters. (AWS Service integration)
2. By exposing a POST method on the /calc resource to invoke the Lambda function, supplying the input in the method request payload. (AWS Service integration)
3. By exposing a GET on nested /calc/{operand1}/{operand2}/{operator} resources to invoke the Lambda function, supplying the input as path parameters. (Lambda Function integration)

In addition to trying out this tutorial, you may wish to study the OpenAPI definition file (p. 107) for the Calc API, which you can import into API Gateway by following the instructions in the section called "Import a REST API" (p. 341).
Create an AWS Account

Before you begin this tutorial, you'll need an AWS account.

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account
2. Follow the online instructions.
   - Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Create an Assumable IAM Role

In order for your API to invoke your Calc Lambda function, you'll need to have an API Gateway assumable IAM role, which is an IAM role with the following trusted relationship:

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

The role you create will need to have Lambda InvokeFunction permission. Otherwise, the API caller will receive a 500 Internal Server Error response. To give the role this permission, you'll attach the following IAM policy to it:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function"
    }
  ]
}
```
Here's how to accomplish all this:

Create an API Gateway assumable IAM role

1. Log in to the IAM console.
2. Choose Roles.
3. Choose Create Role.
4. Under Select type of trusted entity, choose AWS Service.
5. Under Choose the service that will use this role, choose Lambda.
6. Choose Next: Permissions.
7. Choose Create Policy.

A new Create Policy console window will open up. In that window, do the following:

a. In the JSON tab, replace the existing policy with the following:

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

b. Choose Review policy.

c. Under Review Policy, do the following:

   i. For Name, type a name such as lambda_execute.
   ii. Choose Create Policy.

8. In the original Create Role console window, do the following:

   a. Under Attach permissions policies, choose your lambda_execute policy from the dropdown list.

      If you don't see your policy in the list, choose the refresh button at the top of the list. (Don't refresh the browser page!)

   b. Choose Next: Tags.
   c. Choose Next: Review.

9. For the Role name, type a name such as lambda_invoke_function_assume_apigw_role.

   e. Choose Create role.

10. Choose your lambda_invoke_function_assume_apigw_role from the list of roles.

12. Replace the existing policy with the following:

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

13. Choose **Update Trust Policy**.
14. Make a note of the role ARN for the role you just created. You'll need it later.

### Create a Calc Lambda Function

Next you'll create a Lambda function using the Lambda console.

1. In the Lambda console, choose **Create function**.
2. Choose **Author from Scratch**.
3. For **Name**, type **Calc**.
4. Set the **Runtime** to **Node.js 8.10**.
5. Choose **Create function**.
6. Copy the following Lambda function and paste it into the code editor in the Lambda console.

```javascript
console.log('Loading the Calc function');
exports.handler = function(event, context, callback) {
  console.log('Received event:', JSON.stringify(event, null, 2));
  if (event.a === undefined || event.b === undefined || event.op === undefined) {
    callback("400 Invalid Input");
  }
  var res = {};
  res.a = Number(event.a);
  res.b = Number(event.b);
  res.op = event.op;
  if (isNaN(event.a) || isNaN(event.b)) {
    callback("400 Invalid Operand");
  }
  switch(event.op) {
    case "+":
    case "add":
      res.c = res.a + res.b;
      break;
    case "-":
```
7. Under Execution role, choose **Choose an existing role**.
8. Enter the role ARN for the `lambda_invoke_function_assume_apigw_role` role you created earlier.
9. Choose **Save**.

This function requires two operands (a and b) and an operator (op) from the event input parameter. The input is a JSON object of the following format:

```
{
  "a": "Number" | "String",
  "b": "Number" | "String",
  "op": "String"
}
```

This function returns the calculated result (c) and the input. For an invalid input, the function returns either the null value or the "Invalid op" string as the result. The output is of the following JSON format:

```
{
  "a": "Number",
  "b": "Number",
  "op": "String",
  "c": "Number" | "String"
}
```

You should test the function in the Lambda console before integrating it with the API in the next step.

**Test the Calc Lambda Function**

Here’s how to test your Calc function in the Lambda console:

1. In the **Saved test events** dropdown menu, choose **Configure test events**.
2. For the test event name, enter `calc2plus5`.
3. Replace the test event definition with the following:
Create a Calc API

The following procedure shows how to create an API for the Calc Lambda function you just created. In subsequent sections, you'll add resources and methods to it.

Create the Calc API

1. In the API Gateway console, choose Create API.
2. For API Name, type LambdaCalc.
3. Leave the Description blank, and leave the Endpoint Type set to Regional.
4. Choose Create API.

Integration 1: Create a GET Method with Query Parameters to Call the Lambda Function

By creating a GET method that passes query string parameters to the Lambda function, you enable the API to be invoked from a browser. This approach can be useful, especially for APIs that allow open access.

To set up the GET method with query string parameters

1. In the API Gateway console, under your LambdaCalc API’s Resources, choose /.
2. In the Actions drop-down menu, choose Create Resource.
3. For Resource Name, enter calc.
5. Choose the /calc resource you just created.
6. In the Actions drop-down menu, choose Create Method.
7. In the method drop-down menu that appears, choose GET.
8. Choose the checkmark icon to save your choice.
9. In the Set up pane:

```json
{
  "a": "2",
  "b": "5",
  "op": "+
}
```

4. Choose Save.
5. Choose Test.
6. Expand Execution result: succeeded. You should see the following:

```json
{
  "a": 2,
  "b": 5,
  "op": "+
  "c": 7
}
```
a. For **Integration type**, choose **AWS Service**.

b. For **AWS Region**, choose the region (e.g., us-west-2) where you created the Lambda function.

c. For **AWS Service**, choose **Lambda**.

d. Leave **AWS Subdomain** blank, because our Lambda function is not hosted on any AWS subdomain.

e. For **HTTP method**, choose **POST** and choose the checkmark icon to save your choice. Lambda requires that the **POST** request be used to invoke any Lambda function. This example shows that the HTTP method in a frontend method request can be different from the integration request in the backend.

f. Choose **Use path override for Action Type**. This option allows us to specify the ARN of the **Invoke** action to execute our **Calc** function.

g. Enter `/2015-03-31/functions/arn:aws:lambda:region:account-id:function:Calc/invocations` in **Path override**, where **region** is the region where you created your Lambda function and **account-id** is the account number for the AWS account.

h. For **Execution role**, enter the role ARN for the **lambda_invoke_function_assume_apigw_role** IAM role you created earlier (p. 93).

i. Leave **Content Handling** set to **Passthrough**, because this method will not deal with any binary data.

j. Leave **Use default timeout** checked.

k. Choose **Save**.

10. Choose **Method Request**.

Now you will set up query parameters for the **GET** method on `/calc` so it can receive input on behalf of the backend Lambda function.

a. Choose the pencil icon next to **Request Validator** and choose **Validate query string parameters and headers** from the drop-down menu. This setting will cause an error message to return to state the required parameters are missing if the client does not specify them. You will not get charged for the call to the backend.

b. Choose the checkmark icon to save your changes.

c. Expand the **URL Query String Parameters** section.

d. Choose **Add query string**.

e. For **Name**, type **operand1**.

f. Choose the checkmark icon to save the parameter.

g. Repeat the previous steps to create parameters named **operand2** and **operator**.

h. Check the **Required** option for each parameter to ensure that they are validated.

11. Choose **Method Execution** and then choose **Integration Request** to set up the mapping template to translate the client-supplied query strings to the integration request payload as required by the **Calc** function.

a. Expand the **Mapping Templates** section.

b. Choose **When no template matches the request Content-Type header** for **Request body passthrough**.

c. Under **Content-Type**, choose **Add mapping template**.

d. Type **application/json** and choose the checkmark icon to open the template editor.

e. Choose **Yes, secure this integration** to proceed.

f. Copy the following mapping script into the mapping template editor:

```json
{
  "a": "$input.params('operand1')",
  "b": "$input.params('operand2')",
}```
Integration 2: Create a POST Method with a JSON Payload to Call the Lambda Function

By creating a POST method with a JSON payload to call the Lambda function, you make it so that the client must provide the necessary input to the backend function in the request body. To ensure that the client uploads the correct input data, you'll enable request validation on the payload.

**To set up the POST method with a JSON payload to invoke a Lambda function**

1. Go to the API Gateway console.
2. Choose APIs.
3. Choose the LambdaCalc API you created previously.
4. Choose the /calc resource from Resources pane.
5. In the Actions menu, choose Create Method.
6. Choose POST from the method drop-down list.

This template maps the three query string parameters declared in Method Request into designated property values of the JSON object as the input to the backend Lambda function. The transformed JSON object will be included as the integration request payload.
7. Choose the checkmark icon to save your choice.
8. In the **Set up** pane:
   a. For **Integration type**, choose **AWS Service**.
   b. For **AWS Region**, choose the region (e.g., us-west-2) where you created the Lambda function.
   c. For **AWS Service**, choose Lambda.
   d. Leave **AWS Subdomain** blank, because our Lambda function is not hosted on any AWS subdomain.
   e. For **HTTP method**, choose **POST**. This example shows that the HTTP method in a frontend method request can be different from the integration request in the backend.
   f. For **Action**, choose **Use path override for Action Type**. This option allows you to specify the ARN of the Invoke action to execute your Calc function.
   g. For **Path override**, type `/2015-03-31/functions/arn:aws:lambda:region:account-id:function:Calc/invocations`, where `region` is the region where you created your Lambda function and `account-id` is the account number for the AWS account.
   h. For **Execution role**, enter the role ARN for the `lambda_invoke_function_assume_apigw_role` IAM role you created earlier (p. 93).
   i. Leave **Content Handling** set to **Passthrough**, because this method will not deal with any binary data.
   j. Leave **Use Default Timeout** checked.
   k. Choose **Save**.
9. Choose **Models** under your **LambdaCalc** API in the API Gateway console's primary navigation pane to create data models for the method's input and output:
   a. Choose **Create** in the **Models** pane. Type **Input** in **Model name**, type **application/json** in **Content type**, and copy the following schema definition into the **Model schema** box:

   ```json
   
   { 
     "type": "object", 
     "properties": { 
       "a": {"type": "number"}, 
       "b": {"type": "number"}, 
       "op": {"type": "string"} 
     }, 
     "title": "Input"
   }
   
   This model describes the input data structure and will be used to validate the incoming request body.
   
   b. Choose **Create model**.
   
   c. Choose **Create** in the **Models** pane. Type **Output** in **Model name**, type **application/json** in **Content type**, and copy the following schema definition into the **Model schema** box:

   ```json
   
   { 
     "type": "object", 
     "properties": { 
       "c": {"type": "number"} 
     }, 
     "title": "Output"
   }
   
   This model describes the data structure of the calculated output from the backend. It can be used to map the integration response data to a different model. This tutorial relies on the passthrough behavior and does not use this model.
d. Locate the API ID for your API at the top of the console screen and make a note of it. It will appear in parentheses after the API name.

e. In the Models pane, choose Create.

f. Type Result in Model name.

g. Type application/json in Content type.

h. Copy the following schema definition, where restapi-id is the REST API ID you noted earlier, into the Model schema box:

```json
{
   "type": "object",
   "properties":{
      "input":{
         "$ref": "https://apigateway.amazonaws.com/restapis/restapi-id/models/Input"
      },
      "output":{
         "$ref": "https://apigateway.amazonaws.com/restapis/restapi-id/models/Output"
      }
   },
   "title": "Output"
}
```

This model describes the data structure of the returned response data. It references both the Input and Output schemas defined in the specified API (restapi-id). Again, this model is not used in this tutorial because it leverages the passthrough behavior.

i. Choose Create model.

10. In the main navigation pane, under your LambdaCalc API, choose Resources.

11. In the Resources pane, choose the POST method for your API.

12. Choose Method Request.

13. In the Method Request configuration settings, do the following to enable request validation on the incoming request body:

   a. Choose the pencil icon next to Request Validator to choose Validate body. Choose the checkmark icon to save your choice.

   b. Expand the Request Body section, choose Add model

   c. Type application/json in the Content-Type input field and choose Input from the dropdown list in the Model name column. Choose the checkmark icon to save your choice.

14. To test your POST method, do the following:

   a. Choose Method Execution.

   b. Choose Test.

15. Copy the following JSON payload into the Request Body:

```json
{
   "a": 1,
   "b": 2,
   "op": "+
}
```

16. Choose Test.

You should see the following output in Response Body:
Integration 3: Create a GET Method with Path Parameters to Call the Lambda Function

Now you’ll create a GET method on a resource specified by a sequence of path parameters to call the backend Lambda function. The path parameter values specify the input data to the Lambda function. You’ll use a mapping template to map the incoming path parameter values to the required integration request payload.

This time you’ll use the built-in Lambda integration support in the API Gateway console to set up the method integration.

The resulting API resource structure will look like this:

To set up a GET method with URL path parameters

1. Go to the API Gateway console.
2. Under APIs, choose the LambdaCalc API you created previously.
3. In the API's Resources navigation pane, choose /calc.
4. From the Actions drop-down menu, choose Create Resource.
5. For Resource Name, type {operand1}.
6. For Resource Path, type {operand1}.
7. Choose Create Resource.
8. Choose the /calc/{operand1} resource you just created.
9. From the Actions drop-down menu, choose Create Resource.
10. For Resource Name, type {operand2}.
11. For Resource Path, type {operand2}.

```
{
    "a": 1,
    "b": 2,
    "op": "+",
    "c": 3
}
```
13. Choose the `/calc/{operand1}/{operand2}` resource you just created.
14. From the Actions drop-down menu, choose Create Resource.
15. For Resource Path, type `{operator}`.
16. For Resource Name, type `{operator}`.
17. Choose Create Resource.
18. Choose the `/calc/{operand1}/{operand2}/{operator}` resource you just created.
19. From the Actions drop-down menu, choose Create Method.
20. From the method drop-down menu, choose GET.
21. In the Setup pane, choose Lambda Function for Integration type, to use the streamlined setup process enabled by the console.
22. Choose a region (e.g., us-west-2) for Lambda Region. This is the region where the Lambda function is hosted.
23. Choose your existing Lambda function (Calc) for Lambda Function.
24. Choose Save and then choose OK to consent to Add Permissions to Lambda Function.
25. Choose Integration Request.
26. Set up the mapping template as follows:
   a. Expand the Mapping Templates section.
   b. Leave set to When no template matches the requested Content-Type header.
   c. Choose Add mapping template.
   d. Type `application/json` for Content-Type and then choose the check mark icon to open the template editor.
   e. Choose Yes, secure this integration to proceed.
   f. Copy the following mapping script into the template editor:

```
{
    "a": "$input.params('operand1')",
    "b": "$input.params('operand2')",
    "op": 
    #if($input.params('operator')=='%2F')"/"#{else}"$input.params('operator')"#end
}
```

This template maps the three URL path parameters, declared when the `/calc/{operand1}/{operand2}/{operator}` resource was created, into designated property values in the JSON object. Because URL paths must be URL-encoded, the division operator must be specified as `%2F` instead of `/`. This template translates the `%2F` into `/` before passing it to the Lambda function.

g. Choose Save.

When the method is set up correctly, the settings should look more or less like this:
27. To test your GET function, do the following:

a. Choose **Method Execution**.

b. Choose **Test**.

c. Type 1, 2 and + in the `{operand1}`, `{operand2}` and `{operator}` fields, respectively.

d. Choose **Test**.

e. The result should look like this:
This test result shows the original output from the backend Lambda function, as passed through the integration response without mapping, because there is no mapping template. Next, you'll model the data structure of the method response payload after the Result schema.

28. By default, the method response body is assigned an empty model. This will cause the integration response body to be passed through without mapping. However, when you generate an SDK for one of the strongly-type languages, such as Java or Objective-C, your SDK users will receive an empty object as the result. To ensure that both the REST client and SDK clients receive the desired result, you must model the response data using a predefined schema. Here you'll define a model for the method response body and to construct a mapping template to translate the integration response body into the method response body.

a. Choose `/calc/{operand1}/{operand2}/{operator}`.

b. Choose GET.

c. Choose Method Execution.

d. Choose Method Response.

e. Expand the 200 response,
Integration 3: Create a GET Method with Path Parameters to Call the Lambda Function

f. Under Response Body for 200, choose the pencil icon next to the model for the application/json content type.

g. From the Models drop-down list, choose Result.

h. Choose the checkmark icon to save your choice.

Setting the model for the method response body ensures that the response data will be cast into the Result object of a given SDK. To make sure that the integration response data is mapped accordingly, you'll need a mapping template.

29. To create the mapping template, do the following:

a. Choose Method Execution.

b. Choose Integration Response and expand the 200 method response entry.

c. Expand the Mapping Templates section.

d. Choose application/json from the Content-Type list.

e. Choose Result from the Generate template drop-down list to bring up the Result template blueprint.

f. Change the template blueprint to the following:

```java
#set($inputRoot = $input.path(''))
{
   "input" : {
      "a" : $inputRoot.a,
      "b" : $inputRoot.b,
      "op" : "$inputRoot.op"
   },
   "output" : {
      "c" : $inputRoot.c
   }
}
```

Choose Save.

30. To test the mapping template, do the following:

a. Choose Method Execution.

b. Choose Test.

c. Type 1 2 and + in the operand1, operand2 and operator input fields, respectively.

The integration response from the Lambda function is now mapped to a Result object.

d. Choose Test, and you'll see the following under Response Body in the console:

```java
{  
   "input": {  
      "a": 1,
      "b": 2,
      "op": "+
   },
   "output": {  
      "c": 3
   }
}
```

31. At this point the API can be called only via Test Invoke in the API Gateway console. To make it available to clients, you'll need to deploy it as follows:

a. Choose Deploy API from the Actions dropdown menu.

b. Choose [New Stage] from the Deployment Stage dropdown menu.
c. For **Stage Name**, enter **test**.
d. Choose **Deploy**.
e. Note the **Invoke URL** at the top of the console window. You can use this with tools such as Postman and cURL to test your API.

**Note**
Always be sure to redeploy your API whenever you add, modify, or delete a resource or method, update a data mapping, or update stage settings. Otherwise, new features or updates will not be available to clients of your API.

### OpenAPI Definitions of Sample API Integrated with a Lambda Function

**OpenAPI 2.0**

```json
{
  "swagger": "2.0",
  "info": {
    "version": "2017-04-20T04:08:08Z",
    "title": "LambdaCalc"
  },
  "host": "uojnr9hd57.execute-api.us-east-1.amazonaws.com",
  "basePath": "/test",
  "schemes": ["https"],
  "paths": {
    "/calc": {
      "get": {
        "consumes": [
          "application/json"
        ],
        "produces": [
          "application/json"
        ],
        "parameters": [
          {
            "name": "operand2",
            "in": "query",
            "required": true,
            "type": "string"
          },
          {
            "name": "operator",
            "in": "query",
            "required": true,
            "type": "string"
          },
          {
            "name": "operand1",
            "in": "query",
            "required": true,
            "type": "string"
          }
        ],
        "responses": {
          "200": {
            "description": "200 response",
            "schema": {
```
"$ref": "#/definitions/Result"
}

"headers": {
  "operand_1": {
    "type": "string"
  },
  "operand_2": {
    "type": "string"
  },
  "operator": {
    "type": "string"
  }
}

"x-amazon-apigateway-request-validator": "Validate query string parameters and headers",
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
  "responses": {
    "default": {
      "statusCode": "200",
      "responseParameters": {
        "method.response.header.operator": "integration.response.body.op",
        "method.response.header.operand_2": "integration.response.body.b",
        "method.response.header.operand_1": "integration.response.body.a"
      },
      "responseTemplates": {
        "application/json": "#set($res = $input.path(''))\
result": "$res.a, $res.b, $res.op => $res.c",
  "a": "$res.a",
  "b": "$res.b",
  "op": "$res.op",
  "c": "$res.c"
"
"
"passthroughBehavior": "when_no_match",
"httpMethod": "POST",
"requestTemplates": {
  "application/json": "{\n  \"a\": \"$input.params('operand1')\", \n  \"b\": \"$input.params('operand2')\", \n  \"op\": \"$input.params('operator')\"\n}\n",
  "type": "aws"
}

"post": {
  "consumes": [
    "application/json"
  ],
  "produces": [
    "application/json"
  ],
  "parameters": [
    {
      "in": "body",
      "name": "Input",
      "required": true,
      "schema": {
        "$ref": "#/definitions/Input"
      }
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "schema": {"$ref": "#/definitions/Result"}
"$ref": "/definitions/Result"
}
"
"x-amazon-apigateway-request-validator": "Validate body",
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
"default": {
"statusCode": "200",
"responseTemplates": {
"application/json": "#set($inputRoot = $input.path('$'))\n\n"a"": $inputRoot.a,\n"b": $inputRoot.b,\n"op": $inputRoot.op,\n"c": $inputRoot.c
}"
}
"passthroughBehavior": "when_no_templates",
"httpMethod": "POST",
"type": "aws"
}
",
"/calc/{operand1}/{operand2}/{operator}": {
"get": {
"consumes": ["application/json"],
"produces": ["application/json"],
"parameters": [
{"name": "operand2",
"in": "path",
"required": true,
"type": "string"},
{"name": "operator",
"in": "path",
"required": true,
"type": "string"},
{"name": "operand1",
"in": "path",
"required": true,
"type": "string"}
]
,"responses": {
"200": {
"description": "200 response",
"schema": {
"$ref": "/definitions/Result"
}
}
,"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
"default": {
"statusCode": "200",
"responseTemplates": {
"application/json": "#set($inputRoot = $input.path('$'))\n\n"a"": $inputRoot.a,\n"b": $inputRoot.b,\n"op": $inputRoot.op,\n"c": $inputRoot.c
}"
}
"passthroughBehavior": "when_no_templates",
"httpMethod": "POST",
"type": "aws"
}

109
"responseTemplates": {
  "application/json": "#set($inputRoot = $input.path('$'))\n\n\"input\": \n  \"a\": $inputRoot.a, \n  \"b\": $inputRoot.b, \n  \"op\": $inputRoot.op, \n\n\"output\": \n  \"c\": $inputRoot.c\n\n\n"},


"passthroughBehavior": "when_no_templates",

"httpMethod": "POST",

"requestTemplates": {
  "application/json": "\n  \"a\": 
    $input.params('operand1'), \n  \"b\": 
    $input.params('operand2'), \n  \"op\": 
    #if($input.params('operator')=='%2F')"/\n    \"#end\n    \"#end\n    \n  \n    
  \n    
  \n    
  \n"},

"contentHandling": "CONVERT_TO_TEXT",

"type": "aws"},

"definitions": {
  "Input": {
    "type": "object",
    "required": ["a", "b", "op"],
    "properties": {
      "a": {
        "type": "number"
      },
      "b": {
        "type": "number"
      },
      "op": {
        "type": "string",
        "description": "binary op of ['+', 'add', '-', 'sub', '*', 'mul', '%2F', 'div']"
      }
    }
  },

  "title": "Input"},

  "Output": {
    "type": "object",
    "properties": {
      "c": {
        "type": "number"
      }
    }
  },

  "title": "Output"},

  "Result": {
    "type": "object",
    "properties": {
      "input": {
        "$ref": "/definitions/Input"
      },
      "output": {
        "$ref": "/definitions/Output"
      }
    }
  },

  "title": "Result"}
TUTORIAL: Create a REST API as an Amazon S3 Proxy in API Gateway

As an example to showcase using a REST API in API Gateway to proxy Amazon S3, this section describes how to create and configure a REST API to expose the following Amazon S3 operations:

- Expose GET on the API's root resource to list all of the Amazon S3 buckets of a caller.
- Expose GET on a Folder resource to view a list of all of the objects in an Amazon S3 bucket.
- Expose PUT on a Folder resource to add a bucket to Amazon S3.
- Expose DELETE on a Folder resource to remove a bucket from Amazon S3.
- Expose GET on a Folder/Item resource to view or download an object from an Amazon S3 bucket.
- Expose PUT on a Folder/Item resource to upload an object to an Amazon S3 bucket.
- Expose HEAD on a Folder/Item resource to get object metadata in an Amazon S3 bucket.
- Expose DELETE on a Folder/Item resource to remove an object from an Amazon S3 bucket.

**Note**

To integrate your API Gateway API with Amazon S3, you must choose a region where both the API Gateway and Amazon S3 services are available. For region availability, see Regions and Endpoints.

You may want to import the sample API as an Amazon S3 proxy, as shown in OpenAPI Definitions of the Sample API as an Amazon S3 Proxy (p. 128). For instructions on how to import an API using the OpenAPI definition, see Import a REST API into API Gateway (p. 341).

To use the API Gateway console to create the API, you must first sign up for an AWS account.

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

**Topics**

- Set Up IAM Permissions for the API to Invoke Amazon S3 Actions (p. 112)
Set Up IAM Permissions for the API to Invoke Amazon S3 Actions

To allow the API to invoke required Amazon S3 actions, you must have appropriate IAM policies attached to an IAM role. The next section describes how to verify and to create, if necessary, the required IAM role and policies.

For your API to view or list Amazon S3 buckets and objects, you can use the IAM-provided AmazonS3ReadOnlyAccess policy in the IAM role. The ARN of this policy is arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess, which is as shown as follows:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:Get*", "s3:List*"],
      "Resource": "*"
    }
  ]
}
```

This policy document states that any of the Amazon S3 Get* and List* actions can be invoked on any of the Amazon S3 resources.

For your API to update Amazon S3 buckets and objects, you can use a custom policy for any of the Amazon S3 Put* actions as shown as follows:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:Put*",
      "Resource": "*"
    }
  ]
}
```

For your API to work with Amazon S3 Get*, List* and Put* actions, you can add the above read-only and put-only policies to the IAM role.

For your API to invoke the Amazon S3 Post* actions, you must use an Allow policy for the s3:Post* actions in the IAM role. For a complete list of Amazon S3 actions, see Specifying Amazon S3 Permissions in a Policy.
For your API to create, view, update, and delete buckets and objects in Amazon S3, you can use the IAM-provided AmazonS3FullAccess policy in the IAM role. The ARN is `arn:aws:iam::aws:policy/AmazonS3FullAccess`.

The desired IAM policies to use, create an IAM role and attach to it the policies. The resulting IAM role must contain the following trust policy for API Gateway to assume this role at runtime.

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

When using the IAM console to create the role, choose the **Amazon API Gateway** role type to ensure that this trust policy is automatically included.

## Create API Resources to Represent Amazon S3 Resources

We will use the API's root (`/`) resource as the container of an authenticated caller's Amazon S3 buckets. We will also create a `Folder` and `Item` resources to represent a particular Amazon S3 bucket and a particular Amazon S3 object, respectively. The folder name and object key will be specified, in the form of path parameters as part of a request URL, by the caller.

**Note**

When accessing objects whose object key includes `/` or any other special character, the character needs to be URL encoded. For example, `test/test.txt` should be encoded to `test%2Ftest.txt`.

**To create an API resource that exposes the Amazon S3 service features**

1. In the API Gateway console, create an API named **MyS3**. This API's root resource (`/`) represents the Amazon S3 service.
2. Under the API's root resource, create a child resource named **Folder** and set the required **Resource Path** as `/{folder}`.
3. For the API's **Folder** resource, create an **Item** child resource. Set the required **Resource Path** as `/{item}`.
Expose an API Method to List the Caller's Amazon S3 Buckets

Getting the list of Amazon S3 buckets of the caller involves invoking the GET Service action on Amazon S3. On the API's root resource, (/), create the GET method. Configure the GET method to integrate with the Amazon S3, as follows.

To create and initialize the API's GET / method

1. Choose Create method on the root node (/) from the Actions drop-down menu at the top-right corner of the Resources panel.
2. Choose the GET from the drop-down list of HTTP verbs, and choose the check-mark icon to start creating the method.
3. In the / - GET - Setup pane, choose AWS Service for Integration type.
4. From the list, choose a region (e.g., us-west-2) for AWS Region.
5. From AWS Service, choose S3.
6. For AWS Subdomain, leave it blank.
7. From HTTP method, choose GET.
8. For **Action Type**, choose **Use path override**. With path override, API Gateway forwards the client request to Amazon S3 as the corresponding Amazon S3 REST API path-style request, in which a Amazon S3 resource is expressed by the resource path of the `s3-host-name/bucket/key` pattern. API Gateway sets the `s3-host-name` and passes the client specified bucket and key from the client to Amazon S3.

9. (Optional) In **Path override type** `/`.

10. Copy the previously created IAM role's ARN (from the IAM console) and paste it into **Execution role**.

11. Leave any other settings as default.

12. Choose **Save** to finish setting up this method.

This setup integrates the frontend GET `https://your-api-host/stage/` request with the backend GET `https://your-s3-host/`.

**Note**
After the initial setup, you can modify these settings in the **Integration Request** page of the method.

To control who can call this method of our API, we turn on the method authorization flag and set it to **AWS_IAM**.

**To enable IAM to control access to the GET / method**

1. From the **Method Execution**, choose **Method Request**.
2. Choose the pencil icon next to **Authorization**
3. Choose **AWS_IAM** from the drop-down list.
4. Choose the check-mark icon to save the setting.

For our API to return successful responses and exceptions properly to the caller, let us declare the 200, 400 and 500 responses in **Method Response**. We use the default mapping for 200 responses so that backend responses of the status code not declared here will be returned to the caller as 200 ones.

**To declare response types for the GET / method**

1. From the **Method Execution** pane, choose the **Method Response** box. The API Gateway declares the 200 response by default.
2. Choose **Add response**, enter **400** in the input text box, and choose the check-mark to finish the declaration.

3. Repeat the above step to declare the 500 response type. The final setting is shown as follows:

Because the successful integration response from Amazon S3 returns the bucket list as an XML payload and the default method response from API Gateway returns a JSON payload, we must map the backend Content-Type header parameter value to the frontend counterpart. Otherwise, the client will receive `application/json` for the content type when the response body is actually an XML string. The following procedure shows how to set this up. In addition, we also want to display to the client other header parameters, such as Date and Content-Length.

**To set up response header mappings for the GET / method**

1. In the API Gateway console, choose **Method Response**. Add the **Content-Type** header for the 200 response type.
2. In Integration Response, for Content-Type, type integration.response.header.Content-Type for the method response.
With the above header mappings, API Gateway will translate the `Date` header from the backend to the `Timestamp` header for the client.

3. Still in **Integration Response**, choose **Add integration response**, type an appropriate regular expression in the **HTTP status regex** text box for a remaining method response status. Repeat until all the method response status are covered.
As a good practice, let us test our API we have configured so far.

**Test the GET method on the API root resource**

1. Go back to Method Execution, choose Test from the Client box.
2. Choose Test in the GET / - Method Test pane. An example result is shown as follows.
Note
To use the API Gateway console to test the API as an Amazon S3 proxy, make sure that the targeted S3 bucket is from a different region from the API’s region. Otherwise, you may get a 500 Internal Server Error response. This limitation does not apply to any deployed API.

Expose API Methods to Access an Amazon S3 Bucket

To work with an Amazon S3 bucket, we expose the GET, PUT, and DELETE methods on the /{folder} resource to list objects in a bucket, create a new bucket, and delete an existing bucket. The instructions are similar to those described in Expose an API Method to List the Caller’s Amazon S3 Buckets (p. 114). In the following discussions, we outline the general tasks and highlight relevant differences.

To expose GET, PUT and DELETE methods on a folder resource

1. On the /{folder} node from the Resources tree, create the DELETE, GET and PUT methods, one at a time.

2. Set up the initial integration of each created method with its corresponding Amazon S3 endpoints. The following screen shot illustrates this setting for the PUT /{folder} method. For the
DELETE /{folder} and GET /{folder} method, replace the PUT value of HTTP method by DELETE and GET, respectively.

Notice that we used the {bucket} path parameter in the Amazon S3 endpoint URLs to specify the bucket. We will need to map the {folder} path parameter of the method requests to the {bucket} path parameter of the integration requests.

3. To map {folder} to {bucket}:
   a. Choose Method Execution and then Integration Request.
   b. Expand URL Path Parameters and choose Add path
   c. Type bucket in the Name column and method.request.path.folder in the Mapped from column. Choose the check-mark icon to save the mapping.

4. In Method Request, add the Content-Type to the HTTP Request Headers section.
This is mostly needed for testing, when using the API Gateway console, when you must specify application/xml for an XML payload.

5. In Integration Request, set up the following header mappings, following the instructions described in Expose an API Method to List the Caller's Amazon S3 Buckets (p. 114).

The x-amz-acl header is for specifying access control on the folder (or the corresponding Amazon S3 bucket). For more information, see Amazon S3 PUT Bucket Request.

6. To test the PUT method, choose Test in the Client box from Method Execution, and enter the following as input to the testing:

a. In folder, type a bucket name,

b. For the Content-Type header, type application/xml.

c. In Request Body, provide the bucket region as the location constraint, declared in an XML fragment as the request payload. For example,

```xml
<CreateBucketConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <LocationConstraint>{region}</LocationConstraint>
</CreateBucketConfiguration>
```
7. Repeat the preceding steps to create and configure the GET and DELETE method on the API's /{folder} resource.

The above examples illustrate how to create a new bucket in the specified region, to view the list of objects in the bucket, and to delete the bucket. Other Amazon S3 bucket operations allow you work with the metadata or properties of the bucket. For example, you can set up your API to call the Amazon S3's PUT /?notification action to set up notifications on the bucket, to call PUT /?acl to set an access control list on the bucket, etc. The API set up is similar, except for that you must append appropriate query parameters to the Amazon S3 endpoint URLs. At run time, you must provide the appropriate XML payload to the method request. The same can be said about supporting the other GET and DELETE operations on a Amazon S3 bucket. For more information on possible &S3; actions on a bucket, see Amazon S3 Operations on Buckets.

**Expose API Methods to Access an Amazon S3 Object in a Bucket**

Amazon S3 supports GET, DELETE, HEAD, OPTIONS, POST and PUT actions to access and manage objects in a given bucket. For the complete list of supported actions, see Amazon S3 Operations on Objects.

In this tutorial, we expose the PUT Object operation, the GET Object operation, HEAD Object operation, and the DELETE Object operation through the API methods of PUT /{folder}/{item}, GET /{folder}/{item}, HEAD /{folder}/{item} and DELETE /{folder}/{item}, respectively.

The API setups for the PUT, GET and DELETE methods on /{folder}/{item} are the similar to those on /{folder}, as prescribed in Expose API Methods to Access an Amazon S3 Bucket (p. 120). One major difference is that the object-related request path has an additional path parameter of {item} and this path parameter must be mapped to the integration request path parameter of {object}. 
The same is true for the GET and DELETE methods.

As an illustration, the following screen shot shows the output when testing the GET method on a `{folder}/{item}` resource using the API Gateway console. The request correctly returns the plain text of ("Welcome to README.txt") as the content of the specified file (README.txt) in the given Amazon S3 bucket (apig-demo).
To download or upload binary files, which in API Gateway is considered anything other than utf-8 encoded JSON content, additional API settings are necessary. This is outlined as follows:

**To download or upload binary files from S3**

1. Register the media types of the affected file to the API's binaryMediaTypes. You can do this in the console:
   a. Choose **Binary Support** for the API (from the API Gateway primary navigation panel),
   b. Choose **Edit**.
   c. Type the required media type (e.g., `image/png` for **Binary media types**).
   d. Choose **Add binary media type** to save the setting.
2. Add the **Content-Type** (for upload) and/or **Accept** (for download) header to the method request to require the client to specify the required binary media type and map them to the integration request.
3. **Set Content Handling** to **Passthrough** in the integration request (for upload) and in a integration response (for download). Make sure that no mapping template is defined for the affected content type. For more information, see Integration Passthrough Behaviors (p. 292) and Select VTL Mapping Templates (p. 291).
Call the API Using a REST API Client

To provide an end-to-end tutorial, we now show how to call the API using Postman, which supports the AWS IAM authorization.

To call our Amazon S3 proxy API using Postman

1. Deploy or redeploy the API. Make a note of the base URL of the API that is displayed next to Invoke URL at the top of the Stage Editor.
2. Launch Postman.
3. Choose Authorization and then choose AWS Signature. Type your IAM user's Access Key ID and Secret Access Key into the AccessKey and SecretKey input fields, respectively. Type the AWS region to which your API is deployed in the AWS Region text box. Type execute-api in the Service Name input field.

You can create a pair of the keys from the Security Credentials tab from your IAM user account in the IAM Management Console.

4. To add a bucket named apig-demo-5 to your Amazon S3 account in the {region} region:
   a. Choose PUT from the drop-down method list and type the method URL (https://api-id.execute-api.aws-region.amazonaws.com/stage/folder-name)
   b. Set the Content-Type header value as application/xml. You may need to delete any existing headers before setting the content type.
   c. Choose Body menu item and type the following XML fragment as the request body:

   ```xml
   <CreateBucketConfiguration>
   <LocationConstraint>{region}</LocationConstraint>
   </CreateBucketConfiguration>
   ```
   d. Choose Send to submit the request. If successful, you should receive a 200 OK response with an empty payload.

5. To add a text file to a bucket, follow the instructions above. If you specify a bucket name of apig-demo-5 for {folder} and a file name of Readme.txt for {item} in the URL and provide a text string of Hello, World! as the file contents (thereby making it the request payload), the request becomes

   PUT /S3/apig-demo-5/Readme.txt HTTP/1.1
   Host: 9gn28ca086.execute-api.{region}.amazonaws.com
   Content-Type: application/xml
   X-Amz-Date: 20161015T062647Z
   Authorization: AWS4-HMAC-SHA256 Credential=access-key-id/20161015/{region}/execute-api/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
   Signature=ccadb877bd0b395ca38cc57e18a0d76b5ebaf17007a1e40bf6f63d28c705b
Hello, World!

If everything goes well, you should receive a **200 OK** response with an empty payload.

6. To get the content of the Readme.txt file we just added to the **apig-demo-5** bucket, do a GET request like the following one:

```plaintext
GET /S3/apig-demo-5/Readme.txt HTTP/1.1
Host: 9gn28ca086.execute-api.{region}.amazonaws.com
Content-Type: application/xml
X-Amz-Date: 20161015T063759Z
Authorization: AWS4-HMAC-SHA256 Credential=access-key-id/20161015/{region}/execute-api/aws4_request, SignedHeaders=content-type;host;x-amz-date,
Signature=ba09b72b585acf0e578e6ad02555c00e24b420b59025bc7bb8d3f7aed1471339
Cache-Control: no-cache
Postman-Token: d60fcb59-d335-52f7-0025-5bd96928098a
```

If successful, you should receive a **200 OK** response with the **Hello, World!** text string as the payload.

7. To list items in the **apig-demo-5** bucket, submit the following request:

```plaintext
GET /S3/apig-demo-5 HTTP/1.1
Host: 9gn28ca086.execute-api.{region}.amazonaws.com
Content-Type: application/xml
X-Amz-Date: 20161015T064324Z
Authorization: AWS4-HMAC-SHA256 Credential=access-key-id/20161015/{region}/execute-api/aws4_request, SignedHeaders=content-type;host;x-amz-date,
Signature=4ac9bd4574a1e01568134fd16814534d9951649d3a22b3b0db9f1f5cd4dd0ac
Cache-Control: no-cache
Postman-Token: 9c43020a-966f-61e1-81af-4c49ad8d1392
```

If successful, you should receive a **200 OK** response with an XML payload showing a single item in the specified bucket, unless you added more files to the bucket before submitting this request.

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <Name>apig-demo-5</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Readme.txt</Key>
    <LastModified>2016-10-15T06:48:00Z</LastModified>
    <ETag>"65a8e27d8879283831b664bd8b7f0ad4"</ETag>
    <Size>13</Size>
    <Owner>
      <ID>06e4b09e9d...603add12ee</ID>
      <DisplayName>user-name</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

**Note**

To upload or download an image, you need to set content handling to `CONVERT_TO_BINARY`. 
OpenAPI Definitions of the Sample API as an Amazon S3 Proxy

The following OpenAPI definitions describe the sample API, referenced in this tutorial, as an Amazon S3 proxy.

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "version": "2016-10-13T23:04:43Z",
    "title": "MyS3"
  },
  "host": "9gn28ca086.execute-api.{region}.amazonaws.com",
  "basePath": "/S3",
  "schemes": ["https"],
  "paths": {
    "": {
      "get": {
        "produces": ["application/json"],
        "responses": {
          "200": {
            "description": "200 response",
            "schema": {
              "$ref": "#/definitions/Empty"
            },
            "headers": {
              "Content-Length": {
                "type": "string"
              },
              "Timestamp": {
                "type": "string"
              },
              "Content-Type": {
                "type": "string"
              }
            }
          },
          "400": {
            "description": "400 response"
          },
          "500": {
            "description": "500 response"
          }
        },
        "security": [
          { "sigv4": [] }
        ],
        "x-amazon-apigateway-integration": {
          "credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
          "responses": {
            "4\d(2)": {
              "statusCode": "400"
            }
          }
        }
      }
    }
  }
}
```
"default": {
  "statusCode": "200",
  "responseParameters": {
    "method.response.header.Content-Type": "integration.response.header.Content-Type",
    "method.response.header.Timestamp": "integration.response.header.Date"
  },
  "5\d{2}": {
    "statusCode": "500"
  },
  "uri": "arn:aws:apigateway:us-west-2:s3:path/",
  "passthroughBehavior": "when_no_match",
  "httpMethod": "GET",
  "type": "aws"
},
"/{folder}\": {
  "get": {
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "folder",
        "in": "path",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "schema": {
          "$ref": "#/definitions/Empty"
        },
        "headers": {
          "Content-Length": {
            "type": "string"
          },
          "Date": {
            "type": "string"
          },
          "Content-Type": {
            "type": "string"
          }
        }
      },
      "400": {
        "description": "400 response"
      },
      "500": {
        "description": "500 response"
      }
    },
    "security": [
      {
        "sigv4": []
      }
    ],
    "x-amazon-apigateway-integration": {
      "integrations": {
        "default": {
          "requestTemplates": {
          },
          "responses": {
            "200": {
              "statusCode": "200",
              "responseParameters": {
                "method.response.header.Content-Type": "integration.response.header.Content-Type",
                "method.response.header.Timestamp": "integration.response.header.Date"
              }
            }
          }
        }
      }
    }
  }
}
"credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
"responses": {
  "4\d{2}": {
    "statusCode": "400"
  },
  "default": {
    "statusCode": "200",
    "responseParameters": {
      "method.response.header.Content-Type": "integration.response.header.Content-Type",
      "method.response.header.Date": "integration.response.header.Date",
      "method.response.header.Content-Length": "integration.response.header.content-length"
    }
  },
  "5\d{2}": {
    "statusCode": "500"
  }
},
"requestParameters": {
  "integration.request.path.bucket": "method.request.path.folder"
},
"uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}",
"passthroughBehavior": "when_no_match",
"httpMethod": "GET",
"type": "aws"
},
"put": {
  "produces": [
    "application/json"
  ],
  "parameters": [
    {
      "name": "Content-Type",
      "in": "header",
      "required": false,
      "type": "string"
    },
    {
      "name": "folder",
      "in": "path",
      "required": true,
      "type": "string"
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "schema": {
        "$ref": "#/definitions/Empty"
      },
      "headers": {
        "Content-Length": {
          "type": "string"
        },
        "Content-Type": {
          "type": "string"
        }
      }
    },
    "400": {
      "description": "400 response"
    },
    "500": {
"description": "500 response"
},
"security": [
{
"sigv4": []
}
],
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
"responses": {
"4\d(2)": {
"statusCode": "400"
},
"default": {
"statusCode": "200",
"responseParameters": {
"method.response.header.Content-Type": "integration.response.header.Content-Type",
"method.response.header.Content-Length": "integration.response.header.Content-Length"
}
},
"5\d(2)": {
"statusCode": "500"
}
},
"requestParameters": {
"integration.request.header.x-amz-acl": "authenticated-read",
"integration.request.path.bucket": "method.request.path.folder",
"integration.request.header.Content-Type": "method.request.header.Content-Type"
},
"uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}",
"passthroughBehavior": "when_no_match",
"httpMethod": "PUT",
"type": "aws"
}
),
"delete": {
"produces": [
"application/json"
],
"parameters": [
{
"name": "folder",
"in": "path",
"required": true,
"type": "string"
}
],
"responses": {
"200": {
"description": "200 response",
"schema": {
"$ref": "#/definitions/Empty"
},
"headers": {
"Date": {
"type": "string"
},
"Content-Type": {
"type": "string"
}
}
}
"400": {  
  "description": "400 response"
},
"500": {  
  "description": "500 response"
}
},
"security": [
  {  
    "sigv4": [
      ]
  },
  "x-amazon-apigateway-integration": {
    "credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
    "responses": {
      "4\d{2}": {  
        "statusCode": "400"
      },
      "default": {  
        "statusCode": "200",
        "responseParameters": {  
          "method.response.header.Content-Type": "integration.response.header.Content-Type",
          "method.response.header.Date": "integration.response.header.Date"
        }
      },
      "5\d{2}": {  
        "statusCode": "500"
      }
    },
    "requestParameters": {
      "integration.request.path.bucket": "method.request.path.folder"
    },
    "uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}",
    "passthroughBehavior": "when_no_match",
    "httpMethod": "DELETE",
    "type": "aws"
  }
},
"/{folder}/{item}": {
  "get": {
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "item",
        "in": "path",
        "required": true,
        "type": "string"
      },
      {
        "name": "folder",
        "in": "path",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "schema": {
          "$ref": "#/definitions/Empty"
        }
      }
    }
  }
}
headers": {
  "content-type": {
    "type": "string"
  },
  "Content-Type": {
    "type": "string"
  }
},
"400": {
  "description": "400 response"
},
"500": {
  "description": "500 response"
},
"security": [
  {
    "sigv4": []
  }
],
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
  "responses": {
    "4\d{2}": {
      "statusCode": "400"
    },
    "default": {
      "statusCode": "200",
      "responseParameters": {
        "method.response.header.content-type":
        "integration.response.header.content-type",
        "method.response.header.Content-Type":
        "integration.response.header.ContentType"
      }
    },
    "5\d{2}": {
      "statusCode": "500"
    }
  },
  "requestParameters": {
    "integration.request.path.object": "method.request.path.item",
    "integration.request.path.bucket": "method.request.path.folder"
  },
  "uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}/{object}",
  "passthroughBehavior": "when_no_match",
  "httpMethod": "GET",
  "type": "aws"
},
"head": {
  "produces": [
    "application/json"
  ],
  "parameters": [
    {
      "name": "item",
      "in": "path",
      "required": true,
      "type": "string"
    },
    {
      "name": "folder",
      "in": "path",
      "required": true,
      "type": "string"
    }
  ]
}
"required": true,
"type": "string"
],
"responses": {
"200": {
"description": "200 response",
"schema": {
"$ref": "#/definitions/Empty"
},
"headers": {
"Content-Length": {
"type": "string"
},
"Content-Type": {
"type": "string"
}
},
"400": {
"description": "400 response"
},
"500": {
"description": "500 response"
}
},
"security": [
{
"sigv4": []
}
],
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
"responses": {
"4\d\d": {
"statusCode": "400"
},
"default": {
"statusCode": "200",
"responseParameters": {
"integration.response.header.Content-Type": "method.response.header.Content-Type",
"integration.response.header.Content-Length": "method.response.header.Content-Length"
}
},
"5\d\d": {
"statusCode": "500"
}
}
],
"requestParameters": {
"integration.request.path.object": "method.request.path.item",
"integration.request.path.bucket": "method.request.path.folder"
},
"uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}/{object}"
},
"passthroughBehavior": "when_no_match",
"httpMethod": "HEAD",
"type": "aws"
},
"put": {
"produces": [
"application/json"
],
"parameters": [
{  
  "name": "Content-Type",
  "in": "header",
  "required": false,
  "type": "string"
},
{  
  "name": "item",
  "in": "path",
  "required": true,
  "type": "string"
},
{  
  "name": "folder",
  "in": "path",
  "required": true,
  "type": "string"
}
],
"responses": {
  "200": {
    "description": "200 response",
    "schema": {
      "$ref": "#/definitions/Empty"
    },
    "headers": {
      "Content-Length": {
        "type": "string"
      },
      "Content-Type": {
        "type": "string"
      }
    }
  },
  "400": {
    "description": "400 response"
  },
  "500": {
    "description": "500 response"
  }
},
"security": [
  {
    "sigv4": []
  }
],
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
  "responses": {
    "4\d(2)": {
      "statusCode": "400"
    },
    "default": {
      "statusCode": "200",
      "responseParameters": {
        "integration.response.header.Content-Type": "method.response.header.Content-Type",
        "integration.response.header.Content-Length": "method.response.header.Content-Length"
      }
    },
    "5\d(2)": {
      "statusCode": "500"
    }
  }
},
135
"requestParameters": {
    "integration.request.path.object": "method.request.path.item",
    "integration.request.header.x-amz-acl": "authenticated-read",
    "integration.request.path.bucket": "method.request.path.folder",
    "integration.request.header.Content-Type": "method.request.header.Content-Type"
},
"uri": "arn:aws:apigateway:us-west-2:s3:path/{bucket}/{object}",
"passthroughBehavior": "when_no_match",
"httpMethod": "PUT",
"type": "aws"
},
"delete": {
    "produces": [
        "application/json"
    ],
    "parameters": [
        {
            "name": "item",
            "in": "path",
            "required": true,
            "type": "string"
        },
        {
            "name": "folder",
            "in": "path",
            "required": true,
            "type": "string"
        }
    ],
    "responses": {
        "200": {
            "description": "200 response",
            "schema": {
                "$ref": "#/definitions/Empty"
            },
            "headers": {
                "Content-Length": {
                    "type": "string"
                },
                "Content-Type": {
                    "type": "string"
                }
            }
        },
        "400": {
            "description": "400 response"
        },
        "500": {
            "description": "500 response"
        }
    },
    "security": [
        {
            "sigv4": []
        }
    ],
    "x-amazon-apigateway-integration": {
        "credentials": "arn:aws:iam::<replaceable>123456789012</replaceable>:role/apigAwsProxyRole",
        "responses": {
            "4\d(2)": {
                "statusCode": "400"
            },
            "default": {
                "statusCode": "200"
            }
        },
        "passthroughBehavior": "when_no_match",
        "httpMethod": "DELETE",
        "type": "aws"
    }
}
TUTORIAL: Create a REST API as an Amazon Kinesis Proxy in API Gateway

This page describes how to create and configure a REST API with an integration of the AWS type to access Kinesis.

**Note**
To integrate your API Gateway API with Kinesis, you must choose a region where both the API Gateway and Kinesis services are available. For region availability, see [Regions and Endpoints](#).

For the purpose of illustration, we create an example API to enable a client to do the following:

1. List the user's available streams in Kinesis
2. Create, describe, or delete a specified stream
3. Read data records from or write data records into the specified stream

To accomplish the preceding tasks, the API exposes methods on various resources to invoke the following, respectively:

1. The ListStreams action in Kinesis
2. The CreateStream, DescribeStream, or DeleteStream action
3. The GetRecords or PutRecords (including PutRecord) action in Kinesis
Specifically, we build the API as follows:

- Expose an HTTP GET method on the API's /streams resource and integrate the method with the `ListStreams` action in Kinesis to list the streams in the caller's account.
- Expose an HTTP POST method on the API's /streams/{stream-name} resource and integrate the method with the `CreateStream` action in Kinesis to create a named stream in the caller's account.
- Expose an HTTP GET method on the API's /streams/{stream-name} resource and integrate the method with the `DescribeStream` action in Kinesis to describe a named stream in the caller's account.
- Expose an HTTP DELETE method on the API's /streams/{stream-name} resource and integrate the method with the `DeleteStream` action in Kinesis to delete a stream in the caller's account.
- Expose an HTTP PUT method on the API's /streams/{stream-name}/record resource and integrate the method with the `PutRecord` action in Kinesis. This enables the client to add a single data record to the named stream.
- Expose an HTTP PUT method on the API's /streams/{stream-name}/records resource and integrate the method with the `PutRecords` action in Kinesis. This enables the client to add a list of data records to the named stream.
- Expose an HTTP GET method on the API's /streams/{stream-name}/records resource and integrate the method with the `GetRecords` action in Kinesis. This enables the client to list data records in the named stream, with a specified shard iterator. A shard iterator specifies the shard position from which to start reading data records sequentially.
- Expose an HTTP GET method on the API's /streams/{stream-name}/sharditerator resource and integrate the method with the `GetShardIterator` action in Kinesis. This helper method must be supplied to the `ListStreams` action in Kinesis.

You can apply the instructions presented here to other Kinesis actions. For the complete list of the Kinesis actions, see Amazon Kinesis API Reference.

Instead of using the API Gateway console to create the sample API, you can import the sample API into API Gateway using the API Gateway Import API. For information on how to use the Import API, see Import a REST API into API Gateway (p. 341).

If you do not have an AWS account, complete the following steps to create one.

**To sign up for an AWS account**

2. Follow the online instructions.
   
   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

**Create an IAM Role and Policy for the API to Access Kinesis**

To allow the API to invoke Kinesis actions, you must have appropriate IAM policies attached to an IAM role. This section explains how to verify and to create, if necessary, the required IAM role and policies.

To enable read-only access to Kinesis, you can use the AmazonKinesisReadOnlyAccess policy that allows the `Get*`, `List*`, and `Describe*` actions in Kinesis to be invoked.
Create an IAM Role and Policy for the API to Access Kinesis

```json
"Version": "2012-10-17",
"Statement": [

{ "Effect": "Allow",
  "Action": [ "kinesis:Get*",
              "kinesis:List*",
              "kinesis:Describe*" ],
  "Resource": "*"
}
]
```

This policy is available as an IAM-provisioned managed policy and its ARN is arn:aws:iam::aws:policy/AmazonKinesisReadOnlyAccess.

To enable read-write actions in Kinesis, you can use the AmazonKinesisFullAccess policy.

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

This policy is also available as an IAM-provisioned managed policy. Its ARN is arn:aws:iam::aws:policy/AmazonKinesisFullAccess.

After you decide which IAM policy to use, attach it to a new or existing IAM role. Make sure that the API Gateway control service (apigateway.amazonaws.com) is a trusted entity of the role and is allowed to assume the execution role (sts:AssumeRole).

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

If you create the execution role in the IAM console and choose the Amazon API Gateway role type, this trust policy is automatically attached.

Note the ARN of the execution role. You will need it when creating an API method and setting up its integration request.
Start to Create an API as a Kinesis Proxy

Use the following steps to create the API in the API Gateway console.

To create an API as an AWS service proxy for Kinesis

1. In the API Gateway console, choose Create API.
2. Choose New API.
3. In API name, type KinesisProxy. Leave the default values in the other fields.
4. Type a description in Description, if you like.
5. Choose Create API.

After the API is created, the API Gateway console displays the Resources page, which contains only the API's root (/) resource.

List Streams in Kinesis

Kinesis supports the ListStreams action with the following REST API call:

```
POST /?Action=ListStreams HTTP/1.1
Host: kinesis.<region>.<domain>
Content-Length: <PayloadSizeBytes>
User-Agent: <UserAgentString>
Content-Type: application/x-amz-json-1.1
Authorization: <AuthParams>
X-Amz-Date: <Date>
{
  ...
}
```

In the above REST API request, the action is specified in the Action query parameter. Alternatively, you can specify the action in a X-Amz-Target header, instead:

```
POST / HTTP/1.1
Host: kinesis.<region>.<domain>
Content-Length: <PayloadSizeBytes>
User-Agent: <UserAgentString>
Content-Type: application/x-amz-json-1.1
Authorization: <AuthParams>
X-Amz-Date: <Date>
X-Amz-Target: Kinesis_20131202.ListStreams
{
  ...
}
```

In this tutorial, we use the query parameter to specify action.

To expose a Kinesis action in the API, add a /streams resource to the API's root. Then set a GET method on the resource and integrate the method with the ListStreams action of Kinesis.

The following procedure describes how to list Kinesis streams by using the API Gateway console.

To list Kinesis streams by using the API Gateway console

In **Resource Name**, type Streams, leave **Resource Path** and other fields as the default, and choose **Create Resource**.

2. Choose the /Streams resource. From **Actions**, choose **Create Method**, choose **GET** from the list, and then choose the check mark icon to finish creating the method.

    **Note**
    The HTTP verb for a method invoked by a client may differ from the HTTP verb for an integration required by the backend. We chose GET here, because listing streams is intuitively a READ operation.

3. In the method's **Setup** pane, choose **AWS Service**.
   a. For **AWS Region**, choose a region (e.g., **us-east-1**).
   b. For **AWS Service**, choose **Kinesis**.
   c. Leave **AWS Subdomain** blank.
   d. For **HTTP method**, choose **POST**.

    **Note**
    We chose POST here because Kinesis requires that the ListStreams action be invoked with it.

   e. For **Action Type**, choose **Use action name**.
   f. For **Action**, type **ListStreams**.
   g. For **Execution role**, type the ARN for your execution role.
   h. Leave the default of **Passthrough** for **Content Handling**.
   i. Choose **Save** to finish the initial setup of the method.
4. Still in the Integration Request pane, expand the HTTP Headers section:
   a. Choose Add header.
   b. In the Name column, type Content-Type.
   c. In the Mapped from column, type 'application/x-amz-json-1.1'.
   d. Choose the check mark icon to save the setting.

   We used a request parameter mapping to set the Content-Type header to the static value of 'application/x-amz-json-1.1' to inform Kinesis that the input is of a specific version of JSON.

5. Expand the Body Mapping Templates section:
   a. Choose Add mapping template.
   b. For Content-Type, type application/json.
   c. Choose the check mark icon to save the Content-Type setting. Choose Yes, secure this integration in Change passthrough behavior.
d. Type {} in the template editor.
e. Choose the Save button to save the mapping template.

The ListStreams request takes a payload of the following JSON format:

```
{
   "ExclusiveStartStreamName": "string",
   "Limit": number
}
```

However, the properties are optional. To use the default values, we opted for an empty JSON payload here.
6. Test the GET method on the Streams resource to invoke the ListStreams action in Kinesis:

From the API Gateway console, select the /streams.GET entry from the Resources pane, choose the Test invocation option, and then choose Test.
If you already created two streams named "myStream" and "yourStream" in Kinesis, the successful test returns a 200 OK response containing the following payload:

```json
{
    "HasMoreStreams": false,
    "StreamNames": [
        "myStream",
        "yourStream"
    ]
}
```

## Create, Describe, and Delete a Stream in Kinesis

Creating, describing, and deleting a stream in Kinesis involves making the following Kinesis REST API requests, respectively:

**POST /?Action=CreateStream HTTP/1.1**
Host: kinesis.region.domain

```plaintext
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes

{
    "ShardCount": number,
    "StreamName": "string"
}
```

**POST /?Action=DescribeStream HTTP/1.1**
Host: kinesis.region.domain

```plaintext
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes

{
    "ExclusiveStartShardId": "string",
    "Limit": number,
    "StreamName": "string"
}
```

**POST /?Action=DeleteStream HTTP/1.1**
Host: kinesis.region.domain

```plaintext
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes

{
    "StreamName": "string"
}
```
We can build the API to accept the required input as a JSON payload of the method request and pass the payload through to the integration request. However, to provide more examples of data mapping between method and integration requests, and method and integration responses, we create our API somewhat differently.

We expose the GET, POST, and Delete HTTP methods on a to-be-named Stream resource. We use the \{stream-name\} path variable as the placeholder of the stream resource and integrate these API methods with the Kinesis' DescribeStream, CreateStream, and DeleteStream actions, respectively. We require that the client pass other input data as headers, query parameters, or the payload of a method request. We provide mapping templates to transform the data to the required integration request payload.

**To configure and test the GET method on a stream resource**

1. Create a child resource with the \{stream-name\} path variable under the previously created /streams resource.

   ![New Child Resource](image)

   * Required

2. Add the POST, GET, and DELETE HTTP verbs to this resource.

   After the methods are created on the resource, the structure of the API looks like the following:
3. Set up the GET /streams/{stream-name} method to call the POST /?Action=DescribeStream action in Kinesis, as shown in the following.
4. Add the following `Content-Type` header mapping to the integration request:

```
Content-Type: 'x-amz-json-1.1'
```

The task follows the same procedure to set up the request parameter mapping for the `GET` `/streams` method.

5. Add the following body mapping template to map data from the `GET /streams/{stream-name}` method request to the `POST /?Action=DescribeStream` integration request:

```
{
    "StreamName": "$input.params('stream-name')"
}
```

This mapping template generates the required integration request payload for the `DescribeStream` action of Kinesis from the method request's `stream-name` path parameter value.

6. Test the `GET /stream/{stream-name}` method to invoke the `DescribeStream` action in Kinesis:

   From the API Gateway console, select `/streams/{stream-name}/GET` in the Resources pane, choose Test to start testing, type the name of an existing Kinesis stream in the Path field for stream-name,
and choose **Test**. If the test is successful, a 200 OK response is returned with a payload similar to the following:

```json
{
    "StreamDescription": {
        "HasMoreShards": false,
        "RetentionPeriodHours": 24,
        "Shards": [
            {
                "HashKeyRange": {
                    "EndingHashKey": "68056473384187692692674921486353642290",
                    "StartingHashKey": "0"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber": "49559266461454070523309915164834022007924120923395850242"
                },
                "ShardId": "shardId-000000000000"
            },
            ...
            {
                "HashKeyRange": {
                    "EndingHashKey": "34028236692093846346374607431768211455",
                    "StartingHashKey": "2722258935367507707070699685945414569164"
                },
                "SequenceNumberRange": {
                    "StartingSequenceNumber": "49559266461543273504104037657400164881014714369419771970"
                },
                "ShardId": "shardId-000000000004"
            }
        ],
        "StreamName": "myStream",
        "StreamStatus": "ACTIVE"
    }
}
```

After you deploy the API, you can make a REST request against this API method:

```
GET https://your-api-id.execute-api.region.amazonaws.com/stage/streams/myStream
HTTP/1.1
Host: your-api-id.execute-api.region.amazonaws.com
Content-Type: application/json
Authorization: ...
X-Amz-Date: 20160323T194451Z
```

**To configure and test the POST method on a stream resource**

1. Set up the POST /streams/{stream-name} method to call POST /?Action=CreateStream action in Kinesis. The task follows the same procedure to set up the GET /streams/{stream-name} method provided that you replace the DescribeStream action by CreateStream.

2. Add the following **Content-Type** header mapping to the integration request:

```
Content-Type: 'x-amz-json-1.1'
```
The task follows the same procedure to set up the request parameter mapping for the GET / streams method.

3. Add the following body mapping template to map data from the POST /streams/{stream-name} method request to the POST /?Action=CreateStream integration request:

```json
{
    "ShardCount": #if($input.path('$.ShardCount') == '') 5 #else $input.path('$.ShardCount') #end,
    "StreamName": "$input.params('stream-name')"
}
```

In the preceding mapping template, we set ShardCount to a fixed value of 5 if the client does not specify a value in the method request payload.

4. Test the POST /streams/{stream-name} method to create a named stream in Kinesis:

From the API Gateway console, select /streams/{stream-name}/POST in the Resources pane, choose Test to start testing, type the name of an existing Kinesis stream in Path for stream-name, and choose Test. If the test is successful, a 200 OK response is returned with no data.

After you deploy the API, you can also make a REST API request against the POST method on a Stream resource to invoke the CreateStream action in Kinesis:

```plaintext
POST https://your-api-id.execute-api.region.amazonaws.com/stage/streams/yourStream
HTTP/1.1
Host: your-api-id.execute-api.region.amazonaws.com
Content-Type: application/json
Authorization: ...
X-Amz-Date: 20160323T194451Z
{
    "ShardCount": 5
}
```

Configure and test the DELETE method on a stream resource

1. Set up the DELETE /streams/{stream-name} method to integrate with the POST /? Action=DeleteStream action in Kinesis. The task follows the same procedure to set up the GET / streams/{stream-name} method provided that you replace the DescribeStream action by DeleteStream.

2. Add the following Content-Type header mapping to the integration request:

   ```text
   Content-Type: 'x-amz-json-1.1'
   ```

   The task follows the same procedure to set up the request parameter mapping for the GET / streams method.

3. Add the following body mapping template to map data from the DELETE /streams/ {stream-name} method request to the corresponding integration request of POST /? Action=DeleteStream:

   ```json
   {
    "StreamName": "$input.params('stream-name')"
   }
   ```
This mapping template generates the required input for the DELETE /streams/{stream-name} action from the client-supplied URL path name of stream-name.

4. Test the DELETE method to delete a named stream in Kinesis:

From the API Gateway console, select the /streams/{stream-name}/DELETE method node in the Resources pane, choose Test to start testing, type the name of an existing Kinesis stream in Path for stream-name, and choose Test. If the test is successful, a 200 OK response is returned with no data.

After you deploy the API, you can also make the following REST API request against the DELETE method on the Stream resource to call the DeleteStream action in Kinesis:

```
DELETE https://your-api-id.execute-api.region.amazonaws.com/stage/streams/yourStream
HTTP/1.1
Host: your-api-id.execute-api.region.amazonaws.com
Content-Type: application/json
Authorization: ...
X-Amz-Date: 20160323T194451Z
{
}
```

Get Records from and Add Records to a Stream in Kinesis

After you create a stream in Kinesis, you can add data records to the stream and read the data from the stream. Adding data records involves calling the PutRecords or PutRecord action in Kinesis. The former adds multiple records whereas the latter adds a single record to the stream.

```
POST /?Action=PutRecords HTTP/1.1
Host: kinesis.region.domain
Authorization: AWS4-HMAC-SHA256 Credential=..., ...
...
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes
{
  "Records": [
    {
      "Data": blob,
      "ExplicitHashKey": "string",
      "PartitionKey": "string"
    }
  ],
  "StreamName": "string"
}
```

or

```
POST /?Action=PutRecord HTTP/1.1
Host: kinesis.region.domain
Authorization: AWS4-HMAC-SHA256 Credential=..., ...
...
```
Here, StreamName identifies the target stream to add records. StreamName, Data, and PartitionKey are required input data. In our example, we use the default values for all of the optional input data and will not explicitly specify values for them in the input to the method request.

Reading data in Kinesis amounts to calling the GetRecords action:

```plaintext
POST /?Action=GetRecords HTTP/1.1
Host: kinesis.region.domain
Authorization: AWS4-HMAC-SHA256 Credential=..., ...
...
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes
{
    "ShardIterator": "string",
    "Limit": number
}
```

Here, the source stream from which we are getting records is specified in the required ShardIterator value, as is shown in the following Kinesis action to obtain a shard iterator:

```plaintext
POST /?Action=GetShardIterator HTTP/1.1
Host: kinesis.region.domain
Authorization: AWS4-HMAC-SHA256 Credential=..., ...
...
Content-Type: application/x-amz-json-1.1
Content-Length: PayloadSizeBytes
{
    "ShardId": "string",
    "ShardIteratorType": "string",
    "StartingSequenceNumber": "string",
    "StreamName": "string"
}
```

For the GetRecords and PutRecords actions, we expose the GET and PUT methods, respectively, on a /records resource that is appended to a named stream resource (/{stream-name}). Similarly, we expose the PutRecord action as a PUT method on a /record resource.

Because the GetRecords action takes as input a ShardIterator value, which is obtained by calling the GetShardIterator helper action, we expose a GET helper method on a ShardIterator resource (/sharditerator).

The following figure shows the API structure of resources after the methods are created:
The following four procedures describe how to set up each of the methods, how to map data from the method requests to the integration requests, and how to test the methods.

To set up and test the `PUT /streams/{stream-name}/record` method to invoke `PutRecord` in Kinesis:

1. Set up the PUT method, as shown in the following:
2. Add the following request parameter mapping to set the `Content-Type` header to an AWS-compliant version of JSON in the integration request:

```
Content-Type: 'x-amz-json-1.1'
```

The task follows the same procedure to set up the request parameter mapping for the GET / streams method.

3. Add the following body mapping template to map data from the PUT /streams/{stream-name}/record method request to the corresponding integration request of POST /? Action=PutRecord:

```
{
   "StreamName": "$input.params('stream-name')",
   "Data": "$util.base64Encode($input.json('$.Data'))",
   "PartitionKey": "$input.path('$.PartitionKey')"
}
```

This mapping template assumes that the method request payload is of the following format:

```
{
   "Data": "some data",
   "PartitionKey": "some key"
}
```
This data can be modeled by the following JSON schema:

```json
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "PutRecord proxy single-record payload",
    "type": "object",
    "properties": {
        "Data": { "type": "string" },
        "PartitionKey": { "type": "string" }
    }
}
```

You can create a model to include this schema and use the model to facilitate generating the mapping template. However, you can generate a mapping template without using any model.

4. To test the `PUT /streams/{stream-name}/record` method, set the `stream-name` path variable to the name of an existing stream, supply a payload of the required format, and then submit the method request. The successful result is a `200 OK` response with a payload of the following format:

```json
{
    "SequenceNumber": "495594099445788085013334546016986593573102115167928386",
    "ShardId": "shardId-000000000004"
}
```

To set up and test the `PUT /streams/{stream-name}/records` method to invoke `PutRecords` in Kinesis

1. Set up the `PUT /streams/{stream-name}/records` method, as shown in the following:
2. Add the following request parameter mapping to set the Content-Type header to an AWS-compliant version of JSON in the integration request:

```
Content-Type: 'x-amz-json-1.1'
```

The task follows the same procedure to set up the request parameter mapping for the GET / streams method.

3. Add the following body mapping template to map data from the PUT /streams/{stream-name}/records method request to the corresponding integration request of POST /?

```
Action=PutRecords:

{
    "StreamName": "$input.params('stream-name')",
    "Records": [
        #foreach($elem in $input.path('$.records'))
            {
                "Data": "$util.base64Encode($elem.data)",
                "PartitionKey": "$elem.partition-key"
            }
        #if($foreach.hasNext),
        #end
    ]
}
```

This mapping template assumes that the method request payload can be modelled by the following JSON schema:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "PutRecords proxy payload data",
  "type": "object",
  "properties": {
    "records": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "data": { "type": "string" },
          "partition-key": { "type": "string" }
        }
      }
    }
  }
}
```

You can create a model to include this schema and use the model to facilitate generating the mapping template. However, you can generate a mapping template without using any model.

In this tutorial, we used two slightly different payload formats to illustrate that an API developer can choose to expose the backend data format to the client or hide it from the client. One format is for the PUT `/streams/{stream-name}/records` method (above). Another format is used for the PUT `/streams/{stream-name}/record` method (in the previous procedure). In production environment, you should keep both formats consistent.

4. To test the PUT `/streams/{stream-name}/records` method, set the `stream-name` path variable to an existing stream, supply the following payload, and submit the method request.

```json
{
  "records": [
    {
      "data": "some data",
      "partition-key": "some key"
    },
    {
      "data": "some other data",
      "partition-key": "some key"
    }
  ]
}
```

The successful result is a 200 OK response with a payload similar to the following output:

```json
{
  "FailedRecordCount": 0,
  "Records": [
    {
      "SequenceNumber": "49559409944537880850133345460167468741932742152373764162",
      "ShardId": "shardId-000000000004"
    },
    {
      "SequenceNumber": "495594099445378808501333454601686766753356781548470338",
      "ShardId": "shardId-000000000004"
    }
  ]
}
```
To set up and test the GET /streams/{stream-name}/sharditerator method invoke GetShardIterator in Kinesis

The GET /streams/{stream-name}/sharditerator method is a helper method to acquire a required shard iterator before calling the GET /streams/{stream-name}/records method.

1. Set up integration for the GET /streams/{stream-name}/sharditerator method, as shown in the following:

   ![Method Execution](image)

   Provide information about the target backend that this method will call and whether the incoming request data should be modified.

   - **Integration type**: Lambda Function
   - **AWS Region**: us-east-1
   - **AWS Service**: Kinesis
   - **HTTP method**: POST
   - **Action**: GetShardIterator
   - **Execution role**: arn:aws:iam::1234567890:role/apigwProxyRole
   - **Credentials cache**: Do not add caller credentials to cache key
   - **Content Handling**: Pass-through

2. The GetShardIterator action requires an input of a ShardId value. To pass a client-supplied ShardId value, we add a shard-id query parameter to the method request, as shown in the following:
In the following body-mapping template, we set the `shard-id` query parameter value to the ShardId property value of the JSON payload as the input to the `GetShardIterator` action in Kinesis.

3. Configure the body mapping template to generate the required input (`ShardId` and `StreamName`) to the `GetShardIterator` action from the `shard-id` and `stream-name` parameters of the method request. In addition, the mapping template also sets `ShardIteratorType` to `TRIM_HORIZON` as a default.

```json
{
    "ShardId": "$input.params('shard-id')",
    "ShardIteratorType": "TRIM_HORIZON",
    "StreamName": "$input.params('stream-name')"
}
```

4. Using the Test option in the API Gateway console, enter an existing stream name as the stream-name Path variable value, set the shard-id Query string to an existing ShardId value (e.g., shard-000000000004), and choose Test.

The successful response payload is similar to the following output:
Make note of the ShardIterator value. You need it to get records from a stream.

**To configure and test the GET /streams/{stream-name}/records method to invoke the GetRecords action in Kinesis**

1. Set up the GET /streams/{stream-name}/records method, as shown in the following:

   ![Method Execution](image)

   **Integration type**
   - Lambda Function
   - HTTP
   - Mock
   - AWS Service

   **AWS Region** us-east-1
   **AWS Service** Kinesis
   **AWS Subdomain**
   **HTTP method** POST
   **Action** GetRecords
   **Execution role** arn:aws:iam::732524795378:role/apigAwsProxyRole
   **Credentials cache** Do not add caller credentials to cache key
   **Content Handling** Passthrough

2. The GetRecords action requires an input of a ShardIterator value. To pass a client-supplied ShardIterator value, we add a Shard-Iterator header parameter to the method request, as shown in the following:
3. Set up the following mapping template to map the Shard-Iterator header parameter value to the ShardIterator property value of the JSON payload for the GetRecords action in Kinesis.

```json
{
    "ShardIterator": "$input.params('Shard-Iterator')"
}
```

4. Using the Test option in the API Gateway console, type an existing stream name as the stream-name Path variable value, set the Shard-Iterator Header to the ShardIterator value obtained from the test run of the GET /streams/{stream-name}/sharditerator method (above), and choose Test.

The successful response payload is similar to the following output:

```json
{
    "MillisBehindLatest": 0,
    "NextShardIterator": "AAAAAAAAAF...",
    "Records": [ ... ]
}
```
OpenAPI Definitions of a Sample API as a Kinesis Proxy

Following are OpenAPI definitions for the sample API as a Kinesis proxy used in this tutorial.

OpenAPI 3.0

```json
{
"openapi": "3.0.0",
"info": {
"version": "2016-03-31T18:25:32Z",
"title": "KinesisProxy"
},
"paths": {
"/streams": {
"get": {
"responses": {
"200": {
"description": "200 response",
"content": {
"application/json": {
"schema": {
"$ref": "#/components/schemas/Empty"
}
}
}
},
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
"default": {
"statusCode": "200"
}
},
"requestTemplates": {
"application/json": "{\n",
"uri": "arn:aws:apigateway:us-east-1:kinesis:action/ListStreams",
"httpMethod": "POST",
"requestParameters": {
"integration.request.header.Content-Type": "'application/x-amz-json-1.1'"
},
"type": "aws"
}
},
"/streams/{stream-name}": {
"get": {
"parameters": [
{"name": "stream-name",
"in": "path",
"required": true,
"schema": {
"type": "string"
}
}
],
"responses": {
"200": {
"description": "200 response",
"content": {
"application/json": {
"schema": {
"$ref": "#/components/schemas/Empty"
}
}
}
}
}
}"}
```
"content": {
    "application/json": {
        "schema": {
            "$ref": "#/components/schemas/Empty"
        }
    }
}

"x-amazon-apigateway-integration": {
    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
    "responses": {
        "default": {
            "statusCode": "200"
        }
    },
    "requestTemplates": {
        "application/json": "{\n            "StreamName": "$input.params('stream-name')"
        }\n    }
},

"post": {
    "parameters": [
        {
            "name": "stream-name",
            "in": "path",
            "required": true,
            "schema": {
                "type": "string"
            }
        }
    ],
    "responses": {
        "200": {
            "description": "200 response",
            "content": {
                "application/json": {
                    "schema": {
                        "$ref": "#/components/schemas/Empty"
                    }
                }
            }
        }
    },
    "x-amazon-apigateway-integration": {
        "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
        "responses": {
            "default": {
                "statusCode": "200"
            }
        },
        "requestTemplates": {
            "application/json": "{\n                "ShardCount": 5,\n                "StreamName": "$input.params('stream-name')"
            }\n        }
    }
},

"httpMethod": "POST",
"type": "aws"
}
"delete": {
  "parameters": [
   {
    "name": "stream-name",
    "in": "path",
    "required": true,
    "schema": {
      "type": "string"
    }
  }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "headers": {
        "Content-Type": {
          "schema": {
            "type": "string"
          }
        }
      },
      "content": {
        "application/json": {
          "schema": {
            "$ref": "#/components/schemas/Empty"
          }
        }
      }
    },
    "400": {
      "description": "400 response",
      "headers": {
        "Content-Type": {
          "schema": {
            "type": "string"
          }
        }
      }
    },
    "500": {
      "description": "500 response",
      "headers": {
        "Content-Type": {
          "schema": {
            "type": "string"
          }
        }
      }
    }
  },
  "x-amazon-apigateway-integration": {
    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
    "responses": {
      "4\d{2}": {
        "statusCode": "400",
        "responseParameters": {
          "method.response.header.Content-Type": "integration.response.header.Content-Type"
        }
      }
    },
    "default": {
      "statusCode": "200",
      "responseParameters": {
        "x-amazon-apigateway-integration": "Delete Stream"
"method.response.header.Content-Type":
"integration.response.header.Content-Type"
}
},
"5\d{2}": {
    "statusCode": "500",
    "responseParameters": {
    "method.response.header.Content-Type":
"integration.response.header.Content-Type"
    }
}
},
"requestTemplates": {
    "application/json": "{"StreamName": "$input.params('stream-name')""
},
"httpMethod": "POST",
"requestParameters": {
"integration.request.header.Content-Type": "'application/x-amz-json-1.1'"
},
"type": "aws"
}

}/streams/{stream-name}/record": {
  "put": {
    "parameters": [
      { "name": "stream-name",
        "in": "path",
        "required": true,
        "schema": { "type": "string" }
    }
],
  "responses": {
    "200": {
      "description": "200 response",
      "content": { "application/json": { "schema": { "$ref": "#/components/schemas/Empty" } } }
    }
  }
},
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
  "responses": { "default": { "statusCode": "200" } }
},
"requestTemplates": {
  "application/json": "{\"StreamName\": "$input.params('stream-name')",\n  \"Records\": [\n    #foreach($elem in $input.path('$.records'))\n  {\n    \"Data\": "$util.base64Encode($elem.data)",\n    \"PartitionKey\": "$elem.partition-key"
  }#if($foreach.hasNext),#end\n  ]\n},
  "uri": "arn:aws:apigateway:us-east-1:kinesis:action/PutRecord",
  "httpMethod": "POST",
  "requestParameters": {
"integration.request.header.Content-Type": "application/x-amz-json-1.1",
"type": "aws"
}

"/streams/{stream-name}/records": {
  "get": {
    "parameters": [
      {
        "name": "stream-name",
        "in": "path",
        "required": true,
        "schema": {
          "type": "string"
        }
      },
      {
        "name": "Shard-Iterator",
        "in": "header",
        "required": false,
        "schema": {
          "type": "string"
        }
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "content": {
          "application/json": {
            "schema": {
              "$ref": "#/components/schemas/Empty"
            }
          }
        }
      }
    }
  }
},
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
  "responses": {
    "default": {
      "statusCode": "200"
    }
  },
  "requestTemplates": {
    "application/json": "{\n      \"ShardIterator\": \"$input.params('Shard-Iterator')\"\n    }"
  },
  "httpMethod": "POST",
  "requestParameters": {
    "integration.request.header.Content-Type": "application/x-amz-json-1.1"
  },
  "type": "aws"
}
},
"put": {
  "parameters": [
    {
      "name": "Content-Type",
      "in": "header",
      "required": false,
      "schema": {
        "type": "string"
      }
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "content": {
        "application/json": {
          "schema": {
            "$ref": "#/components/schemas/Empty"
          }
        }
      }
    }
  }
},
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
  "responses": {
    "default": {
      "statusCode": "200"
    }
  },
  "requestTemplates": {
    "application/json": "{\n      \"ShardIterator\": \"$input.params('Shard-Iterator')\"\n    }"
  },
  "httpMethod": "POST",
  "requestParameters": {
    "integration.request.header.Content-Type": "application/x-amz-json-1.1"
  },
  "type": "aws"
}
}
"type": "string"
},
{
"name": "stream-name",
"in": "path",
"required": true,
"schema": {
"type": "string"
}
],
"responses": {
"200": {
"description": "200 response",
"content": {
"application/json": {
"schema": {
"$ref": "#/components/schemas/Empty"
}
}
}
},
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
"default": {
"statusCode": "200"
}
},
"requestTemplates": {
"application/json": "{\n    "StreamName": "$input.params('stream-name')",
    "Records": [\n        {\n            "Data": \"$util.base64Encode($elem.data)\",
            "PartitionKey": \"$elem.partition-key\"
        }#if($foreach.hasNext),#end
    ]
}#if($foreach.hasNext),#end
}
},
"application/x-amz-json-1.1": "{\n    "StreamName": "$input.params('stream-name')",
    "records": [\n        {\n            "Data": "$elem.data",
            "PartitionKey": "$elem.partition-key"
        }#if($foreach.hasNext),#end
    ]
}#if($foreach.hasNext),#end
}
},
"uri": "arn:aws:apigateway:us-east-1:kinesis:action/PutRecords",
"httpMethod": "POST",
"requestParameters": {
"integration.request.header.Content-Type": "application/x-amz-json-1.1",
"type": "aws",
"requestBody": {
"content": {
"application/json": {
"schema": {
"$ref": "#/components/schemas/PutRecordsMethodRequestPayload"
}
},
"application/x-amz-json-1.1": {
"schema": {
"$ref": "#/components/schemas/PutRecordsMethodRequestPayload"
}
}
},
"required": true
}
}
"/streams/{stream-name}/sharditerator": {
  "get": {
    "parameters": [
      {
        "name": "stream-name",
        "in": "path",
        "required": true,
        "schema": {
          "type": "string"
        }
      },
      {
        "name": "shard-id",
        "in": "query",
        "required": false,
        "schema": {
          "type": "string"
        }
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "content": {
          "application/json": {
            "schema": {
              "$ref": "#/components/schemas/Empty"
            }
          }
        }
      }
    },
    "x-amazon-apigateway-integration": {
      "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
      "responses": {
        "default": {
          "statusCode": "200"
        }
      },
      "requestTemplates": {
        "application/json": "{\n          \"ShardId\": \"$input.params('shard-id')\",\n          \"ShardIteratorType\": \"TRIM_HORIZON\",\n          \"StreamName\": \"$input.params('stream-name')\"\n        }\n      },
      "httpMethod": "POST",
      "requestParameters": {
        "integration.request.header.Content-Type": "'application/x-amz-json-1.1'"
      },
      "type": "aws"
    }
  }
},
"servers": [
  {
    "url": "https://wd4zclrobb.execute-api.us-east-1.amazonaws.com/{basePath}"
  },
  {
    "url": "https://wd4zclrobb.execute-api.us-east-1.amazonaws.com/{basePath}"
  }
],
"components": {
OpenAPI 2.0

{
    "swagger": "2.0",
    "info": {
        "version": "2016-03-31T18:25:32Z",
        "title": "KinesisProxy"
    },
    "host": "wd4zclrobb.execute-api.us-east-1.amazonaws.com",
    "basePath": "/test",
    "schemes": [
        "https"
    ],
    "paths": {
        "/streams": {
            "get": {
                "consumes": [
                    "application/json"
                ],
                "produces": [
                    "application/json"
                ],
                "responses": {
                    "200": {
                        "description": "200 response",
                        "schema": {
                            "$ref": "#/definitions/Empty"
                        }
                    }
                },
                "x-amazon-apigateway-integration": {
                    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
                    "responses": {
                        "default": {
                            "statusCode": "200"
                        }
                    }
                },
                "requestTemplates": {


```json
"schemas": {
    "PutRecordsMethodRequestPayload": {
        "type": "object",
        "properties": {
            "records": {
                "type": "array",
                "items": {
                    "type": "object",
                    "properties": {
                        "data": {
                            "type": "string"
                        },
                        "partition-key": {
                            "type": "string"
                        }
                    }
                }
            }
        }
    },
    "Empty": {
        "type": "object"
    }
}

OpenAPI 2.0

{
    "swagger": "2.0",
    "info": {
        "version": "2016-03-31T18:25:32Z",
        "title": "KinesisProxy"
    },
    "host": "wd4zclrobb.execute-api.us-east-1.amazonaws.com",
    "basePath": "/test",
    "schemes": [
        "https"
    ],
    "paths": {
        "/streams": {
            "get": {
                "consumes": [
                    "application/json"
                ],
                "produces": [
                    "application/json"
                ],
                "responses": {
                    "200": {
                        "description": "200 response",
                        "schema": {
                            "$ref": "#/definitions/Empty"
                        }
                    }
                },
                "x-amazon-apigateway-integration": {
                    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
                    "responses": {
                        "default": {
                            "statusCode": "200"
                        }
                    }
                },
                "requestTemplates": {

```
"application/json": "{"n"
},
"uri": "arn:aws:apigateway:us-east-1:kinesis:action/ListStreams",
"httpMethod": "POST",
"requestParameters": {
  "integration.request.header.Content-Type": "application/x-amz-json-1.1"
},
"type": "aws"
},
"/streams/{stream-name}": {
  "get": {
    "consumes": [
      "application/json"
    ],
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "stream-name",
        "in": "path",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "schema": {
          "$ref": "#/definitions/Empty"
        }
      }
    },
    "x-amazon-apigateway-integration": {
      "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
      "responses": {
        "default": {
          "statusCode": "200"
        }
      },
      "requestTemplates": {
        "application/json": "{\n    "StreamName": "$input.params('stream-name')"\n}\n",
        "httpMethod": "POST",
        "type": "aws"
      }
    },
    "post": {
      "consumes": [
        "application/json"
      ],
      "produces": [
        "application/json"
      ],
      "parameters": [
        {
          "name": "stream-name",
          "in": "path",
          "required": true,
          "type": "string"
        }
      ],
      
      
    }
  }
}
"responses": {
    "200": {
        "description": "200 response",
        "schema": {
            "$ref": "#/definitions/Empty"
        }
    }
},
"x-amazon-apigateway-integration": {
    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
    "responses": {
        "default": {
            "statusCode": "200"
        }
    },
    "requestTemplates": {
        "application/json": "{"ShardCount": 5, "StreamName": $input.params('stream-name')}" 
    },
    "uri": "arn:aws:apigateway:us-east-1:kinesis:action/CreateStream",
    "httpMethod": "POST",
    "requestParameters": {
        "integration.request.header.Content-Type": "application/x-amz-json-1.1"
    },
    "type": "aws"
}
},
"delete": {
    "consumes": ["application/json"],
    "produces": ["application/json"],
    "parameters": [
        {
            "name": "stream-name",
            "in": "path",
            "required": true,
            "type": "string"
        }
    ],
    "responses": {
        "200": {
            "description": "200 response",
            "schema": {
                "$ref": "#/definitions/Empty"
            },
            "headers": {
                "Content-Type": {
                    "type": "string"
                }
            }
        },
        "400": {
            "description": "400 response",
            "headers": {
                "Content-Type": {
                    "type": "string"
                }
            }
        },
        "500": {
            "description": "500 response",
            "headers": {
                "Content-Type": {
                    "type": "string"
                }
            }
        }
    }
}
"type": "string"
},

"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
  "4\d{2}": {
    "statusCode": "400",
    "responseParameters": {
      "method.response.header.Content-Type": "integration.response.header.Content-Type"
    }
  },
  "default": {
    "statusCode": "200",
    "responseParameters": {
      "method.response.header.Content-Type": "integration.response.header.Content-Type"
    }
  },
  "5\d{2}": {
    "statusCode": "500",
    "responseParameters": {
      "method.response.header.Content-Type": "integration.response.header.Content-Type"
    }
  }
},
"requestTemplates": {
  "application/json": "{\n    "StreamName": "$input.params('stream-name')\\n\n}"
},
"httpMethod": "POST",
"requestParameters": {
  "integration.request.header.Content-Type": "application/x-amz-json-1.1"
},
"type": "aws"
}
},
"/streams/{stream-name}/record": {
"put": {
  "consumes": [
    "application/json"
  ],
  "produces": [
    "application/json"
  ],
  "parameters": [
    {
      "name": "stream-name",
      "in": "path",
      "required": true,
      "type": "string"
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "schema": {
        "$ref": "#/definitions/Empty"
      }
    }
  }
}
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
  "responses": {
    "default": {
      "statusCode": "200"
    }
  },
  "requestTemplates": {
    "application/json": "{\n      "StreamName": "$input.params('stream-name')",\n      "Records": [{\n        "Data": "$util.base64Encode($elem.data)",
        "PartitionKey": "$elem.partition-key"
      }{#if($foreach.hasNext),#end}]
    }"#if($foreach.hasNext),#end
  },
  "uri": "arn:aws:apigateway:us-east-1:kinesis:action/PutRecord",
  "httpMethod": "POST",
  "requestParameters": {
    "integration.request.header.Content-Type": "application/x-amz-json-1.1"
  },
  "type": "aws"
}
},
"/streams/{stream-name}/records": {
  "get": {
    "consumes": [
      "application/json"
    ],
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "stream-name",
        "in": "path",
        "required": true,
        "type": "string"
      },
      {
        "name": "Shard-Iterator",
        "in": "header",
        "required": false,
        "type": "string"
      }
    ],
    "responses": {
      "200": {
        "description": "200 response",
        "schema": {
          "$ref": "#/definitions/Empty"
        }
      }
    },
    "x-amazon-apigateway-integration": {
      "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
      "responses": {
        "default": {
          "statusCode": "200"
        }
      },
      "requestTemplates": {
        "application/json": "{\n          "ShardIterator": "$input.params('Shard-Iterator')"\n        }"#if($foreach.hasNext),#end
      },
      "httpMethod": "POST",
    }
"requestParameters": {
   "integration.request.header.Content-Type": "application/x-amz-json-1.1",
   "type": "aws"
},
"put": {
   "consumes": [
      "application/json",
      "application/x-amz-json-1.1"
   ],
   "produces": [
      "application/json"
   ],
   "parameters": [
   {
      "name": "Content-Type",
      "in": "header",
      "required": false,
      "type": "string"
   },
   {
      "name": "stream-name",
      "in": "path",
      "required": true,
      "type": "string"
   },
   {
      "in": "body",
      "name": "PutRecordsMethodRequestPayload",
      "required": true,
      "schema": {
         "$ref": "#/definitions/PutRecordsMethodRequestPayload"
      }
   }
],
"responses": {
   "200": {
      "description": "200 response",
      "schema": {
         "$ref": "#/definitions/Empty"
      }
   }
},
"x-amazon-apigateway-integration": {
   "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
   "responses": {
      "default": {
         "statusCode": "200"
      }
   }
},
"requestTemplates": {
   "application/json": "{\n    "StreamName": "$input.params('stream-name')",
    "Records": [\n      #foreach($elem in $input.path('$.records'))\n      {\n        "Data": "$util.base64Encode($elem.data)",
        "PartitionKey": "$elem.partition-key"
      }#if($foreach.hasNext),#end\n    ]\n  }",
   "application/x-amz-json-1.1": "set($inputRoot = $input.path(''))\n   {\n      "$set($inputRoot['stream-name'] = $inputRoot['$'].name, $inputRoot['records'] = [\n         {\n            "$elem = $inputRoot[\n                "Records": [\n                    #foreach($elem in $inputRoot['records'])\n                    \n                ]\n            ]\n        }#if($foreach.hasNext),#end\n        ]\n      }"}
},
"uri": "arn:aws:apigateway:us-east-1:kinesis:action/PutRecords",
"httpMethod": "POST",
"requestParameters": {
"integration.request.header.Content-Type": "application/x-amz-json-1.1",
"type": "aws"
},
"path": "/streams/{stream-name}/sharditerator",
"get": {
"consumes": [
"application/json"
],
"produces": [
"application/json"
],
"parameters": [
{
"name": "stream-name",
"in": "path",
"required": true,
"type": "string"
},
{
"name": "shard-id",
"in": "query",
"required": false,
"type": "string"
}
],
"responses": {
"200": {
"description": "200 response",
"schema": {
"$ref": "#/definitions/Empty"
}
}
},
"x-amazon-apigateway-integration": {
"credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
"responses": {
"default": {
"statusCode": "200"
}
},
"requestTemplates": {
"application/json": "{
"ShardId": "$input.params('shard-id')",
"ShardIteratorType": "TRIM_HORIZON",
"StreamName": "$input.params('stream-name')"
}",
"httpMethod": "POST",
"requestParameters": {
"integration.request.header.Content-Type": "application/x-amz-json-1.1"
}
},
"type": "aws"
}
"definitions": {
"PutRecordsMethodRequestPayload": {
"type": "object",
"properties": {
"records": {
"type": "array",
"items": {
"type": "object",
"properties": {
"data": {
"type": "string",
"description": "The data to be added to the stream",
"schema": {
"format": "binary"}
}
}}
}
"properties": {
  "data": {
    "type": "string"
  },
  "partition-key": {
    "type": "string"
  }
}
"Empty": {
  "type": "object"
}
Creating, Deploying, and Invoking a REST API in Amazon API Gateway

Topics
- Creating a REST API in Amazon API Gateway (p. 177)
- Controlling and Managing Access to a REST API in API Gateway (p. 346)
- Documenting a REST API in API Gateway (p. 446)
- Update and Maintain a REST API in Amazon API Gateway (p. 489)
- Deploying a REST API in Amazon API Gateway (p. 494)
- Invoking a REST API in Amazon API Gateway (p. 536)
- Tracing, Logging, and Monitoring an API Gateway API (p. 558)
- API Gateway Extensions to OpenAPI (p. 575)

Creating a REST API in Amazon API Gateway

In Amazon API Gateway, you build a REST API as a collection of programmable entities known as API Gateway resources. For example, you use a RestApi resource to represent an API that can contain a collection of Resource entities. Each Resource entity can in turn have one or more Method resources. Expressed in the request parameters and body, a Method defines the application programming interface for the client to access the exposed Resource and represents an incoming request submitted by the client. You then create an Integration resource to integrate the Method with a backend endpoint, also known as the integration endpoint, by forwarding the incoming request to a specified integration endpoint URI. If necessary, you transform request parameters or body to meet the backend requirements. For responses, you can create a MethodResponse resource to represent a request response received by the client and you create an IntegrationResponse resource to represent the request response that is returned by the backend. You can configure the integration response to transform the backend response data before returning the data to the client or to pass the backend response as-is to the client.

To help your customers understand your API, you can also provide documentation for the API, as part of the API creation or after the API is created. To enable this, add a DocumentationPart resource for a supported API entity.

To control how clients call an API, use IAM permissions (p. 362), a Lambda authorizer (p. 380), or an Amazon Cognito user pool (p. 397). To meter the use of your API, set up usage plans (p. 432) to throttle API requests. You can enable these when creating or updating the API.

You can perform these and other tasks by using the API Gateway console, the API Gateway REST API, the AWS CLI, or one of the AWS SDKs. We discuss how to perform these tasks next.

Topics
- Choose an Endpoint Type to Set up for an API Gateway API (p. 178)
- Initialize REST API Setup in API Gateway (p. 179)
- Set up REST API Methods in API Gateway (p. 199)
Choose an API Endpoint Type to Set up for an API Gateway API

An API endpoint (p. 6) type refers to the hostname of the API. The API endpoint type can be _edge-optimized_, _regional_, or _private_, depending on where the majority of your API traffic originates from.

**Edge-Optimized API Endpoints**

An _edge-optimized API endpoint_ (p. 6) is best for geographically distributed clients. API requests are routed to the nearest CloudFront Point of Presence (POP). This is the default endpoint type for API Gateway REST APIs.

Edge-optimized APIs capitalize the names of HTTP headers (for example, `Cookie`).

CloudFront sorts HTTP cookies in natural order by cookie name before forwarding the request to your origin. For more information about the way CloudFront processes cookies, see _Caching Content Based on Cookies_.

Any custom domain name that you use for an edge-optimized API applies across all regions.

**Regional API Endpoints**

A _regional API endpoint_ (p. 8) is intended for clients in the same region. When a client running on an EC2 instance calls an API in the same region, or when an API is intended to serve a small number of clients with high demands, a regional API reduces connection overhead. For more information, see the section called "Set up a Regional API" (p. 192).

For a regional API, any custom domain name that you use is specific to the region where the API is deployed. If you deploy a regional API in multiple regions, it can have the same custom domain name in all regions. You can use custom domains together with Amazon Route 53 to perform tasks such as latency-based routing. For more information, see the section called "Set Up a Regional Custom Domain Name for REST or WebSocket API" (p. 655) and the section called "How to Create an Edge-Optimized Custom Domain Name" (p. 649).

Regional API endpoints pass all header names through as-is.

**Private API Endpoints**

A _private API endpoint_ (p. 7) is an API endpoint that can only be accessed from your Amazon Virtual Private Cloud (VPC) using an interface VPC endpoint, which is an endpoint network interface (ENI) that you create in your VPC. For more information, see the section called "Create a Private API" (p. 194).

Private API endpoints pass all header names through as-is.
Initialize REST API Setup in API Gateway

For this example, we use a simplified PetStore API, with the HTTP integration, that exposes the GET /pets and GET /pets/{petId} methods. The methods are integrated with the two HTTP endpoints, respectively, of http://petstore-demo-endpoint.execute-api.com/petstore/pets and http://petstore-demo-endpoint.execute-api.com/petstore/pets/{petId}. The API handles 200 OK responses. The examples focus on the essential programming tasks for creating an API in API Gateway, taking advantage of default settings when possible.

Because of the default settings, the resulting API is edge-optimized. An alternative is to set up a regional API (p. 192). To set up a regional API, you must set explicitly the endpoint type of the API as REGIONAL. To set up an edge-optimized API explicitly, you can set EDGE as the type of the endpointConfiguration.

When setting up an API, you must choose a region. When deployed, the API is region-specific. For an edge-optimized API, the base URL is of the http[s]://{restapi-id}.execute-api.amazonaws.com/stage format, where {restapi-id} is the API's id value generated by API Gateway. You can assign a custom domain name (for example, apis.example.com) as the API's host name and call the API with a base URL of the https://apis.example.com/myApi format.

Topics
• Set up an API Using the API Gateway Console (p. 179)
• Set up an Edge-Optimized API Using AWS CLI Commands (p. 179)
• Set up an Edge-Optimized API Using the AWS SDK for Node.js (p. 184)
• Set up an Edge-Optimized API by Importing OpenAPI Definitions (p. 190)
• Set up a Regional API in API Gateway (p. 192)
• Create a Private API in Amazon API Gateway (p. 194)

Set up an API Using the API Gateway Console

To set up an API Gateway API using the API Gateway console, see TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).

You can learn how to set up an API by following an example. For more information, see TUTORIAL: Create a REST API by Importing an Example (p. 42).

Alternatively, you can set up an API by using the API Gateway Import API (p. 341) feature to upload an external API definition, such as one expressed in OpenAPI 2.0 with the API Gateway Extensions to OpenAPI (p. 575). The example provided in TUTORIAL: Create a REST API by Importing an Example (p. 42) uses the Import API feature.

Set up an Edge-Optimized API Using AWS CLI Commands

Setting up an API using the AWS CLI requires working with the create-rest-api, create-resource or get-resources, put-method, put-method-response, put-integration, and put-integration-response commands. The following procedures show how to work with these AWS CLI commands to create the simple PetStore API of the HTTP integration type.

To create a simple PetStore API using AWS CLI

1. Call the create-rest-api command to set up the RestApi in a specific region (us-west-2).

```bash
aws apigateway create-rest-api --name 'Simple PetStore (AWS CLI)' --region us-west-2
```

The following is the output of this command:
Note the returned id of the newly created RestApi. You need it to set up other parts of the API.

2. Call the get-resources command to retrieve the root resource identifier of the RestApi.

```bash
aws apigateway get-resources --rest-api-id vaz7da96z6 --region us-west-2
```

The following is the output of this command:

```
{
  "items": [
    {
      "path": "/",
      "id": "begaltmsm8"
    }
  ]
}
```

Note the root resource Id. You need it to start setting the API's resource tree and configuring methods and integrations.

3. Call the create-resource command to append a child resource (pets) under the root resource (begaltmsm8):

```bash
aws apigateway create-resource --rest-api-id vaz7da96z6 \
  --region us-west-2 \
  --parent-id begaltmsm8 \
  --path-part pets
```

The following is the output of this command:

```
{
  "path": "/pets",
  "pathPart": "pets",
  "id": "6sxz2j",
  "parentId": "begaltmsm8"
}
```

To append a child resource under the root, you specify the root resource Id as the parentId property value. Similarly, to append a child resource under the pets resource, you repeat the preceding step while replacing the parent-id value with the pets resource id of 6sxz2j:

```bash
aws apigateway create-resource --rest-api-id vaz7da96z6 \
  --region us-west-2 \
  --parent-id 6sxz2j \
  --path-part '{petId}'
```

To make a path part a path parameter, enclose it in a pair of curly brackets. If successful, this command returns the following response:

```
{
  "path": "/pets/{petId}",
```
Now that you created two resources: /pets (6sxz2j) and /pets/{petId} (rjkmth), you can proceed to set up methods on them.

4. Call the `put-method` command to add the GET HTTP method on the /pets resource. This creates an API Method of GET /pets with open access, referencing the /pets resource by its ID value of 6sxz2j.

```bash
aws apigateway put-method --rest-api-id vaz7da96z6
  --resource-id 6sxz2j
  --http-method GET
  --authorization-type "NONE"
  --region us-west-2
```

The following is the successful output of this command:

```
{
  "apiKeyRequired": false,
  "httpMethod": "GET",
  "authorizationType": "NONE"
}
```

The method is for open access because `authorization-type` is set to NONE. To permit only authenticated users to call the method, you can use IAM roles and policies, a Lambda authorizer (formerly known as a custom authorizer), or an Amazon Cognito user pool. For more information, see the section called “Controlling and Managing Access to a REST API” (p. 346).

To enable read access to the /pets/{petId} resource (rjkmth), add the GET HTTP method on it to create an API Method of GET /pets/{petId} as follows.

```bash
aws apigateway put-method --rest-api-id vaz7da96z6
  --resource-id rjkmth
  --http-method GET
  --authorization-type "NONE"
  --region us-west-2
  --request-parameters method.request.path.petId=true
```

The following is the successful output of this command:

```
{
  "apiKeyRequired": false,
  "httpMethod": "GET",
  "authorizationType": "NONE",
  "requestParameters": {
    "method.request.path.petId": true
  }
}
```

Note that the method request path parameter of petId must be specified as a required request parameter for its dynamically set value to be mapped to a corresponding integration request parameter and passed to the backend.

5. Call the `put-method-response` command to set up the 200 OK response of the GET /pets method, specifying the /pets resource by its ID value of 6sxz2j.

```bash
aws apigateway put-method-response --rest-api-id vaz7da96z6
```

Initialize REST API Setup

```
--resource-id 6sxz2j --http-method GET \
--status-code 200 --region us-west-2
```

The following is the output of this command:

```
{
  "statusCode": "200"
}
```

Similarly, to set the 200 OK response of the GET /pets/{petId} method, do the following, specifying the /pets/{petId} resource by its resource ID value of rjkmth:

```
aws apigateway put-method-response --rest-api-id vaz7da96z6 \
  --resource-id rjkmth --http-method GET \
  --status-code 200 --region us-west-2
```

Having set up a simple client interface for the API, you can proceed to set up the integration of the API methods with the backend.

6. Call the `put-integration` command to set up an Integration with a specified HTTP endpoint for the GET /pets method. The /pets resource is identified by its resource Id 6sxz2j:

```
aws apigateway put-integration --rest-api-id vaz7da96z6 \
  --resource-id 6sxz2j --http-method GET --type HTTP \
  --integration-http-method GET \
  --uri 'http://petstore-demo-endpoint.execute-api.com/petstore/pets' \
  --region us-west-2
```

The following is the output of this command:

```
{
  "httpMethod": "GET",
  "passthroughBehavior": "WHEN_NO_MATCH",
  "cacheKeyParameters": [],
  "type": "HTTP",
  "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets",
  "cacheNamespace": "6sxz2j"
}
```

Notice that the integration uri of http://petstore-demo-endpoint.execute-api.com/petstore/pets specifies the integration endpoint of the GET /pets method.

Similarly, you create an integration request for the GET /pets/{petId} method as follows:

```
aws apigateway put-integration \
  --rest-api-id vaz7da96z6 \
  --resource-id rjkmth \
  --http-method GET \
  --type HTTP \
  --integration-http-method GET \
  --uri 'http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}' \
  --request-parameters \
  '{}"integration.request.path.id":"method.request.path.petId"'}' \
  --region us-west-2
```

Here, the integration endpoint, uri of http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}, also uses a path parameter (id). Its value is mapped from the corresponding method request path parameter of {petId}. The mapping is defined as part of the
request-parameters. If this mapping is not defined here, the client gets an error response when trying to call the method.

The following is the output of this command:

```
{
  "passthroughBehavior": "WHEN_NO_MATCH",
  "cacheKeyParameters": [],
  "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}",
  "httpMethod": "GET",
  "cacheNamespace": "rjkmth",
  "type": "HTTP",
  "requestParameters": {
    "integration.request.path.id": "method.request.path.petId"
  }
}
```

7. Call the `put-integration-response` command to create an IntegrationResponse of the GET /pets method integrated with an HTTP backend.

```
aws apigateway put-integration-response --rest-api-id vaz7da96z6 \
   --resource-id 6sxz2j --http-method GET \n   --status-code 200 --selection-pattern "" \n   --region us-west-2
```

The following is the output of this command:

```
{
  "selectionPattern": "",
  "statusCode": "200"
}
```

Similarly, call the following `put-integration-response` command to create an IntegrationResponse of the GET /pets/{petId} method:

```
aws apigateway put-integration-response --rest-api-id vaz7da96z6 \
   --resource-id rjkmth --http-method GET \
   --status-code 200 --selection-pattern "" \
   --region us-west-2
```

With the preceding steps, you finished setting up a simple API that allows your customers to query available pets on the PetStore website and to view an individual pet of a specified identifier. To make it callable by your customer, you must deploy the API.

8. Deploy the API to a stage, for example, by calling `create-deployment`:

```
aws apigateway create-deployment --rest-api-id vaz7da96z6 \
   --region us-west-2 \
   --stage-name test \
   --stage-description 'Test stage' \
   --description 'First deployment'
```

You can test this API by typing the `https://vaz7da96z6.execute-api.us-west-2.amazonaws.com/test/pets` URL in a browser, and substituting `vaz7da96z6` with the identifier of your API. The expected output should be as follows:

```
[
  
]```
To test the GET /pets/{petId} method, type https://vaz7da96z6.execute-api.us-west-2.amazonaws.com/test/pets/3 in the browser. You should receive the following response:

```
{
  "id": 3,
  "type": "fish",
  "price": 0.99
}
```

Set up an Edge-Optimized API Using the AWS SDK for Node.js

As an illustration, we use AWS SDK for Node.js to describe how you can use an AWS SDK to create an API Gateway API. For more information using an AWS SDK, including how to set up the development environment, see AWS SDKs.

Setting up an API using the AWS SDK for Node.js involves calling the createRestApi, createResource or getResources, putMethod, putMethodResponse, putIntegration, and putIntegrationResponse functions.

The following procedures walk you through the essential steps to use these SDK commands to set up a simple PetStore API supporting the GET /pets and GET /pets/{petId} methods.

To set up a simple PetStore API using the AWS SDK for Node.js

1. Instantiate the SDK:

   ```javascript
   var AWS = require('aws-sdk');
   AWS.config.region = 'us-west-2';
   var apig = new AWS.APIGateway({apiVersion: '2015/07/09'});
   ```

2. Call the createRestApi function to set up the RestApi entity.

   ```javascript
   apig.createRestApi({
     name: "Simple PetStore (node.js SDK)",
     binaryMediaTypes: [
       '*',
     ],
     description: "Demo API created using the AWS SDK for node.js",
     version: "0.00.001"
   }, function(err, data){
     if (!err) {
       console.log(data);
     } else {
   ```
The function returns an output similar to the following result:

```javascript
{
  id: 'iuo308uaq7',
  name: 'PetStore (node.js SDK)',
  description: 'Demo API created using the AWS SDK for node.js',
  createdAt: 2017-09-05T19:32:35.000Z,
  version: '0.00.001',
  binaryMediaTypes: [ '*' ]
}
```

The resulting API's identifier is `iuo308uaq7`. You need to supply this to continue the setup of the API.

3. Call the `getResources` function to retrieve the root resource identifier of the `RestApi`.

```javascript
api.getRestApis({'restApiId': 'iuo308uaq7'}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log('Get the root resource failed:
', err);
  }
});
```

This function returns an output similar to the following result:

```javascript
{
  "items": [
    {
      "path": "/",
      "id": "s4fb0trnk0"
    }
  ]
}
```

The root resource identifier is `s4fb0trnk0`. This is the starting point for you to build the API resource tree, which you do next.

4. Call the `createResource` function to set up the `/pets` resource for the API, specifying the root resource identifier (`s4fb0trnk0`) on the `parentId` property.

```javascript
api.createResource({'
  restApiId: 'iuo308uaq7',
  parentId: 's4fb0trnk0',
  pathPart: 'pets'
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("The '/pets' resource setup failed:
", err);
  }
});
```

The successful result is as follows:
To set up the /pets/{petId} resource, call the following createResource function, specifying the newly created /pets resource (8sxa2j) on the parentId property.

```javascript
apig.createResource({
  restApiId: 'iuo308uaq7',
  parentId: '8sxa2j',
  pathPart: '{petId}'
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("The '/pets/{petId}' resource setup failed:
", err);
  }
});
```

The successful result returns the newly created resource id value:

```json
{
  "path": "/pets/{petId}",
  "pathPart": "{petId}",
  "id": "au5df2",
  "parentId": "8sxa2j"
}
```

Throughout this procedure, you refer to the /pets resource by specifying its resource ID of 8sxa2j, and the /pets/{petId} resource by specifying its resource ID of au5df2.

5. Call the putMethod function to add the GET HTTP method on the /pets resource (8sxa2j). This sets up the GET /pets Method with open access.

```javascript
apig.putMethod({
  restApiId: 'iuo308uaq7',
  resourceId: '8sxa2j',
  httpMethod: 'GET',
  authorizationType: 'NONE'
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("The 'GET /pets' method setup failed:
", err);
  }
});
```

This function returns an output similar to the following result:

```json
{
  "apiKeyRequired": false,
  "httpMethod": "GET",
  "authorizationType": "NONE"
}
```
To add the GET HTTP method on the /pets/{petId} resource (au5df2), which sets up the API method of GET /pets/{petId} with open access, call the putMethod function as follows.

```javascript
apig.putMethod({
  restApiId: 'iuo308uaq7',
  resourceId: 'au5df2',
  httpMethod: 'GET',
  authorizationType: 'NONE',
  requestParameters: {
    "method.request.path.petId" : true
  }
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("The 'GET /pets/{petId}' method setup failed:
", err);
  }
});
```

This function returns an output similar to the following result:

```javascript
{
  "apiKeyRequired": false,
  "httpMethod": "GET",
  "authorizationType": "NONE",
  "requestParameters": {
    "method.request.path.petId": true
  }
}
```

You need to set the requestParameters property as shown in the preceding example to map and pass the client-supplied petId value to the backend.

6. Call the putMethodResponse function to set up a method response for the GET /pets method.

```javascript
apig.putMethodResponse({
  restApiId: 'iuo308uaq7',
  resourceId: "8sxa2j",
  httpMethod: 'GET',
  statusCode: '200'
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("Set up the 200 OK response for the 'GET /pets' method failed:
", err);
  }
});
```

This function returns an output similar to the following result:

```javascript
{
  "statusCode": "200"
}
```

To set the 200 OK response of the GET /pets/{petId} method, call the putMethodResponse function, specifying the /pets/{petId} resource identifier (au5df2) on the resourceId property.

```javascript
apig.putMethodResponse({
```
7. Call the `putIntegration` function to set up the Integration with a specified HTTP endpoint for the GET /pets method, supplying the /pets resource identifier (8sxa2j) on the `parentId` property.

```javascript
apig.putIntegration({
  restApiId: 'iuo308uaq7',
  resourceId: '8sxa2j',
  httpMethod: 'GET',
  type: 'HTTP',
  integrationHttpMethod: 'GET',
  uri: 'http://petstore-demo-endpoint.execute-api.com/pets'
}, function(err, data){
  if (!err) {
    console.log(data);
  } else {
    console.log("Set up the integration of the 'GET /' method of the API failed:
    " + err);
  }
})
```

This function returns an output similar the following:

```javascript
{
  "httpMethod": "GET",
  "passthroughBehavior": "WHEN_NO_MATCH",
  "cacheKeyParameters": [],
  "type": "HTTP",
  "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets",
  "cacheNamespace": "8sxa2j"
}
```

To set up the integration of the GET /pets/{petId} method with the HTTP endpoint of `http://petstore-demo-endpoint.execute-api.com/pets/{id}` of the backend, call the following `putIntegration` function, supplying the API's /pets/{petId} resource identifier (au5df2) on the `parentId` property.

```javascript
apig.putIntegration({
  restApiId: 'iuo308uaq7',
  resourceId: 'au5df2',
  httpMethod: 'GET',
  type: 'HTTP',
  integrationHttpMethod: 'GET',
  uri: 'http://petstore-demo-endpoint.execute-api.com/pets/{id}',
  requestParameters: {
    "integration.request.path.id": "method.request.path.petId"
  }
}, function(err, data){
})
```
if (!err) {
    console.log(data);
} else {
    console.log("The '\GET /pets/{petId}' method integration setup failed:\n", err);
}
}

This function returns a successful output similar to the following:

```javascript
{
    "httpMethod": "GET",
    "passthroughBehavior": "WHEN_NO_MATCH",
    "cacheKeyParameters": [],
    "type": "HTTP",
    "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}"
}
```

8. Call the `putIntegrationResponse` function to set up the 200 OK integration response for the `GET /pets` method, specifying the API's `/pets` resource identifier (8sx2j) on the `resourceId` property.

```javascript
apig.putIntegrationResponse({
    restApiId: 'iuo308uaq7',
    resourceId: '8sx2j',
    httpMethod: 'GET',
    statusCode: '200',
    selectionPattern: ''
}, function(err, data){
    if (!err) {
        console.log(data);
    } else {
        console.log("The 'GET /pets' method integration response setup failed:\n", err);
    }
})
```

This function will return an output similar to the following result:

```javascript
{
    "selectionPattern": "",
    "statusCode": "200"
}
```

To set up the 200 OK integration response of the `GET /pets/{petId}` method, call the `putIntegrationResponse` function, specifying the API's `/pets/{petId}` resource identifier (au5df2) on the `resourceId` property.

```javascript
apig.putIntegrationResponse({
    restApiId: 'iuo308uaq7',
    resourceId: 'au5df2',
    httpMethod: 'GET',
    statusCode: '200',
    selectionPattern: ''
}, function(err, data){
    if (!err) {
        console.log(data);
    }
})
```
9. As a good practice, test invoking the API before deploying it. To test invoking the GET /pets method, call the testInvokeMethod, specifying the /pets resource identifier (8sxa2j) on the resourceId property:

```javascript
apig.testInvokeMethod({
    restApiId: 'iuo308uaq7',
    resourceId: '8sxa2j',
    httpMethod: "GET",
    pathWithQueryString: '/'
}, function(err, data){
    if (!err) {
        console.log(data)
    } else {
        console.log('Test-invoke-method on 'GET /pets' failed:\n', err);
    }
})
```

To test invoking the GET /pets/{petId} method, call the testInvokeMethod, specifying the /pets/{petId} resource identifier (au5df2) on the resourceId property:

```javascript
apig.testInvokeMethod({
    restApiId: 'iuo308uaq7',
    resourceId: 'au5df2',
    httpMethod: "GET",
    pathWithQueryString: '/'
}, function(err, data){
    if (!err) {
        console.log(data)
    } else {
        console.log('Test-invoke-method on 'GET /pets/{petId}' failed:\n', err);
    }
})
```

10. Finally, you can deploy the API for your customers to call.

```javascript
apig.createDeployment({
    restApiId: 'iuo308uaq7',
    stageName: 'test',
    stageDescription: 'test deployment',
    description: 'API deployment'
}, function(err, data){
    if (err) {
        console.log('Deploying API failed:\n', err);
    } else {
        console.log("Deploying API succeeded\n", data);
    }
})
```

**Set up an Edge-Optimized API by Importing OpenAPI Definitions**

You can set up an API in API Gateway by specifying OpenAPI definitions of appropriate API Gateway API entities and importing the OpenAPI definitions into API Gateway.
The following OpenAPI definitions describe the simple API, exposing only the GET / method integrated with an HTTP endpoint of the PetStore website in the backend, and returning a 200 OK response.

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "title": "Simple PetStore (OpenAPI)"
  },
  "schemes": ["https"],
  "paths": {
    "/pets": {
      "get": {
        "responses": {
          "200": {
            "description": "200 response"
          }
        },
        "x-amazon-apigateway-integration": {
          "responses": {
            "default": {
              "statusCode": "200"
            }
          },
          "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets",
          "passthroughBehavior": "when_no_match",
          "httpMethod": "GET",
          "type": "http"
        }
      }
    },
    "/pets/{petId}": {
      "get": {
        "parameters": [
          {
            "name": "petId",
            "in": "path",
            "required": true,
            "type": "string"
          }
        ],
        "responses": {
          "200": {
            "description": "200 response"
          }
        },
        "x-amazon-apigateway-integration": {
          "responses": {
            "default": {
              "statusCode": "200"
            }
          },
          "requestParameters": {
            "integration.request.path.id": "method.request.path.petId"
          },
          "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets/{id}",
          "passthroughBehavior": "when_no_match",
          "httpMethod": "GET",
          "type": "http"
        }
      }
    }
  }
}``
The following procedure describes how to import these OpenAPI definitions into API Gateway using the API Gateway console.

**To import the simple OpenAPI definitions using the API Gateway console**

1. Sign in to the API Gateway console.
2. Choose **Create API**.
3. Choose **Import from OpenAPI**.
4. If you saved the preceding OpenAPI definitions in a file, choose **Select OpenAPI File**. You can also copy the OpenAPI definitions and paste them into the import text editor.
5. Choose **Import** to finish importing the OpenAPI definitions.

To import the OpenAPI definitions using the AWS CLI, save the OpenAPI definitions into a file and then run the following command, assuming that you use the `us-west-2` region and the absolute OpenAPI file path is `file:///path/to/API_OpenAPI_template.json`:

```
aws apigateway import-rest-api --body 'file:///path/to/API_OpenAPI_template.json' --region us-west-2
```

**Set up a Regional API in API Gateway**

When API requests predominantly originate from an EC2 instance or services within the same region as the API is deployed, a regional API endpoint will typically lower the latency of connections and is recommended for such scenarios.

**Note**

In cases where API clients are geographically dispersed, it may still make sense to use a regional API endpoint, together with your own Amazon CloudFront distribution to ensure that API Gateway does not associate the API with service-controlled CloudFront distributions. For more information about this use case, see [How do I set up API Gateway with my own CloudFront distribution?](#).

To create a regional API, you follow the steps in [creating an edge-optimized API](#), but must explicitly set `REGIONAL` type as the only option of the API's `endpointConfiguration`.

In the following, we show how to create a regional API using the API Gateway console, AWS CLI, and the AWS SDK for Javascript for Node.js.

**Topics**

- Create a Regional API Using the API Gateway Console (p. 192)
- Create a Regional API Using the AWS CLI (p. 193)
- Create a Regional API Using the AWS SDK for JavaScript (p. 193)
- Test a Regional API (p. 194)

**Create a Regional API Using the API Gateway Console**

To create a regional API using the API Gateway console

1. Sign in to the API Gateway console and choose **Create API**.
2. **Under Create new API**, choose the **New API** option.
3. Type a name (for example, Simple PetStore (Console, Regional)) for **API name**.
4. Choose Regional for **Endpoint Type**.
5. Choose **Create API**.

From here on, you can proceed to set up API methods and their associated integrations as described in creating an edge optimized API (p. 179).

**Create a Regional API Using the AWS CLI**

To create a regional API using the AWS CLI, call the `create-rest-api` command:

```sh
aws apigateway create-rest-api \
  --name 'Simple PetStore (AWS CLI, Regional)' \
  --description 'Simple regional PetStore API' \
  --region us-west-2 \
  --endpoint-configuration '{ "types": ["REGIONAL"] }'
```

A successful response returns a payload similar to the following:

```json
{
  "createdDate": "2017-10-13T18:41:39Z",
  "description": "Simple regional PetStore API",
  "endpointConfiguration": {
    "types": "REGIONAL"
  },
  "id": "0qzs2sy7bh",
  "name": "Simple PetStore (AWS CLI, Regional)"
}
```

From here on, you can follow the same instructions given in the section called “Set up an Edge-Optimized API Using AWS CLI Commands” (p. 179) to set up methods and integrations for this API.

**Create a Regional API Using the AWS SDK for JavaScript**

To create a regional API, using the AWS SDK for JavaScript:

```js
apig.createRestApi({
  name: "Simple PetStore (node.js SDK, regional)",
  endpointConfiguration: {
    types: ['REGIONAL']
  },
  description: "Demo regional API created using the AWS SDK for node.js",
  version: "0.00.001"
}, function(err, data){
  if (!err) {
    console.log('Create API succeeded:
  restApiId = data.id;
  } else {
    console.log('Create API failed:
  }
});
```

A successful response returns a payload similar to the following:

```json
{
  "createdDate": "2017-10-13T18:41:39Z",
```
"description": "Demo regional API created using the AWS SDK for node.js",
"endpointConfiguration": {
    "types": "REGIONAL"
},
"id": "0qzs2sy7bh",
"name": "Simple PetStore (node.js SDK, regional)"
}

After completing the preceding steps, you can follow the instructions in the section called “Set up an Edge-Optimized API Using the AWS SDK for Node.js” (p. 184) to set up methods and integrations for this API.

Test a Regional API

Once deployed, the regional API's default URL host name is of the following format:

{restapi-id}.execute-api.{region}.amazonaws.com

The base URL to invoke the API is like the following:

https://{restapi-id}.execute-api.{region}.amazonaws.com/{stage}

Assuming you set up the GET /pets and GET /pets/{petId} methods in this example, you can test the API by typing the following URLs in a browser:

https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets

and

https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets/1

Alternatively, you can use cURL commands:

curl -X GET https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets

and

curl -X GET https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets/2

Create a Private API in Amazon API Gateway

Using Amazon API Gateway, you can create private REST APIs that can only be accessed from your Amazon Virtual Private Cloud (VPC) using an interface VPC endpoint, which is an endpoint network interface (ENI) that you create in your VPC. Using resource policies (p. 198), you can allow or deny access to your API from selected VPCs and VPC endpoints, including across AWS accounts. Each endpoint can be used to access multiple private APIs. You can also use AWS Direct Connect to establish a connection from an on-premises network to Amazon VPC and access your private API over that connection. In all cases, traffic to your private API uses secure connections and does not leave the Amazon network; it is isolated from the public internet.

You can access (p. 556) your private APIs through interface VPC endpoints for API Gateway as shown in the following diagram. If you have private DNS enabled, you can use private or public DNS names to access your APIs. If you have private DNS disabled, you can only use public DNS names.
At a high level, the steps for creating a private API are as follows:

1. First, create an interface VPC endpoint (p. 196) for the API Gateway component service for API execution, known as execute-api, in your VPC.
2. Create and test your private API.
   a. Use one of the following procedures to create your API:
      • API Gateway console (p. 196)
      • API Gateway CLI (p. 197)
      • AWS SDK for JavaScript (p. 197)
   b. To grant access to your VPC endpoint, create a resource policy and attach it to your API (p. 198).
   c. Test your API (p. 556).

Note
The procedures below assume you already have a fully configured VPC. For more information, and to get started with creating a VPC, see Getting Started With Amazon VPC in the Amazon VPC User Guide.

Topics
- Create an Interface VPC Endpoint for API Gateway execute-api (p. 196)
- Create a Private API Using the API Gateway Console (p. 196)
- Create a Private API Using the AWS CLI (p. 197)
- Create a Private API Using the AWS SDK for JavaScript (p. 197)
- Set Up a Resource Policy for a Private API (p. 198)
- Deploy a Private API Using the API Gateway Console (p. 198)
- Private API Development Considerations (p. 198)
Create an Interface VPC Endpoint for API Gateway `execute-api`

The API Gateway component service for API execution is called `execute-api`. To access your private API once it's deployed, you'll need to create an interface VPC endpoint for it in your VPC.

Once you've created your VPC endpoint, you can use it to access multiple private APIs.

**To create an interface VPC endpoint for API Gateway `execute-api`**

1. Log in to the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Endpoints**, **Create Endpoint**.
3. For **Service category**, ensure that **AWS services** is selected.
4. For **Service Name**, choose the API Gateway service endpoint, including the region to which to connect. This will be in the form `com.amazonaws.region.execute-api`, for example `com.amazonaws.us-east-1.execute-api`.

   For **Type**, ensure that it indicates **Interface**.
5. Complete the following information:

   - For **VPC**, choose the VPC in which to you want create the endpoint.
   - For **Subnets**, choose the subnets (Availability Zones) in which to create the endpoint network interfaces.

     **Note**

     Not all Availability Zones may be supported for all AWS services.

   - For **Enable Private DNS Name**, leave the check box selected. Private DNS is enabled by default.

     When private DNS is enabled, you'll be able to access your API via private or public DNS. (This setting does not affect who can access your API, only which DNS addresses they can use.) However, you cannot access public APIs from a VPC by using an API Gateway VPC endpoint with private DNS enabled. Note that these DNS settings do not affect the ability to call these public APIs from the VPC if you are using an edge-optimized custom domain name to access the public API. Using an edge-optimized custom domain name to access your public API (while using private DNS to access your private API) is one way to access both public and private APIs from a VPC where the endpoint has been created with private DNS enabled.

     **Note**

     Leaving private DNS enabled is the recommended choice. If you choose not to enable private DNS, you'll only be able to access your API via public DNS.

     To use the private DNS option, the `enableDnsSupport` and `enableDnsHostnames` attributes of your VPC must be set to `true`. For more information, see **DNS Support in Your VPC** and **Updating DNS Support for Your VPC** in the Amazon VPC User Guide.

   - For **Security group**, select the security group to associate with the VPC endpoint network interfaces.

     The security group you choose must be set to allow TCP Port 443 inbound HTTPS traffic from either an IP range in your VPC or another security group in your VPC.
6. Choose **Create endpoint**.

Create a Private API Using the API Gateway Console

**To create a private API using the API Gateway console**

1. Sign in to the API Gateway console and choose **+ Create API**.
2. Under **Create new API**, choose the **New API** option.
3. Type a name (for example, Simple PetStore (Console, Private)) for API name.
4. For Endpoint Type, choose Private.
5. Choose Create API.

From here on, you can set up API methods and their associated integrations as described in steps 1-6 of ?? (p. 57).

Note
Until your API has a resource policy that grants access to your VPC or VPC endpoint (p. 196), all API calls will fail. Before you test and deploy your API, you'll need to create a resource policy and attach it to the API as described in ?? (p. 198).

Create a Private API Using the AWS CLI

To create a private API using the AWS CLI, call the create-rest-api command:

```
aws apigateway create-rest-api \
   --name 'Simple PetStore (AWS CLI, Private)' \
   --description 'Simple private PetStore API' \
   --region us-west-2 \
   --endpoint-configuration '{ "types": ["PRIVATE"] }'
```

A successful call returns output similar to the following:

```
{
   "createdDate": "2017-10-13T18:41:39Z",
   "description": "Simple private PetStore API",
   "endpointConfiguration": {
      "types": "PRIVATE"
   },
   "id": "0qzs2sy7bh",
   "name": "Simple PetStore (AWS CLI, Private)"
}
```

From here on, you can follow the same instructions given in the section called “Set up an Edge-Optimized API Using AWS CLI Commands” (p. 179) to set up methods and integrations for this API.

When you are ready to test your API, be sure to create a resource policy and attach it to the API as described in ?? (p. 198).

Create a Private API Using the AWS SDK for JavaScript

To create a private API, using the AWS SDK for JavaScript:

```
apig.createRestApi(
   { 
      name: "Simple PetStore (node.js SDK, private)",
      endpointConfiguration: { 
         types: ['PRIVATE']
      }, 
      description: "Demo private API created using the AWS SDK for node.js",
      version: "0.00.001"
   }, function(err, data){
      if (!err) {
         console.log('Create API succeeded:
', data);
         restApiId = data.id;
      } else {
         console.log('Create API failed:
', err);
   }
```

```
A successful call returns output similar to the following:

```json
{
    "createdDate": "2017-10-13T18:41:39Z",
    "description": "Demo private API created using the AWS SDK for node.js",
    "endpointConfiguration": {
        "types": "PRIVATE"
    },
    "id": "0qzs2sy7bh",
    "name": "Simple PetStore (node.js SDK, private)"
}
```

After completing the preceding steps, you can follow the instructions in the section called “Set up an Edge-Optimized API Using the AWS SDK for Node.js” (p. 184) to set up methods and integrations for this API.

When you are ready to test your API, be sure to create a resource policy and attach it to the API as described in ??? (p. 198).

### Set Up a Resource Policy for a Private API

Before your private API can be accessed, you need to create a resource policy and attach it to the API. This will grant access to the API from your VPCs and VPC endpoints or from VPCs and VPC endpoints in other AWS accounts that you explicitly grant access.

To do this, follow the instructions in the section called “Create and Attach an API Gateway Resource Policy to an API” (p. 360). In step 4, choose the Source VPC Whitelist example. Replace `{{vpceID}}` (including the curly braces) with your VPC endpoint ID, and then choose Save to save your resource policy.

You should also consider attaching an endpoint policy to the VPC endpoint to specify the access that's being granted. For more information, see the section called “Use VPC Endpoint Policies for Private APIs” (p. 378).

### Deploy a Private API Using the API Gateway Console

To deploy your private API, do the following in the API Gateway console:

1. In the left navigation pane, select the API and then choose Deploy API from the Actions drop-down menu.
2. In the Deploy API dialog, choose a stage (or [New Stage] for the API's first deployment); enter a name (e.g., "test", "prod", "dev", etc.) in the Stage name input field; optionally, provide a description in Stage description and/or Deployment description; and then choose Deploy.

### Private API Development Considerations

- You can convert an existing public API (regional or edge-optimized) to a private API, and you can convert a private API to a regional API. You cannot convert a private API to an edge-optimized API. For more information, see ??? (p. 490).
- To grant access to your private API to VPCs and VPC endpoints, you'll need to create a resource policy and attach it to the newly created (or converted) API. Until you do so, all calls to the API will fail. For more information, see ??? (p. 198).
- Custom domain names (p. 641) are not supported for private APIs.
- You can use a single VPC endpoint to access multiple private APIs.
Set up REST API Methods in API Gateway

In API Gateway, an API method embodies a method request and a method response. You set up an API method to define what a client should or must do to submit a request to access the service at the backend and to define the responses that the client receives in return. For input, you can choose method request parameters, or an applicable payload, for the client to provide the required or optional data at run time. For output, you determine the method response status code, headers, and applicable body as targets to map the backend response data into, before they are returned to the client. To help the client developer understand the behaviors and the input and output formats of your API, you can document your API (p. 446) and provide proper error messages (p. 252) for invalid requests (p. 329).

An API method request is an HTTP request. To set up the method request, you configure an HTTP method (or verb), the path to an API resource, headers, applicable query string parameters. You also configure a payload when the HTTP method is POST, PUT, or PATCH. For example, to retrieve a pet using the PetStore sample API (p. 42), you define the API method request of GET /pets/{petId}, where {petId} is a path parameter that can take a number at run time.

```
GET /pets/1
Host: apigateway.us-east-1.amazonaws.com
...
```

If the client specifies an incorrect path, for example, /pet/1 or /pets/one instead of /pets/1, an exception is thrown.

An API method response is an HTTP response with a given status code. For a non-proxy integration, you must set up method responses to specify the required or optional targets of mappings. These transform integration response headers or body to associated method response headers or body. The mapping can be as simple as an identity transform that passes the headers or body through the integration as-is. For example, the following 200 method response shows an example of passthrough of a successful integration response as-is.

```
200 OK
Content-Type: application/json
...
{
  "id": "1",
  "type": "dog",
  "price": "$249.99"
}
```

In principle, you can define a method response corresponding to a specific response from the backend. Typically, this involves any 2XX, 4XX, and 5XX responses. However, this may not be practical, because often you may not know in advance all the responses that a backend may return. In practice, you can designate one method response as the default to handle the unknown or unmapped responses from the backend. It is good practice to designate the 500 response as the default. In any case, you must set up at least one method response for non-proxy integrations. Otherwise, API Gateway returns a 500 error response to the client even when the request succeeds at the backend.

To support a strongly typed SDK, such as a Java SDK, for your API, you should define the data model for input for the method request, and define the data model for output of the method response.

**Topics**
• Set up a Method Request in API Gateway (p. 200)
• Set up Method Responses in API Gateway (p. 206)
• Set up a Method Using the API Gateway Console (p. 208)

Set up a Method Request in API Gateway

Setting up a method request involves performing the following tasks, after creating a RestApi resource:

1. Creating a new API or choosing an existing API Resource entity.
2. Creating an API Method resource that is a specific HTTP verb on the new or chosen API Resource. This task can be further divided into the following sub tasks:
   • Adding an HTTP method to the method request
   • Configuring request parameters
   • Defining a model for the request body
   • Enacting an authorization scheme
   • Enabling request validation

You can perform these tasks using the following methods:

- API Gateway console (p. 208)
- AWS CLI commands (create-resource and put-method)
- AWS SDK functions (for example, in Node.js, createResource and putMethod)
- API Gateway REST API (resource:create and method:put).

For examples of using these tools, see Initialize REST API Setup in API Gateway (p. 179).

Topics
• Set up API Resources (p. 200)
• Set up an HTTP Method (p. 203)
• Set up Method Request Parameters (p. 203)
• Set up Method Request Model (p. 204)
• Set up Method Request Authorization (p. 205)
• Set up Method Request Validation (p. 206)

Set up API Resources

In an API Gateway API, you expose addressable resources as a tree of API Resources entities, with the root resource (/) at the top of the hierarchy. The root resource is relative to the API’s base URL, which consists of the API endpoint and a stage name. In the API Gateway console, this base URI is referred to as the Invoke URI and is displayed in the API's stage editor after the API is deployed.

The API endpoint can be a default host name or a custom domain name. The default host name is of the following format:

{api-id}.execute-api.{region}.amazonaws.com

In this format, the {api-id} represents the API identifier that is generated by API Gateway. The {region} variable represents the AWS Region (for example, us-east-1) that you chose when creating the API. A custom domain name is any user-friendly name under a valid internet domain. For example,
if you have registered an internet domain of example.com, any of *.example.com is a valid custom domain name. For more information, see create a custom domain name (p. 641).

For the PetStore sample API (p. 42), the root resource (/) exposes the pet store. The /pets resource represents the collection of pets available in the pet store. The /pets/{petId} exposes an individual pet of a given identifier (petId). The path parameter of {petId} is part of the request parameters.

To set up an API resource, you choose an existing resource as its parent and then create the child resource under this parent resource. You start with the root resource as a parent, add a resource to this parent, add another resource to this child resource as the new parent, and so on, to its parent identifier. Then you add the named resource to the parent.

With AWS CLI, you can call the get-resources command to find out which resources of an API are available:

```
aws apigateway get-resources --rest-api-id <apiId> \ 
  --region <region>
```

The result is a list of the currently available resources of the API. For our PetStore sample API, this list looks like the following:

```
{
  "items": [
    
    
    "path": "/pets",
    "resourceMethods": {
      "GET": {}
    },
    "id": "6sxz2j",
    "pathPart": "pets",
    "parentId": "svzr2028x8"
  },
  
  "path": "/pets/{petId}",
  "resourceMethods": {
    "GET": {}
  },
  "id": "rjkmth",
  "pathPart": "{petId}",
  "parentId": "6sxz2j"
  
  "path": "/",
  "id": "svzr2028x8"
  
    ]
}
```

Each item lists the identifiers of the resource (id) and, except for the root resource, its immediate parent (parentId), as well as the resource name (pathPart). The root resource is special in that it does not have any parent. After choosing a resource as the parent, call the following command to add a child resource.

```
aws apigateway create-resource --rest-api-id <apiId> \ 
  --region <region> \ 
  --parent-id <parentId> \ 
  --path-part <resourceName>
```

For example, to add pet food for sale on the PetStore website, add a food resource to the root (/) by setting path-part to food and parent-id to svzr2028x8. The result looks like the following:
Use a Proxy Resource to Streamline API Setup

As business grows, the PetStore owner may decide to add food, toys, and other pet-related items for sale. To support this, you can add /food, /toys, and other resources under the root resource. Under each sale category, you may also want to add more resources, such as /food/{type}/{item}, /toys/{type}/{item}, etc. This can get tedious. If you decide to add a middle layer {subtype} to the resource paths to change the path hierarchy into /food/{type}/{subtype}/{item}, /toys/{type}/{subtype}/{item}, etc., the changes will break the existing API set up. To avoid this, you can use an API Gateway proxy resource (p. 215) to expose a set of API resources all at once.

API Gateway defines a proxy resource as a placeholder for a resource to be specified when the request is submitted. A proxy resource is expressed by a special path parameter of \( {\text{proxy}\ }^+ \), often referred to as a greedy path parameter. The \( ^+ \) sign indicates whichever child resources are appended to it. The /parent/ {proxy+} placeholder stands for any resource matching the path pattern of /parent/*. The greedy path parameter name, proxy, can be replaced by another string in the same way you treat a regular path parameter name.

Using the AWS CLI, you call the following command to set up a proxy resource under the root (/{proxy+}):

```bash
aws apigateway create-resource --rest-api-id <apiId> \ 
   --region <region> \ 
   --parent-id <rootResourceId> \ 
   --path-part {proxy+}
```

The result is similar to the following:

```json
{
   "path": "/{proxy+}",
   "pathPart": "{proxy+}",
   "id": "234jdr",
   "parentId": "svzr2028x8"
}
```

For the PetStore API example, you can use /{proxy+} to represent both the /pets and /pets/{petId}. This proxy resource can also reference any other (existing or to-be-added) resources, such as /food/{type}/{item}, /toys/{type}/{item}, etc., or /food/{type}/{subtype}/{item}, /toys/{type}/{subtype}/{item}, etc. The backend developer determines the resource hierarchy and the client developer is responsible for understanding it. API Gateway simply passes whatever the client submitted to the backend.

An API can have more than one proxy resource. For example, the following proxy resources are allowed within an API.

```bash
/{proxy+}
/parent/{proxy+}
/parent/{child}/{proxy+}
```

When a proxy resource has non-proxy siblings, the sibling resources are excluded from the representation of the proxy resource. For the preceding examples, /{proxy+} refers to any resources under the root.
resource except for the /parent[/*] resources. In other words, a method request against a specific resource takes precedence over a method request against a generic resource at the same level of the resource hierarchy.

A proxy resource cannot have any child resource. Any API resource after (proxy+) is redundant and ambiguous. The following proxy resources are not allowed within an API.

/\{proxy\+/child
"/parent/\{proxy\+\}/\{child\}
"/parent/\{child\}/(proxy+)/(grandchild+)

Set up an HTTP Method

An API method request is encapsulated by the API Gateway Method resource. To set up the method request, you must first instantiate the Method resource, setting at least an HTTP method and an authorization type on the method.

Closely associated with the proxy resource, API Gateway supports an HTTP method of ANY. This ANY method represents any HTTP method that is to be supplied at run time. It allows you to use a single API method setup for all of the supported HTTP methods of DELETE, GET, HEAD, OPTIONS, PATCH, POST, and PUT.

You can set up the ANY method on a non-proxy resource as well. Combining the ANY method with a proxy resource, you get a single API method setup for all of the supported HTTP methods against any resources of an API. Furthermore, the backend can evolve without breaking the existing API setup.

Before setting up an API method, consider who can call the method. Set the authorization type according to your plan. For open access, set it to NONE. To use IAM permissions, set the authorization type to AWS_IAM. To use a Lambda authorizer function, set this property to CUSTOM. To use an Amazon Cognito user pool, set the authorization type to COGNITO_USER_POOLS.

The following AWS CLI command shows how to create a method request of the ANY verb against a specified resource (6sxz2j), using the IAM permissions to control its access.

```bash
aws apigateway put-method --rest-api-id vaz7da96z6 \
    --resource-id 6sxz2j \
    --http-method ANY \
    --authorization-type AWS_IAM \
    --region us-west-2
```

To create an API method request with a different authorization type, see the section called “Set up Method Request Authorization" (p. 205).

Set up Method Request Parameters

Method request parameters are a way for a client to provide input data or execution context necessary to complete the method request. A method parameter can be a path parameter, a header, or a query string parameter. As part of method request setup, you must declare required request parameters to make them available for the client. For non-proxy integration, you can translate these request parameters to a form that is compatible with the backend requirement.

For example, for the GET /pets/{petId} method request, the {petId} path variable is a required request parameter. You can declare this path parameter when calling the put-method command of the AWS CLI. This is illustrated as follows:

```bash
aws apigateway put-method --rest-api-id vaz7da96z6 \
    --resource-id rjkmth \
```
If a parameter is not required, you can set it to false in request-parameters. For example, if the GET /pets method uses an optional query string parameter of type, and an optional header parameter of breed, you can declare them using the following CLI command, assuming that the /pets resource id is 6sxz2j:

```bash
aws apigateway put-method --rest-api-id vaz7da96z6 \
    --resource-id 6sxz2j \
    --http-method GET \
    --authorization-type "NONE" \
    --region us-west-2 \
    --request-parameters method.request.querystring.type=false,method.request.header.breed=false
```

Instead of this abbreviated form, you can use a JSON string to set the request-parameters value:

```json
"{"method.request.querystring.type":false,"method.request-header.breed":false}"
```

With this setup, the client can query pets by type:

GET /pets?type=dog

And the client can query dogs of the poodle breed as follows:

GET /pets?type=dog
breed:poodle

For information on how to map method request parameters to integration request parameters, see the section called “Set up REST API Integrations” (p. 211).

**Set up Method Request Model**

For an API method that can take input data in a payload, you can use a model. A model is expressed in a JSON schema draft 4 and describes the data structure of the request body. With a model, a client can determine how to construct a method request payload as input. More importantly, API Gateway uses the model to validate a request (p. 329), generate an SDK (p. 521), and initialize a mapping template for setting up the integration in the API Gateway console. For information about how to create a model, see Models and Mapping Templates (p. 262).

Depending on the content types, a method payload can have different formats. A model is indexed against the media type of the applied payload. To set up method request models, add key-value pairs of the "<media-type>":<model-name>" format to the requestModels map when calling the AWS CLI put-method command.

For example, to set a model on the JSON payload of the POST /pets method request of the PetStore example API, you can call the following AWS CLI command:

```bash
aws apigateway put-method \
    --rest-api-id vaz7da96z6 \
    --resource-id 6sxz2j \
    --http-method POST \
    --authorization-type "NONE"
```
Here, petModel is the name property value of a Model resource describing a pet. The actual schema definition is expressed as a JSON string value of the schema property of the Model resource.

In a Java, or other strongly typed SDK, of the API, the input data is cast as the petModel class derived from the schema definition. With the request model, the input data in the generated SDK is cast into the Empty class, which is derived from the default Empty model. In this case, the client cannot instantiate the correct data class to provide the required input.

Set up Method Request Authorization

To control who can call the API method, you can configure the authorization type on the method. You can use this type to enact one of the supported authorizers, including IAM roles and policies (AWS_IAM), an Amazon Cognito user pool (COGNITO_USER_POOLS), or a Lambda authorizer (CUSTOM).

To use IAM permissions to authorize access to the API method, set the authorization-type input property to AWS_IAM. When this option is set, API Gateway verifies the caller's signature on the request, based on the caller's IAM user's access key identifier and secret key. If the verified user has permission to call the method, the request is accepted. Otherwise, the request is rejected and the caller receives an unauthorized error response. The call to the method does not succeed unless the caller has been granted permission to invoke the API method or if the caller is allowed to assume a role that has been granted the permission. The caller has permissions to call this and any other API methods created by anyone of the same AWS account if the caller has the following IAM policy attached to his or her IAM user:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "execute-api:Invoke"
      ],
      "Resource": "arn:aws:execute-api:*::*:*
    }
  ]
}
```

For more information, see the section called "Use IAM Permissions" (p. 362).

At present, such a policy can be granted to only the IAM users of the API owner's account. Users from a different AWS account can call the API methods if they are allowed to assume a role of the API owner account and the assumed role has the proper permissions for the execute-api:Invoke action. For information on cross-account permissions, see Using IAM Roles.

You can use AWS CLI, an AWS SDK, or a REST API client, such as Postman, which implements Signature Version 4 Signing.

To use a Lambda authorizer to authorize access to the API method, set the authorization-type input property to CUSTOM and set the authorizer-id input property to the id property value of a Lambda authorizer that already exists. The referenced Lambda authorizer can be of the TOKEN or REQUEST type. For information about creating a Lambda authorizer, see the section called “Use Lambda Authorizers” (p. 380).

To use an Amazon Cognito user pool to authorize access to the API method, set the authorization-type input property to COGNITO_USER_POOLS and set the authorizer-id input property to the id property value of the COGNITO_USER_POOLS authorizer that was already created. For information
about creating an Amazon Cognito user pool authorizer, see the section called “Use Cognito User Pool as Authorizer for a REST API” (p. 397).

**Set up Method Request Validation**

You can enable request validation when setting up an API method request. You need to first to create a request validator:

```
aws apigateway create-request-validator \
  --rest-api-id 7zw9uyk9k1 \
  --name bodyOnlyValidator \
  --validate-request-body \
  --no-validate-request-parameters
```

This CLI command creates a body-only request validator. Example output is as follows:

```
{
  "validateRequestParameters": true,
  "validateRequestBody": true,
  "id": "jgpyy6",
  "name": "bodyOnlyValidator"
}
```

With this request validator, you can enable request validation as part of the method request setup:

```
aws apigateway put-method \
  --rest-api-id 7zw9uyk9k1 \
  --region us-west-2 \
  --resource-id xdsvhp \
  --http-method PUT \
  --authorization-type "NONE" \
  --request-parameters '{"method.request.querystring.type": false,
  "method.request.querystring.page":false}' \
  --request-models '{"application/json"="petModel"}' \
  --request-validator-id jgpyy6
```

To be included in request validation, a request parameter must be declared as required. If the query string parameter for the page is used in request validation, the `request-parameters` map of the preceding example must be specified as `'{"method.request.querystring.type": false,
"method.request.querystring.page":true}'`.

**Set up Method Responses in API Gateway**

An API method response encapsulates the output of an API method request that the client will receive. The output data includes an HTTP status code, some headers, and possibly a body.

With non-proxy integrations, the specified response parameters and body can be mapped from the associated integration response data or can be assigned certain static values according to mappings. These mappings are specified in the integration response. The mapping can be an identical transformation that passes the integration response through as-is.

With a proxy integration, API Gateway passes the backend response through to the method response automatically. There is no need for you to set up the API method response. However, with the Lambda proxy integration, the Lambda function must return a result of this output format (p. 230) for API Gateway to successfully map the integration response to a method response.

Programmatically, the method response setup amounts to creating a `MethodResponse` resource of API Gateway and setting the properties of `statusCode`, `responseParameters`, and `responseModels`.
When setting status codes for an API method, you should choose one as the default to handle any integration response of an unanticipated status code. It is reasonable to set 500 as the default because this amounts to casting otherwise unmapped responses as a server-side error. For instructional reasons, the API Gateway console sets the 200 response as the default. But you can reset it to the 500 response.

To set up a method response, you must have created the method request.

**Set up Method Response Status Code**

The status code of a method response defines a type of response. For example, responses of 200, 400, and 500 indicate successful, client-side error and server-side error responses, respectively.

To set up a method response status code, set the `statusCode` property to an HTTP status code. The following AWS CLI command creates a method response of 200.

```
aws apigateway put-method-response \
  --region us-west-2 \
  --rest-api-id vz7da96z6 \
  --resource-id 6sxz2j \
  --http-method GET \
  --status-code 200
```

**Set up Method Response Parameters**

Method response parameters define which headers the client receives in response to the associated method request. Response parameters also specify a target to which API Gateway maps an integration response parameter, according to mappings prescribed in the API method's integration response.

To set up the method response parameters, add to the `responseParameters` map of MethodResponse key-value pairs of the "{parameter-name}":"{boolean}" format. The following CLI command shows an example of setting the `my-header` header, the `petId` path variable, and the `query` query parameter as the mapping targets:

```
aws apigateway put-method-response \
  --region us-west-2 \
  --rest-api-id vz7da96z6 \
  --resource-id 6sxz2j \
  --http-method GET \
  --status-code 200 \
  --response-parameters method.request.header.my-header=false,method.request.path.petId=true,method.request.querystring.query=false
```

**Set up Method Response Models**

A method response model defines a format of the method response body. Before setting up the response model, you must first create the model in API Gateway. To do so, you can call the `create-model` command. The following example shows how to create a `PetStorePet` model to describe the body of the response to the `GET /pets/{petId}` method request.

```
aws apigateway create-model \
  --region us-west-2 \
  --rest-api-id vz7da96z6 \
  --content-type application/json \
  --name PetStorePet \
  --schema '{ 
    "$schema": "http://json-schema.org/draft-04/schema#", 
    "title": "PetStorePet", 
    "properties": { 
      "id": { 
        "type": "integer", 
        "description": "Pet's number" 
      }, 
      "name": { 
        "type": "string", 
        "description": "Pet's name" 
      }, 
      "petType": { 
        "type": "string", 
        "description": "Pet type" 
      } 
    } 
  }'
```
The result is created as an API Gateway Model resource.

To set up the method response models to define the payload format, add the "application/json":"PetStorePet" key-value pair to the requestModels map of MethodResponse resource. The following AWS CLI command of put-method-response shows how this is done:

```
aws apigateway put-method-response \
  --region us-west-2 \
  --rest-api-id vaz7da96z6 \
  --resource-id 6sxz2j \
  --http-method GET \
  --status-code 200 \
  --request-parameters method.request.header.my-header=false,method.request.path.petId=true,method.request.querystring.query=false \
  --request-models '{"application/json":"PetStorePet"}'
```

Setting up a method response model is necessary when you generate a strongly typed SDK for the API. It ensures that the output is cast into an appropriate class in Java or Objective-C. In other cases, setting a model is optional.

**Set up a Method Using the API Gateway Console**

Before setting up an API method, verify the following:

- You must have the method available in API Gateway. Follow the instructions in TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).
- If you want the method to communicate with a Lambda function, you must have already created the Lambda invocation role and Lambda execution role in IAM. You must also have created the Lambda function with which your method will communicate in AWS Lambda. To create the roles and function, use the instructions in Create a Lambda Function for Lambda Non-Proxy Integration (p. 34) of the Build an API Gateway API with Lambda Integration (p. 26).
- If you want the method to communicate with an HTTP or HTTP proxy integration, you must have already created, and have access to, the HTTP endpoint URL with which your method will communicate.
- Verify that your certificates for HTTP and HTTP proxy endpoints are supported by API Gateway. For details see API Gateway-Supported Certificate Authorities for HTTP and HTTP Proxy Integrations (p. 414).

**Topics**

- Set up an API Gateway Method Request in the API Gateway Console (p. 208)
- Set up an API Gateway Method Response Using the API Gateway Console (p. 211)

**Set up an API Gateway Method Request in the API Gateway Console**

To use the API Gateway console to specify an API's method request/response, and to configure how the method will authorize requests, follow these instructions.
Note
These instructions assume you have already completed the steps in Set up an API Integration Request Using the API Gateway Console (p. 216). They are best used to supplement the discussions given in Build an API Gateway API with Lambda Integration (p. 26).

1. With the method selected in the Resources pane, choose Method Request from the Method Execution pane.

2. Under Settings, choose the pencil icon to open the Authorization drop-down menu and choose one of the available authorizers.

   a. To enable open access to the method for any user, choose NONE. This step can be skipped if the default setting has not been changed.

   b. To use IAM permissions to control the client access to the method, choose AWS_IAM. With this choice, only users of the IAM roles with the correct IAM policy attached are allowed to call this method.

   To create the IAM role, specify an access policy with a format like the following:

   ```json
   {
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
   "Action": [
   "execute-api:Invoke"
   ],
   "Resource": [
   "resource-statement"
   ]
   }
   }
   }
   ```

   In this access policy, resource-statement is the value of the ARN field in the Authorization Settings section. For more information about setting the IAM permissions, see Control Access to an API with IAM Permissions (p. 362).

   To create the IAM role, you can adapt the instructions in "To create the Lambda invocation role and its policy" and "To create the Lambda execution role and its policy" in the Create Lambda Functions (p. 34) section of the Build an API Gateway API with Lambda Integration (p. 26).

   To save your choice, choose Update. Otherwise, choose Cancel.

   c. To use a Lambda authorizer, choose one under Token authorizer. You must have created a Lambda authorizer to have this choice displayed in the drop-down menu. For information on how to create a Lambda authorizer, see Use API Gateway Lambda Authorizers (p. 380).

   d. To use an Amazon Cognito user pool, choose an available user pool under Cognito user pool authorizers. You must have created a user pool in Amazon Cognito and an Amazon Cognito user pool authorizer in API Gateway to have this choice displayed in the drop-down menu. For information on how to create an Amazon Cognito user pool authorizer, see Control Access to a REST API Using Amazon Cognito User Pools as Authorizer (p. 397).

3. To enable or disable request validation, choose the pencil icon from the Request Validator drop-down menu and choose one of the listed options. For more information about each option, see Enable Request Validation in API Gateway (p. 329).

4. To require an API key, choose the pencil icon to open the API Key Required drop-down menu and choose either true or false according to your API requirements. When enabled, API keys are used in usage plans (p. 432) to throttle client traffic.

5. To add a query string parameter to the method, do the following:
a. Choose the arrow next to **URL Query String Parameters**, and then choose **Add query string**.

b. For **Name**, type the name of the query string parameter.

c. Choose the check-mark icon to save the new query string parameter name.

d. If the newly created query string parameter is to be used for request validation, choose the **Required** option. For more information about the request validation, see Enable Request Validation in API Gateway (p. 329).

e. If the newly created query string parameter is to be used as part of a caching key, check the **Caching** option. This is applicable only when caching is enabled. For more information about caching, see Use Method/Integration Parameters as Cache Keys (p. 502).

**Tip**

To remove the query string parameter, choose the x icon associated with it and then choose **Remove this parameter and any dependent parameters** to confirm the removal.

To change the name of the query string parameter, remove it and then create a new one.

6. To add a header parameter to the method, do the following:

   a. Choose the arrow next to **HTTP Request Headers**, and then choose **Add header**.

   b. For **Name**, type the name of the header parameter and then choose the check-mark icon to save the settings.

   c. If the newly created header parameter is to be used for request validation, choose the **Required** option. For more information about request validation, see Enable Request Validation in API Gateway (p. 329).

   d. If the newly created header parameter is to be used as part of a caching key, choose the **Caching** option. This is applicable only when caching is enabled. For more information about caching, see Use Method/Integration Parameters as Cache Keys (p. 502).

   **Tip**

   To remove the header parameter, choose the x icon associated with it and then choose **Remove this parameter and any dependent parameters** to confirm the removal.

   To change the name of the header parameter, remove it and then create a new one.

7. To declare the payload format of a method request with the **POST**, **PUT**, or **PATCH** HTTP verb, expand **Request Body**, and do the following:

   a. Choose **Add model**.

   b. Type a MIME-type (for example, **application/json**) for **Content type**.

   c. Open the **Model name** drop-down menu to choose an available model for the payload and choose the check-mark icon to save the settings.

   The currently available models for the API include the default **Empty** and **Error** models as well as any models you have created and added to the **Models** collection of the API. For more information about creating a model, see Create a Model (p. 268).

   **Note**

   The model is useful to inform the client of the expected data format of a payload. It is helpful to generate a skeletal mapping template. It is important to generate a strongly typed SDK of the API in such languages as Java, C#, Objective-C, and Swift. It is only required if request validation is enabled against the payload.

8. To assign an operation name in a Java SDK of this API, generated by API Gateway, expand **SDK Settings** and type a name in **Operation name**. For example, for the method request of **GET /pets/{petId}**, the corresponding Java SDK operation name is, by default, `GetPetsPetId`. This name is constructed from the method's HTTP verb (GET) and the resource path variable names (Pets and PetId). If you set the operation name as `getPetById`, the SDK operation name becomes `GetPetById`.

210
Set up an API Gateway Method Response Using the API Gateway Console

An API method can have one or more responses. Each response is indexed by its HTTP status code. By default, the API Gateway console adds 200 response to the method responses. You can modify it, for example, to have the method return 201 instead. You can add other responses, for example, 409 for access denial and 500 for uninitialized stage variables used.

To use the API Gateway console to modify, delete, or add a response to an API method, follow these instructions.

1. Choose **Method Response** from **Method Execution** for a given method of an API resource.
2. To add a new response, choose **Add Response**.
   a. Type an HTTP status code; for example, 200, 400, or 500) for **HTTP Status**, and then choose the check-mark icon to save the choice.
      
      When a backend-returned response does not have a corresponding method response defined, API Gateway fails to return the response to the client. Instead, it returns a 500 Internal server error error response.
   b. Expand the response of the given status code.
   c. Choose **Add Header**.
   d. Type a name for **Name** under **Response Headers for** `{status}`, and then choose the check-mark icon to save the choice.
      
      If you need to translate any backend-returned header to one defined in a method response, you must first add the method response header as described in this step.
   e. Choose **Add Response Model** under **Response Body for** `{status}`.
   f. Type the media type of the response payload for **Content type** and choose a model from the **Models** drop-down menu.
   g. Choose the check-mark icon to save the settings.
3. To modify an existing response, expand the response and follow Step 2 above.
4. To remove a response, choose the x icon for the response and confirm you want to delete the response.

For every response returned from the backend, you must have a compatible response configured as the method response. However, the configuring method response headers and payload model are optional unless you map the result from the backend to the method response before returning to the client. Also, a method response payload model is important if you are generating a strongly typed SDK for your API.

Set up REST API Integrations in API Gateway

After setting up an API method, you must integrate it with an endpoint in the backend. A backend endpoint is also referred to as an integration endpoint and can be a Lambda function, an HTTP webpage, or an AWS service action. As with the API method, the API integration has an integration request and an integration response. An integration request encapsulates an HTTP request received by the backend. It may or may not differ from the method request submitted by the client.

An integration response is an HTTP response encapsulating the output returned by the backend.

Setting up an integration request involves the following: configuring how to pass client-submitted method requests to the backend; configuring how to transform the request data, if necessary, to the integration request data; specifying which Lambda function to call, specifying which HTTP server to forward the incoming request to, or specifying the AWS service action to invoke.

Setting up an integration response, applicable to non-proxy integrations only, involves the following: configuring how to pass the backend-returned result to a method response of a given status code,
configuring how to transform specified integration response parameters to preconfigured method response parameters, and configuring how to map the integration response body to the method response body according to the specified body-mapping templates.

Programmatically, an integration request is encapsulated by the Integration resource and an integration response by the IntegrationResponse resource of API Gateway. To set up an integration request, you create an Integration resource and use it to configure the integration endpoint URL. You then set the IAM permissions to access the backend, and specify mappings to transform the incoming request data before passing it to the backend. To set up an integration response for non-proxy integration, you create an IntegrationResponse resource and use it to set its target method response. You then configure how to map backend output to the method response.

Topics
- Set up an Integration Request in API Gateway (p. 212)
- Set up an Integration Response in API Gateway (p. 218)
- Set up Lambda Integrations in API Gateway (p. 219)
- Set up HTTP Integrations in API Gateway (p. 239)
- Set up API Gateway Private Integrations (p. 244)
- Set up Mock Integrations in API Gateway (p. 250)

Set up an Integration Request in API Gateway

To set up an integration request, you perform the following required and optional tasks:

1. Choose an integration type that determines how method request data is passed to the backend.
2. For non-mock integrations, specify an HTTP method and the URI of the targeted integration endpoint, except for the MOCK integration.
3. For integrations with Lambda functions and other AWS service actions, set an IAM role with required permissions for API Gateway to call the backend on your behalf.
4. For non-proxy integrations, set necessary parameter mappings to map predefined method request parameters to appropriate integration request parameters.
5. For non-proxy integrations, set necessary body mappings to map the incoming method request body of a given content type according to the specified mapping template.
6. For non-proxy integrations, specify the condition under which the incoming method request data is passed through to the backend as-is.
7. Optionally, specify how to handle type conversion for a binary payload.
8. Optionally, declare a cache namespace name and cache key parameters to enable API caching.

Performing these tasks involves creating an Integration resource of API Gateway and setting appropriate property values. You can do so using the API Gateway console, AWS CLI commands, an AWS SDK, or the API Gateway REST API.

Topics
- Basic Tasks of an API Integration Request (p. 213)
- Choose an API Gateway API Integration Type (p. 214)
- Set up a Proxy Integration with a Proxy Resource (p. 215)
- Set up an API Integration Request Using the API Gateway Console (p. 216)
Basic Tasks of an API Integration Request

An integration request is an HTTP request that API Gateway submits to the backend, passing along the client-submitted request data, and transforming the data, if necessary. The HTTP method (or verb) and URI of the integration request are dictated by the backend (that is, the integration endpoint). They can be the same as or different from the method request's HTTP method and URI, respectively. For example, when a Lambda function returns a file that is fetched from Amazon S3, you can expose this operation intuitively as a GET method request to the client even though the corresponding integration request requires that a POST request be used to invoke the Lambda function. For an HTTP endpoint, it is likely that the method request and the corresponding integration request both use the same HTTP verb. However, this is not required. You can integrate the following method request:

```
GET /{var}?query=value
Host: api.domain.net
```

With the following integration request:

```
POST /
Host: service.domain.com
Content-Type: application/json
Content-Length: ...
{
  path: "{var}'s value",
  type: "value"
}
```

As an API developer, you can use whatever HTTP verb and URI for a method request suit your requirements. But you must follow the requirements of the integration endpoint. When the method request data differs from the integration request data, you can reconcile the difference by providing mappings from the method request data to the integration request data. In the preceding examples, the mapping translates the path variable ({var}) and the query parameter (query) values of the GET method request to the values of the integration request's payload properties of path and type. Other mappable request data includes request headers and body. These are described in Set up Request and Response Data Mappings Using the API Gateway Console (p. 259).

When setting up the HTTP or HTTP proxy integration request, you assign the backend HTTP endpoint URL as the integration request URI value. For example, in the PetStore API, the method request to get a page of pets has the following integration request URI:

```
http://petstore-demo-endpoint.execute-api.com/petstore/pets
```

When setting up the Lambda or Lambda proxy integration, you assign the Amazon Resource Name (ARN) for invoking the Lambda function as the integration request URI value. This ARN has the following format:

```
```

The part after arn:aws:apigateway:api-region:lambda:path/, namely, /2015-03-31/functions/arn:aws:lambda:lambda-region:account-id:function:lambda-function-name/invocations, is the REST API URI path of the Lambda Invoke action. If you use the API Gateway console to set up the Lambda integration, API Gateway creates the ARN and assigns it to the integration URI after prompting you to choose the lambda-function-name from a region.
When setting up the integration request with another AWS service action, the integration request URI is also an ARN, similar to the integration with the Lambda Invoke action. For example, for the integration with the GetBucket action of Amazon S3, the integration request URI is an ARN of the following format:

```
ar:aws:apigateway:api-region:s3:path/{bucket}
```

The integration request URI is of the path convention to specify the action, where `{bucket}` is the placeholder of a bucket name. Alternatively, an AWS service action can be referenced by its name. Using the action name, the integration request URI for the GetBucket action of Amazon S3 becomes the following:

```
```

With the action-based integration request URI, the bucket name `{bucket}` must be specified in the integration request body (`{ Bucket: "{bucket}" }`), following the input format of GetBucket action.

For AWS integrations, you must also configure credentials to allow API Gateway to call the integrated actions. You can create a new or choose an existing IAM role for API Gateway to call the action and then specify the role using its ARN. The following shows an example of this ARN:

```
ar:aws:iam::account-id:role/iam-role-name
```

This IAM role must contain a policy to allow the action to be executed. It must also have API Gateway declared (in the role's trust relationship) as a trusted entity to assume the role. Such permissions can be granted on the action itself. They are known as resource-based permissions. For the Lambda integration, you can call the Lambda's addPermission action to set the resource-based permissions and then set credentials to null in the API Gateway integration request.

We discussed the basic integration setup. Advanced settings involve mapping method request data to the integration request data. After discussing the basic setup for an integration response, we cover advanced topics in Set up Request and Response Data Mappings Using the API Gateway Console (p. 259), where we also cover passing payload through and handling content encodings.

**Choose an API Gateway API Integration Type**

You choose an API integration type according to the types of integration endpoint you work with and how you want data to pass to and from the integration endpoint. For a Lambda function, you can have the Lambda proxy integration, or the Lambda custom integration. For an HTTP endpoint, you can have the HTTP proxy integration or the HTTP custom integration. For an AWS service action, you have the AWS integration of the non-proxy type only. API Gateway also supports the mock integration, where API Gateway serves as an integration endpoint to respond to a method request.

The Lambda custom integration is a special case of the AWS integration, where the integration endpoint corresponds to the function-invoking action of the Lambda service.

Programmatically, you choose an integration type by setting the `type` property on the Integration resource. For the Lambda proxy integration, the value is `AWS_PROXY`. For the Lambda custom integration and all other AWS integrations, it is `AWS`. For the HTTP proxy integration and HTTP custom integration, the value is `HTTP_PROXY` and `HTTP`, respectively. For the mock integration, the `type` value is `MOCK`.

The Lambda proxy integration supports a streamlined integration setup with a single Lambda function. The setup is simple and can evolve with the backend without having to tear down the existing setup. For these reasons, it is highly recommended for integration with a Lambda function. In contrast, the Lambda custom integration allows for reuse of configured mapping templates for various integration endpoints that have similar requirements of the input and output data formats. The setup is more involved and is recommended for more advanced application scenarios.
Similarly, the HTTP proxy integration has a streamlined integration setup and can evolve with the backend without having to tear down the existing setup. The HTTP custom integration is more involved to set up, but allows for reuse of configured mapping templates for other integration endpoints.

The following list summarizes the supported integration types:

- **AWS**: This type of integration lets an API expose AWS service actions. In AWS integration, you must configure both the integration request and integration response and set up necessary data mappings from the method request to the integration request, and from the integration response to the method response.

- **AWS_PROXY**: This type of integration lets an API method be integrated with the Lambda function invocation action with a flexible, versatile, and streamlined integration setup. This integration relies on direct interactions between the client and the integrated Lambda function. With this type of integration, also known as the Lambda proxy integration, you do not set the integration request or the integration response. API Gateway passes the incoming request from the client as the input to the backend Lambda function. The integrated Lambda function takes the input of this format (p. 227) and parses the input from all available sources, including request headers, URL path variables, query string parameters, and applicable body. The function returns the result following this output format (p. 230). This is the preferred integration type to call a Lambda function through API Gateway and is not applicable to any other AWS service actions, including Lambda actions other than the function-invoking action.

- **HTTP**: This type of integration lets an API expose HTTP endpoints in the backend. With the HTTP integration, also known as the HTTP custom integration, you must configure both the integration request and integration response. You must set up necessary data mappings from the method request to the integration request, and from the integration response to the method response.

- **HTTP_PROXY**: The HTTP proxy integration allows a client to access the backend HTTP endpoints with a streamlined integration setup on single API method. You do not set the integration request or the integration response. API Gateway passes the incoming request from the client to the HTTP endpoint and passes the outgoing response from the HTTP endpoint to the client.

- **MOCK**: This type of integration lets API Gateway return a response without sending the request further to the backend. This is useful for API testing because it can be used to test the integration setup without incurring charges for using the backend and to enable collaborative development of an API. In collaborative development, a team can isolate their development effort by setting up simulations of API components owned by other teams by using the MOCK integrations. It is also used to return CORS-related headers to ensure that the API method permits CORS access. In fact, the API Gateway console integrates the OPTIONS method to support CORS with a mock integration. Gateway responses (p. 252) are other examples of mock integrations.

### Set up a Proxy Integration with a Proxy Resource

To set up a proxy integration in an API Gateway API with a proxy resource, you perform the following tasks:

- Create a proxy resource with a greedy path variable of `{proxy+}`.
- Set the ANY method on the proxy resource.
- Integrate the resource and method with a backend using the HTTP or Lambda integration type.

**Note**

Greedy path variables, ANY methods, and proxy integration types are independent features, although they are commonly used together. You can configure a specific HTTP method on a greedy resource or apply non-proxy integration types to a proxy resource.

API Gateway enacts certain restrictions and limitations when handling methods with either a Lambda proxy integration or an HTTP proxy integration. For details, see the section called “Important Notes” (p. 692).
Note
When using proxy integration with a passthrough, API Gateway returns the default Content-Type: application/json header if the content type of a payload is unspecified.

A proxy resource is most powerful when it is integrated with a backend using either HTTP proxy integration or Lambda proxy integration.

HTTP Proxy Integration with a Proxy Resource

The HTTP proxy integration, designated by HTTP_PROXY in the API Gateway REST API, is for integrating a method request with a backend HTTP endpoint. With this integration type, API Gateway simply passes the entire request and response between the frontend and the backend, subject to certain restrictions and limitations (p. 692).

Note
HTTP proxy integration supports multi-valued headers and query strings.

When applying the HTTP proxy integration to a proxy resource, you can set up your API to expose a portion or an entire endpoint hierarchy of the HTTP backend with a single integration setup. For example, suppose the backend of the website is organized into multiple branches of tree nodes off the root node (/site) as: /site/a0/a1/.../aN, /site/b0/b1/.../bM, etc. If you integrate the ANY method on a proxy resource of /api/{proxy+} with the backend endpoints with URL paths of /site/{proxy}, a single integration request can support any HTTP operations (GET, POST, etc.) on any of [a0, a1, ..., aN, b0, b1, ...bM, ...]. If you apply a proxy integration to a specific HTTP method, for example, GET, instead, the resulting integration request works with the specified (that is, GET) operations on any of those backend nodes.

Lambda Proxy Integration with a Proxy Resource

The Lambda proxy integration, designated by AWS_PROXY in the API Gateway REST API, is for integrating a method request with a Lambda function in the backend. With this integration type, API Gateway applies a default mapping template to send the entire request to the Lambda function and transforms the output from the Lambda function to HTTP responses.

Similarly, you can apply the Lambda proxy integration to a proxy resource of /api/{proxy+} to set up a single integration to have a backend Lambda function react individually to changes in any of the API resources under /api.

Set up an API Integration Request Using the API Gateway Console

An API method setup defines the method and describes its behaviors. To set up a method, you must specify a resource, including the root ("/"), on which the method is exposed, an HTTP method (GET, POST, etc.), and how it will be integrated with the targeted backend. The method request and response specify the contract with the calling app, stipulating which parameters the API can receive and what the response looks like.

The following procedure describes how to use the API Gateway console to specify method settings.

1. In the Resources pane, choose the method.
2. In the Method Execution pane, choose Integration Request. For Integration type, choose one of the following:
   - Choose Lambda Function if your API will be integrated with a Lambda function. At the API level, this is an AWS integration type.
   - Choose HTTP if your API will be integrated with an HTTP endpoint. At the API level, this is the HTTP integration type.
   - Choose AWS Service if your API will be integrated directly with an AWS service. At the API level, this is the AWS integration type. The Lambda Function option above is a special case of the AWS integration for invoking a Lambda function and is available only in the API Gateway console. To
set up an API Gateway API to create a new Lambda function in AWS Lambda, to set a resource
permission on the Lambda function, or to perform any other Lambda service actions, you must
choose the **AWS Service** option here.

- Choose **Mock** if you want API Gateway to act as your backend to return static responses. At the
API level, this is the **MOCK** integration type. Typically, you can use the **MOCK** integration when
your API is not yet final, but you want to generate API responses to unblock dependent teams
for testing. For the **OPTION** method, API Gateway sets the **MOCK** integration as default to return
CORS-enabling headers for the applied API resource. If you choose this option, skip the rest of the
instructions in this topic and see Set up Mock Integrations in API Gateway (p. 250).

3. If you chose **Lambda Function**, do the following:

   a. For **Lambda Region**, choose the region identifier that corresponds to the region where you
      created the Lambda function. For example, if you created the Lambda function in the US East
      (N. Virginia) Region, choose **us-east-1**. For a list of region names and identifiers, see **AWS
      Lambda in the Amazon Web Services General Reference**.

   b. For **Lambda Function**, type the name of the Lambda function, and then choose the function's
      corresponding ARN.

   c. Choose **Save**.

4. If you chose **HTTP**, do the following:

   a. For **HTTP method**, choose the HTTP method type that most closely matches the method in the
      HTTP backend.

   b. For **Endpoint URL**, type the URL of the HTTP backend you want this method to use.

   c. Choose **Save**.

5. If you chose **Mock**, do the following:

   - Choose **Save**.

6. If you chose **AWS Service**, do the following:

   a. For **AWS Region**, choose the AWS Region you want this method to use to call the action.

   b. For **AWS Service**, choose the AWS service you want this method to call.

   c. For **AWS Subdomain**, type the subdomain used by the AWS service. Typically, you would leave
      this blank. Some AWS services can support subdomains as part of the hosts. Consult the service
      documentation for the availability and, if available, details.

   d. For **HTTP method**, choose the HTTP method type that corresponds to the action. For HTTP
      method type, see the API reference documentation for the AWS service you chose for **AWS
      Service**.

   e. For **Action**, type the action you want to use. For a list of available actions, see the API reference
      documentation for the AWS service you chose for **AWS Service**.

   f. For **Execution Role**, type the ARN of the IAM role that the method will use to call the action.

To create the IAM role, you can adapt the instructions in “To create the Lambda invocation role
and its policies” and “To create the Lambda execution role and its policy” in the Create Lambda
Functions (p. 34) section. Specify an access policy of the following format, with the desired
number of action and resource statements:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "action-statement"
      ],
      "Resource": [
```

217
For the action and resource statement syntax, see the documentation for the AWS service you chose for **AWS Service**.

For the IAM role's trust relationship, specify the following, which enables API Gateway to take action on behalf of your AWS account:

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

g. If the action you typed for **Action** provides a custom resource path that you want this method to use, for **Path Override**, type this custom resource path. For the custom resource path, see the API reference documentation for the AWS service you chose for **AWS Service**.

h. Choose **Save**.

### Set up an Integration Response in API Gateway

For a non-proxy integration, you must set up at least one integration response, and make it the default response, to pass the result returned from the backend to the client. You can choose to pass through the result as-is or to transform the integration response data to the method response data if the two have different formats.

For a proxy integration, API Gateway automatically passes the backend output to the client as an HTTP response. You do not set either an integration response or a method response.

To set up an integration response, you perform the following required and optional tasks:

1. Specify an HTTP status code of a method response to which the integration response data is mapped. This is required.
2. Define a regular expression to select backend output to be represented by this integration response. If you leave this empty, the response is the default response that is used to catch any response not yet configured.
3. If needed, declare mappings consisting of key-value pairs to map specified integration response parameters to given method response parameters.
4. If needed, add body-mapping templates to transform given integration response payloads into specified method response payloads.
5. If needed, specify how to handle type conversion for a binary payload.

An integration response is an HTTP response encapsulating the backend response. For an HTTP endpoint, the backend response is an HTTP response. The integration response status code can take the
The backend-returned status code, and the integration response body is the backend-returned payload. For a Lambda endpoint, the backend response is the output returned from the Lambda function. With the Lambda integration, the Lambda function output is returned as a 200 OK response. The payload can contain the result as JSON data, including a JSON string or a JSON object, or an error message as a JSON object. You can assign a regular expression to the selectionPattern property to map an error response to an appropriate HTTP error response. For more information about the Lambda function error response, see Handle Lambda Errors in API Gateway (p. 235). With the Lambda proxy integration, the Lambda function must return output of the following format:

```json
{
    statusCode: "...",            // a valid HTTP status code
    headers: {
        custom-header: "..."      // any API-specific custom header
    },
    body: "...",                  // a JSON string.
    isBase64Encoded: true|false  // for binary support
}
```

There is no need to map the Lambda function response to its proper HTTP response.

To return the result to the client, set up the integration response to pass the endpoint response through as-is to the corresponding method response. Or you can map the endpoint response data to the method response data. The response data that can be mapped includes the response status code, response header parameters, and response body. If no method response is defined for the returned status code, API Gateway returns a 500 error. For more information, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

## Set up Lambda Integrations in API Gateway

You can integrate an API method with a Lambda function using Lambda proxy integration or Lambda non-proxy (custom) integration.

In Lambda proxy integration, the setup is simple. If your API does not require content encoding or caching, you only need to set the integration’s HTTP method to POST, the integration endpoint URI to the ARN of the Lambda function invocation action of a specific Lambda function, and the credential to an IAM role with permissions to allow API Gateway to call the Lambda function on your behalf.

In Lambda non-proxy integration, in addition to the proxy integration setup steps, you also specify how the incoming request data is mapped to the integration request and how the resulting integration response data is mapped to the method response.

### Topics
- Set up Lambda Proxy Integrations in API Gateway (p. 219)
- Set up Lambda Custom Integrations in API Gateway (p. 231)
- Set up Asynchronous Invocation of the Backend Lambda Function (p. 235)
- Handle Lambda Errors in API Gateway (p. 235)

## Set up Lambda Proxy Integrations in API Gateway

### Topics
- Understand API Gateway Lambda Proxy Integration (p. 220)
- Support for Multi-Value Headers and Query String Parameters (p. 221)
- Set up a Proxy Resource with Lambda Proxy Integration (p. 221)
- Set up Lambda Proxy Integration Using the AWS CLI (p. 223)
- Input Format of a Lambda Function for Proxy Integration (p. 227)
Output Format of a Lambda Function for Proxy Integration (p. 230)

Understand API Gateway Lambda Proxy Integration

Amazon API Gateway Lambda proxy integration is a simple, powerful, and nimble mechanism to build an API with a setup of a single API method. The Lambda proxy integration allows the client to call a single Lambda function in the backend. The function accesses many resources or features of other AWS services, including calling other Lambda functions.

In Lambda proxy integration, when a client submits an API request, API Gateway passes to the integrated Lambda function the raw request as-is, except that the order of the request parameters is not preserved. This request data (p. 227) includes the request headers, query string parameters, URL path variables, payload, and API configuration data. The configuration data can include current deployment stage name, stage variables, user identity, or authorization context (if any). The backend Lambda function parses the incoming request data to determine the response that it returns. For API Gateway to pass the Lambda output as the API response to the client, the Lambda function must return the result in this format (p. 230).

Because API Gateway doesn't intervene very much between the client and the backend Lambda function for the Lambda proxy integration, the client and the integrated Lambda function can adapt to changes in each other without breaking the existing integration setup of the API. To enable this, the client must follow application protocols enacted by the backend Lambda function.

You can set up a Lambda proxy integration for any API method. But a Lambda proxy integration is more potent when it is configured for an API method involving a generic proxy resource. The generic proxy resource can be denoted by a special templated path variable of \( \{proxy+\} \), the catch-all ANY method placeholder, or both. The client can pass the input to the backend Lambda function in the incoming request as request parameters or applicable payload. The request parameters include headers, URL path variables, query string parameters, and the applicable payload. The integrated Lambda function verifies all of the input sources before processing the request and responding to the client with meaningful error messages if any of the required input is missing.

When calling an API method integrated with the generic HTTP method of ANY and the generic resource of \( \{proxy+\} \), the client submits a request with a particular HTTP method in place of ANY. The client also specifies a particular URL path instead of \( \{proxy+\} \), and includes any required headers, query string parameters, or an applicable payload.

The following list summarizes runtime behaviors of different API methods with the Lambda proxy integration:

- **ANY \/(proxy+)**: The client must choose a particular HTTP method, must set a particular resource path hierarchy, and can set any headers, query string parameters, and applicable payload to pass the data as input to the integrated Lambda function.
- **ANY /res**: The client must choose a particular HTTP method and can set any headers, query string parameters, and applicable payload to pass the data as input to the integrated Lambda function.
- **GET|POST|PUT|... /\(proxy+\)**: The client can set a particular resource path hierarchy, any headers, query string parameters, and applicable payload to pass the data as input to the integrated Lambda function.
- **GET|POST|PUT|... /res/\(path\)/...**: The client must choose a particular path segment (for the \(\{path\}\) variable) and can set any request headers, query string parameters, and applicable payload to pass input data to the integrated Lambda function.
- **GET|POST|PUT|... /res**: The client can choose any request headers, query string parameters, and applicable payload to pass input data to the integrated Lambda function.

Both the proxy resource of \(\{proxy+\}\) and the custom resource of \(\{custom\}\) are expressed as templated path variables. However \(\{proxy+\}\) can refer to any resource along a path hierarchy, while \(\{custom\}\)
refers to a particular path segment only. For example, a grocery store might organize its online product
inventory by department names, produce categories, and product types. The grocery store's website
can then represent available products by the following templated path variables of custom resources: /{department}/(produce-category)/ (product-type). For example, apples are represented by /produce/fruit/apple and carrots by /produce/vegetables/carrot. It can also use /{proxy+} to represent any department, any produce category, or any product type that a customer can search for while shopping in the online store. For example, /{proxy+} can refer to any of the following items:

- /produce
- /produce/fruit
- /produce/vegetables/carrot

To let customers search for any available product, its produce category, and the associated store
department, you can expose a single method of GET /{proxy+} with read-only permissions. Similarly,
to allow a supervisor to update the produce department's inventory, you can set up another single
method of PUT /produce/{proxy+} with read/write permissions. To allow a cashier to update the
running total of a vegetable, you can set up a POST /produce/vegetables/{proxy+} method with
read/write permissions. To let a store manager perform any possible action on any available product,
the online store developer can expose the ANY /{proxy+} method with read/write permissions. In any
case, at run time, the customer or the employee must select a particular product of a given type in a
chosen department, a specific produce category in a chosen department, or a specific department.

For more information about setting up API Gateway proxy integrations, see Set up a Proxy Integration
with a Proxy Resource (p. 215).

Proxy integration requires that the client have more detailed knowledge of the backend requirements.
Therefore, to ensure optimal app performance and user experience, the backend developer must
communicate clearly to the client developer the requirements of the backend, and provide a robust error
feedback mechanism when the requirements are not met.

Support for Multi-Value Headers and Query String Parameters

API Gateway supports multiple headers and query string parameters that have the same name. Multi-
value headers as well as single-value headers and parameters can be combined in the same requests and
responses. For more information, see Input Format of a Lambda Function for Proxy Integration (p. 227)
and Output Format of a Lambda Function for Proxy Integration (p. 230).

Set up a Proxy Resource with Lambda Proxy Integration

To set up a proxy resource with the Lambda proxy integration type, create an API
resource with a greedy path parameter (for example, /parent/{proxy+}) and integrate
this resource with a Lambda function backend (for example, arn:aws:lambda:us-
west-2:123456789012:function:SimpleLambda4ProxyResource) on the ANY method. The
greedy path parameter must be at the end of the API resource path. As with a non-proxy resource, you
can set up the proxy resource by using the API Gateway console, importing an OpenAPI definition file, or
calling the API Gateway REST API directly.

The following OpenAPI API definition file shows an example of an API with a proxy resource that is
integrated with a Lambda function named SimpleLambda4ProxyResource.

OpenAPI 3.0

```json
{
   "openapi": "3.0.0",
   "info": {
      "version": "2016-09-12T17:50:37Z",
      "title": "ProxyIntegrationWithLambda"
   }
}```
OpenAPI 2.0

{
  "swagger": "2.0",
  "info": {
    "version": "2016-09-12T17:50:37Z",
    "title": "ProxyIntegrationWithLambda"
  },
  "host": "gy415nuibc.execute-api.us-east-1.amazonaws.com",
  "basePath": "/testStage",
  "schemes": ["https"],
  "paths": {
    "/{proxy+}": {
      "x-amazon-apigateway-any-method": {
        "parameters": [
          {
            "name": "proxy",
            "in": "path",
            "required": true,
            "schema": {
              "type": "string"
            }
          }
        ],
        "responses": {},
        "x-amazon-apigateway-integration": {
          "responses": {
            "default": {
              "statusCode": "200"
            }
          },
          "passthroughBehavior": "when_no_match",
          "httpMethod": "POST",
          "cacheNamespace": "roq9wj",
          "cacheKeyParameters": [
            "method.request.path.proxy"
          ],
          "type": "aws_proxy"
        }
      }
    }
  }
}
In Lambda proxy integration, at run time, API Gateway maps an incoming request into the input `event` parameter of the Lambda function. The input includes the request method, path, headers, any query string parameters, any payload, associated context, and any defined stage variables. The input format is explained in Input Format of a Lambda Function for Proxy Integration (p. 227). For API Gateway to map the Lambda output to HTTP responses successfully, the Lambda function must output the result in the format described in Output Format of a Lambda Function for Proxy Integration (p. 230).

In Lambda proxy integration of a proxy resource through the `ANY` method, the single backend Lambda function serves as the event handler for all requests through the proxy resource. For example, to log traffic patterns, you can have a mobile device send its location information of state, city, street, and building by submitting a request with `/state/city/street/house` in the URL path for the proxy resource. The backend Lambda function can then parse the URL path and insert the location tuples into a DynamoDB table.

**Set up Lambda Proxy Integration Using the AWS CLI**

In this section, we show how to use AWS CLI to set up an API with the Lambda proxy integration.

**Note**
For detailed instructions for using the API Gateway console to configure a proxy resource with the Lambda proxy integration, see TUTORIAL: Build a Hello World API with Lambda Proxy Integration (p. 26).

As an example, we use the following sample Lambda function as the backend of the API:

```javascript
exports.handler = function(event, context, callback) {
    console.log('Received event:', JSON.stringify(event, null, 2));
    var res ={
        "statusCode": 200,
        "headers": {
            "Content-Type": "*/*
```
var greeter = 'World';
if (event.greeter && event.greeter !== '') {
  greeter = event.greeter;
} else if (event.body && event.body !== '') {
  var body = JSON.parse(event.body);
  if (body.greeter && body.greeter !== '') {
    greeter = body.greeter;
  }
} else if (event.queryStringParameters && event.queryStringParameters.greeter &&
  event.queryStringParameters.greeter !== '') {
  greeter = event.queryStringParameters.greeter;
} else if (event.multiValueHeaders && event.multiValueHeaders.greeter &&
  event.multiValueHeaders.greeter !== '') {
  greeter = event.multiValueHeaders.greeter.join(' and ');
} else if (event.headers && event.headers.greeter && event.headers.greeter !== '') {
  greeter = event.headers.greeter;
}
res.body = 'Hello, ' + greeter + '!';
callback(null, res);

Comparing this to the Lambda custom integration setup (p. 232), the input to this Lambda function can be expressed in the request parameters and body. You have more latitude to allow the client to pass the same input data. Here, the client can pass the greeter's name in as a query string parameter, a header, or a body property. The function can also support the Lambda custom integration. The API setup is simpler. You do not configure the method response or integration response at all.

To set up a Lambda proxy integration using the AWS CLI

1. Call the create-rest-api command to create an API:

   ```bash
   aws apigateway create-rest-api --name 'HelloWorld (AWS CLI)' --region us-west-2
   ```

   Note the resulting API's id value (te6si5ach7) in the response:

   ```json
   {
     "name": "HelloWorldProxy (AWS CLI)",
     "id": "te6si5ach7",
     "createdDate": 1508461860
   }
   ```

   You need the API id throughout this section.

2. Call the get-resources command to get the root resource id:

   ```bash
   aws apigateway get-resources --rest-api-id te6si5ach7 --region us-west-2
   ```

   The successful response is shown as follows:

   ```json
   {
     "items": [
     {
       "path": "/",
       "id": "krznpq9xpg"
     }
   ]
   ```
Note the root resource id value (krznpq9xpg). You need it in the next step and later.

3. Call `create-resource` to create an API Gateway Resource of /greeting:

```
aws apigateway create-resource --rest-api-id te6si5ach7
   --region us-west-2
   --parent-id krznpq9xpg
   --path-part {proxy+}
```

The successful response is similar to the following:

```
{
   "path": "/{proxy+}",
   "pathPart": "{proxy+}",
   "id": "2jf6xt",
   "parentId": "krznpq9xpg"
}
```

Note the resulting `{proxy+}` resource's id value (2jf6xt). You need it to create a method on the /{proxy+} resource in the next step.

4. Call `put-method` to create an ANY method request of ANY /{proxy+}:

```
aws apigateway put-method --rest-api-id te6si5ach7
   --region us-west-2
   --resource-id 2jf6xt
   --http-method ANY
   --authorization-type "NONE"
```

The successful response is similar to the following:

```
{
   "apiKeyRequired": false,
   "httpMethod": "ANY",
   "authorizationType": "NONE"
}
```

This API method allows the client to receive or send greetings from the Lambda function at the backend.

5. Call `put-integration` to set up the integration of the ANY /{proxy+} method with a Lambda function, named HelloWorld. This function responds to the request with a message of "Hello, {name}!", if the greeter parameter is provided, or "Hello, World!", if the query string parameter is not set.

```
aws apigateway put-integration
   --region us-west-2
   --rest-api-id vaz7da96z6
   --resource-id 2jf6xt
   --http-method ANY
   --type AWS_PROXY
   --integration-http-method POST
   --credentials arn:aws:iam::123456789012:role/apigAwsProxyRole
```

**Important**

For Lambda integrations, you must use the HTTP method of POST for the integration request, according to the specification of the Lambda service action for function.
invocations. The IAM role of apigAwsProxyRole must have policies allowing the apigateway service to invoke Lambda functions. For more information about IAM permissions, see the section called “API Gateway Permissions Model for Invoking an API” (p. 363).

The successful output is similar to the following:

```json
{
    "passthroughBehavior": "WHEN_NO_MATCH",
    "cacheKeyParameters": [],
    "httpMethod": "POST",
    "cacheNamespace": "vvom7n",
    "credentials": "arn:aws:iam::1234567890:role/apigAwsProxyRole",
    "type": "AWS_PROXY"
}
```

Instead of supplying an IAM role for credentials, you can call the add-permission command to add resource-based permissions. This is what the API Gateway console does.

6. Call create-deployment to deploy the API to a test stage:

```bash
aws apigateway create-deployment --rest-api-id te6si5ach7 --stage-name test
```

7. Test the API using the following cURL commands in a terminal.

**Calling the API with the query string parameter of ?greeter=jane:**

```bash
-H 'authorization: AWS4-HMAC-SHA256 Credential={access_key}/20171020/us-west-2/execute-api/aws4_request, 
    SignedHeaders=content-type;host;x-amz-date, Signature=f327...5751'
```

**Calling the API with a header parameter of greeter:jane:**

```bash
curl -X GET https://te6si5ach7.execute-api.us-west-2.amazonaws.com/test/hi 
-H 'authorization: AWS4-HMAC-SHA256 Credential={access_key}/20171020/us-west-2/execute-api/aws4_request, 
    SignedHeaders=content-type;host;x-amz-date, Signature=f327...5751' 
-H 'content-type: application/json' 
-H 'greeter: jane'
```

**Calling the API with a body of {"greeter":"jane"}**: 

```bash
curl -X POST https://te6si5ach7.execute-api.us-west-2.amazonaws.com/test 
-H 'authorization: AWS4-HMAC-SHA256 Credential={access_key}/20171020/us-west-2/execute-api/aws4_request, 
    SignedHeaders=content-type;host;x-amz-date, Signature=f327...5751' 
-H 'content-type: application/json' 
-d '{ "greeter": "jane" }'
```

In all the cases, the output is a 200 response with the following response body:

```json
"Hello, jane!"
```
Input Format of a Lambda Function for Proxy Integration

In Lambda proxy integration, API Gateway maps the entire client request to the input event parameter of the backend Lambda function as follows:

```
{
    "resource": "Resource path",
    "path": "Path parameter",
    "httpMethod": "Incoming request's method name"
    "headers": {String containing incoming request headers}
    "multiValueHeaders": {List of strings containing incoming request headers}
    "queryStringParameters": {query string parameters}
    "multiValueQueryStringParameters": {List of query string parameters}
    "pathParameters":  {path parameters}
    "stageVariables": {Applicable stage variables}
    "requestContext": {Request context, including authorizer-returned key-value pairs}
    "body": "A JSON string of the request payload."
    "isBase64Encoded": "A boolean flag to indicate if the applicable request payload is Base64-encode"
}
```

**Note**

In the input:

- The headers key can only contain single-value headers.
- The multiValueHeaders key can contain multi-value headers as well as single-value headers.
- If you specify values for both headers and multiValueHeaders, API Gateway merges them into a single list. If the same key-value pair is specified in both, only the values from multiValueHeaders will appear in the merged list.

The following POST request shows an API deployed to testStage with a stage variable of stageVariableName=stageVariableValue:

```
POST /testStage/hello/world?name=me HTTP/1.1
Host: gy415nuibc.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
headerName: headerValue

{
    "a": 1
}
```

This request produces the following response payload, which contains the output returned from the backend Lambda function, where input was set to the event parameter to the Lambda function.

```
{
    "message": "Hello me!",
    "input": {
        "resource": "/{proxy+}"
        "path": "hello/world",
        "httpMethod": "POST",
        "headers": {
            "Accept": "*/*",
            "Accept-Encoding": "gzip, deflate",
            "cache-control": "no-cache",
            "CloudFront-Forwarded-Proto": "https",
            "CloudFront-Is-Desktop-Viewer": "true",
            "CloudFront-Is-Mobile-Viewer": "false",
            "CloudFront-Is-SmartTV-Viewer": "false",
```

227
In the input to the backend Lambda function, the `requestContext` object is a map of key-value pairs. In each pair, the key is the name of a `$context` (p. 293) variable property, and the value is the value of that property. API Gateway may add new keys to the map.

Depending on the features that are enabled, the `requestContext` map may vary from API to API. For example, in the preceding example, no authorization type is specified, so no `$context.authorizer.*` or `$context.identity.*` properties are present. When an authorization type is specified, this causes API Gateway to pass authorized user information to the integration endpoint in a `requestContext.identity` object as follows:
When the authorization type is **AWS_IAM**, the authorized user information includes $context.identity.* properties.

When the authorization type is **COGNITO_USER_POOLS** (Amazon Cognito authorizer), the authorized user information includes $context.identity.cognito* and $context.authorizer.claims.* properties.

When the authorization type is **CUSTOM** (Lambda authorizer), the authorized user information includes $context.authorizer.principalId and other applicable $context.authorizer.* properties.

The following shows an example of a `requestContext` that is passed to a Lambda proxy integration endpoint when the authorization type is set to **AWS_IAM**.

```json
{
   ...
   "requestContext": {
      "requestTime": "20/Feb/2018:22:48:57 +0000",
      "path": "/test/",
      "accountId": "123456789012",
      "protocol": "HTTP/1.1",
      "resourceId": "yx5mhem7ye",
      "stage": "test",
      "requestTimeEpoch": 1519166937665,
      "requestId": "3c3ecbaa-1690-11e8-ae31-8f39f1d24af6",
      "identity": {
         "cognitoIdentityPoolId": null,
         "accountId": "123456789012",
         "cognitoIdentityId": null,
         "caller": "AIDAJ........4HCKVJZG",
         "sourceIp": "51.240.196.104",
         "accessKey": "IAM_user_access_key",
         "cognitoAuthenticationType": null,
         "cognitoAuthenticationProvider": null,
         "userArn": "arn:aws:iam::123456789012:user/alice",
         "userAgent": "PostmanRuntime/7.1.1",
         "user": "AIDAJ........4HCKVJZG"
      },
      "resourcePath": "/",
      "httpMethod": "GET",
      "apiId": "qr2gd9cfmf"
   },
   ...
}
```

### Output Format of a Lambda Function for Proxy Integration

In Lambda proxy integration, API Gateway requires the backend Lambda function to return output according to the following JSON format:

```json
{
   "isBase64Encoded": true|false,
   "statusCode": httpStatusCode,
   "headers": { "headerName": "headerValue", ... },
   "multiValueHeaders": { "headerName": ["headerValue", "headerValue2", ...], ... },
   "body": "...
```

In the output:

- The `headers` and `multiValueHeaders` keys can be unspecified if no extra response headers are to be returned.
- The `headers` key can only contain single-value headers.
• The multiValueHeaders key can contain multi-value headers as well as single-value headers. You can use the multiValueHeaders key to specify all of your extra headers, including any single-value ones.

• If you specify values for both headers and multiValueHeaders, API Gateway merges them into a single list. If the same key-value pair is specified in both, only the values from multiValueHeaders will appear in the merged list.

To enable CORS for the Lambda proxy integration, you must add Access-Control-Allow-Origin: domain-name to the output headers. domain-name can be * for any domain name. The output body is marshalled to the frontend as the method response payload. If body is a binary blob, you can encode it as a Base64-encoded string by setting isBase64Encoded to true and configuring */* as a Binary Media Type. Otherwise, you can set it to false or leave it unspecified.

Note
For more information about enabling binary support, see Enable Binary Support Using the API Gateway Console (p. 306).

If the function output is of a different format, API Gateway returns a 502 Bad Gateway error response.

To return a response in a Lambda function in Node.js, you can use commands such as the following:

• To return a successful result, call callback(null, {"statusCode": 200, "body": "results"}).

• To throw an exception, call callback(new Error('internal server error')).

• For a client-side error (if, for example, a required parameter is missing), you can call callback(null, {"statusCode": 400, "body": "Missing parameters of ..."}) to return the error without throwing an exception.

In a Lambda async function in Node.js 8.10, the equivalent syntax would be:

• To return a successful result, call return {"statusCode": 200, "body": "results"}.

• To throw an exception, call throw new Error("internal server error").

• For a client-side error (if, for example, a required parameter is missing), you can call return {"statusCode": 400, "body": "Missing parameters of ..."} to return the error without throwing an exception.

Set up Lambda Custom Integrations in API Gateway

To show how to set up the Lambda custom integration, we create an API Gateway API to expose the GET /greeting?greeter={name} method to invoke a Lambda function. The function responds with a message of "Hello, {name}!" if the greeter parameter value is a non-empty string. It returns a message of "Hello, World!" if the greeter value is an empty string. The function returns an error message of "Missing the required greeter parameter." if the greeter parameter is not set in the incoming request. We name the function HelloWorld.

For reference, a Node.js version of the Lambda function is shown as follows:

```javascript
exports.handler = function(event, context, callback) {
  var res ={
    "statusCode": 200,
    "headers": {
      "Content-Type": "/*/*"
    }
  };
  if (event.greeter==null) {
```
You can create it in the Lambda console or by using the AWS CLI. In this section, we reference this function using the following ARN:

```
arn:aws:lambda:us-east-1:123456789012:function:HelloWorld
```

With the Lambda function set in the backend, proceed to set up the API.

### To set up the Lambda custom integration using the AWS CLI

1. Call the `create-rest-api` command to create an API:

   ```
   aws apigateway create-rest-api --name 'HelloWorld (AWS CLI)' --region us-west-2
   ```

   Note the resulting API's id value (te6si5ach7) in the response:

   ```
   {
   "name": "HelloWorld (AWS CLI)",
   "id": "te6si5ach7",
   "createdDate": 1508461860
   }
   ```

   You need the API id throughout this section.

2. Call the `get-resources` command to get the root resource id:

   ```
   aws apigateway get-resources --rest-api-id te6si5ach7 --region us-west-2
   ```

   The successful response is as follows:

   ```
   {
   "items": [
   {
   "path": "/",
   "id": "krznpq9xpg"
   }
   ]
   }
   ```

   Note the root resource id value (krznpq9xpg). You need it in the next step and later.

3. Call `create-resource` to create an API Gateway Resource of `/greeting`:

   ```
   aws apigateway create-resource --rest-api-id te6si5ach7 --region us-west-2 --parent-id kruznpq9xpg --path-part greeting
   ```

   The successful response is similar to the following:
Note the resulting `greeting` resource's id value (2jf6xt). You need it to create a method on the `/greeting` resource in the next step.

4. Call `put-method` to create an API method request of `GET /greeting?greeter={name}`:

```bash
aws apigateway put-method --rest-api-id te6si5ach7
    --region us-west-2
    --resource-id 2jf6xt
    --http-method GET
    --authorization-type "NONE"
    --request-parameters method.request.querystring.greeter=false
```

The successful response is similar to the following:

```json
{
    "apiKeyRequired": false,
    "httpMethod": "GET",
    "authorizationType": "NONE",
    "requestParameters": {
        "method.request.querystring.greeter": false
    }
}
```

This API method allows the client to receive a greeting from the Lambda function at the backend. The `greeter` parameter is optional because the backend should handle either an anonymous caller or a self-identified caller.

5. Call `put-method-response` to set up the 200 OK response to the method request of `GET /greeting?greeter={name}`:

```bash
aws apigateway put-method-response
    --region us-west-2
    --rest-api-id te6si5ach7
    --resource-id 2jf6xt
    --http-method GET
    --status-code 200
```

6. Call `put-integration` to set up the integration of the `GET /greeting?greeter={name}` method with a Lambda function, named `HelloWorld`. The function responds to the request with a message of "Hello, {name}!", if the `greeter` parameter is provided, or "Hello, World!", if the query string parameter is not set.

```bash
aws apigateway put-integration
    --region us-west-2
    --rest-api-id vaz7da96z6
    --resource-id 2jf6xt
    --http-method GET
    --type AWS
    --integration-http-method POST
    --request-templates file://path/to/integration-request-template.json
```
Here, the request-template parameter value, file://path/to/integration-request-template.json, points to a JSON file, named integration-request-template.json in the path/to directory, which contains a key-value map as a JSON object. The key is a media type of the request payload and the value is a mapping template for the body of the specified content type. In this example, the JSON file contains the following JSON object:

```json
{"application/json":"{"greeter":"$input.params('greeter')"}"
}
```

The mapping template supplied here translates the greeter query string parameter to the greeter property of the JSON payload. This is necessary because input to a Lambda function in the Lambda function must be expressed in the body. You could use JSON string of the map (for example, "{"greeter": "'john'"}") as the request-template input value to the put-integration command. However, using the file input avoids the difficult, and sometimes impossible, quote-escaping that is required to stringify a JSON object.

**Important**

For Lambda integrations, you must use the HTTP method of POST for the integration request, according to the specification of the Lambda service action for function invocations. The uri parameter is the ARN of the function-invoking action. Successful output is similar to the following:

```json
{
    "passthroughBehavior": "WHEN_NO_MATCH",
    "cacheKeyParameters": [],
    "httpMethod": "POST",
    "requestTemplates": {
        "application/json": "{\"greeter\":\"$input.params('greeter')\"}"
    },
    "cacheNamespace": "krznpq9xpg",
    "credentials": "arn:aws:iam::123456789012:role/apigAwsProxyRole",
    "type": "AWS"
}
```

The IAM role of apigAwsProxyRole must have policies that allow the apigateway service to invoke Lambda functions. Instead of supplying an IAM role for credentials, you can call the add-permission command to add resource-based permissions. This is how the API Gateway console adds these permissions.

7. Call put-integration-response to set up the integration response to pass the Lambda function output to the client as the 200 OK method response.

```bash
aws apigateway put-integration-response \
  --region us-west-2 \
  --rest-api-id te6si5ach7 \
  --resource-id 2jf6xt \
  --http-method GET \
  --status-code 200 \
  --selection-pattern ""
```

By setting the selection-pattern to an empty string, the 200 OK response is the default.

The successful response should be similar to the following:
8. Call `create-deployment` to deploy the API to a test stage:

```bash
aws apigateway create-deployment --rest-api-id te6si5ach7 --stage-name test
```

9. Test the API using the following cURL command in a terminal:

```bash
curl -X GET 'https://te6si5ach7.execute-api.us-west-2.amazonaws.com/test/greeting?greeter=me' \
   -H 'authorization: AWS4-HMAC-SHA256 Credential={access_key}/20171020/us-west-2/execute-api/aws4_request, SignedHeaders=content-type;host;x-amz-date, Signature=f327...5751'
```

## Set up Asynchronous Invocation of the Backend Lambda Function

In Lambda non-proxy (custom) integration, the backend Lambda function is invoked synchronously by default. This is the desired behavior for most REST API operations. Some applications, however, require work to be performed asynchronously (as a batch operation or a long-latency operation), typically by a separate backend component. In this case, the backend Lambda function is invoked asynchronously, and the front-end REST API method doesn't return the result.

You can configure the Lambda function for a Lambda non-proxy integration to be invoked asynchronously by specifying 'Event' as the Lambda invocation type. This is done as follows:

### Configure Lambda asynchronous invocation in the API Gateway console

1. In **Integration Request**, add an `X-Amz-Invocation-Type` header.
2. In **Method Request**, add an `InvocationType` header and map it to the `X-Amz-Invocation-Type` header in the **Integration Request** with either a static value of 'Event' or the header mapping expression of `method.request.header.InvocationType`. For the latter, the client must include the `InvocationType:Event` header when making a request to the API method.

### Handle Lambda Errors in API Gateway

For Lambda custom integrations, you must map errors returned by Lambda in the integration response to standard HTTP error responses for your clients. Otherwise, Lambda errors are returned as 200 OK responses by default and the result is not intuitive for your API users.

There are two types of errors that Lambda can return: standard errors and custom errors. In your API, you must handle these differently.

With the Lambda proxy integration, Lambda is required to return an output of the following format:

```json
{
   "isBase64Encoded": "boolean",
   "statusCode": "number",
   "headers": { ... },
   "body": "JSON string"
}
```

In this output, `statusCode` is typically 4XX for a client error and 5XX for a server error. API Gateway handles these errors by mapping the Lambda error to an HTTP error response, according to the specified
statusCode. For API Gateway to pass the error type (for example, `InvalidParameterException`), as part of the response to the client, the Lambda function must include a header (for example, "X-Amzn-ErrorType": "InvalidParameterException") in the headers property.

**Topics**
- Handle Standard Lambda Errors in API Gateway (p. 236)
- Handle Custom Lambda Errors in API Gateway (p. 237)

### Handle Standard Lambda Errors in API Gateway

A standard AWS Lambda error has the following format:

```json
{
  "errorMessage": "<replaceable>string</replaceable>",
  "errorType": "<replaceable>string</replaceable>",
  "stackTrace": [  
    "<replaceable>string</replaceable>",
    ...
  ]
}
```

Here, `errorMessage` is a string expression of the error. The `errorType` is a language-dependent error or exception type. The `stackTrace` is a list of string expressions showing the stack trace leading to the occurrence of the error.

For example, consider the following JavaScript (Node.js) Lambda function.

```javascript
exports.handler = function(event, context, callback) {
  callback(new Error("Malformed input ...");
};
```

This function returns the following standard Lambda error, containing `Malformed input ...` as the error message:

```json
{
  "errorMessage": "Malformed input ...",
  "errorType": "Error",
  "stackTrace": [
    "exports.handler (/var/task/index.js:3:14)"
  ]
}
```

Similarly, consider the following Python Lambda function, which raises an `Exception` with the same `Malformed input ...` error message.

```python
def lambda_handler(event, context):
  raise Exception('Malformed input ...')
```

This function returns the following standard Lambda error:

```json
{
  "stackTrace": [
    [  
      "/var/task/lambda_function.py",
      3,
      "lambda_handler",
      "raise Exception('Malformed input ...')"
    ]
  ]
}
```
Note that the errorType and stackTrace property values are language-dependent. The standard error also applies to any error object that is an extension of the Error object or a subclass of the Exception class.

To map the standard Lambda error to a method response, you must first decide on an HTTP status code for a given Lambda error. You then set a regular expression pattern on the selectionPattern property of the IntegrationResponse associated with the given HTTP status code. In the API Gateway console, this selectionPattern is denoted as Lambda Error Regex in the Integration Response configuration editor.

**Note**
API Gateway uses Java pattern-style regexes for response mapping. For more information, see Pattern in the Oracle documentation.

For example, to set up a new selectionPattern expression, using AWS CLI, call the following put-integration-response command:

```bash
aws apigateway put-integration-response --rest-api-id z0vprf0mdh --resource-id x3o5ih --http-method GET --status-code 400 --selection-pattern "Invalid*" --region us-west-2
```

Make sure that you also set up the corresponding error code (400) on the method response (p. 207). Otherwise, API Gateway throws an invalid configuration error response at runtime.

**Note**
At runtime, API Gateway matches the Lambda error's errorMessage against the pattern of the regular expression on the selectionPattern property. If there is a match, API Gateway returns the Lambda error as an HTTP response of the corresponding HTTP status code. If there is no match, API Gateway returns the error as a default response or throws an invalid configuration exception if no default response is configured.

Setting the selectionPattern value to .* for a given response amounts to resetting this response as the default response. This is because such a selection pattern will match all error messages, including null, i.e., any unspecified error message. The resulting mapping overrides the default mapping.

To update an existing selectionPattern value using the AWS CLI, call the update-integration-response operation to replace the /selectionPattern path value with the specified regex expression of the Malformed* pattern.

To set the selectionPattern expression using the API Gateway console, type the expression in the Lambda Error Regex text box when setting up or updating an integration response of a specified HTTP status code.

**Handle Custom Lambda Errors in API Gateway**

Instead of the standard error described in the preceding section, AWS Lambda allows you to return a custom error object as JSON string. The error can be any valid JSON object. For example, the following JavaScript (Node.js) Lambda function returns a custom error:

```javascript
exports.handler = (event, context, callback) => {
  ...
  // Error caught here:
  var myErrorObj = {
    errorType : "InternalServerError",
    httpStatus : 500,
    requestId : context.awsRequestId,
```
You must turn the `myErrorObj` object into a JSON string before calling `callback` to exit the function. Otherwise, the `myErrorObj` is returned as a string of `"[object Object]"`. When a method of your API is integrated with the preceding Lambda function, API Gateway receives an integration response with the following payload:

```
{
    "errorMessage": "{\"errorType\":\"InternalServerError\",\"httpStatus\":500,\"requestId\":\"e5849002-39a0-11e7-a419-5bb5807c9fb2\",\"trace\":{"\"function\":\"abc()\",\"line\":123,\"file\":\"abc.js\"}}"
}
```

As with any integration response, you can pass through this error response as-is to the method response. Or you can have a body-mapping template to transform the payload into a different format. For example, consider the following body-mapping template for a method response of 500 status code:

```
{
    errorMessage: $input.path('$.errorMessage');
}
```

This template translates the integration response body that contains the custom error JSON string to the following method response body. This method response body contains the custom error JSON object:

```
{
    "errorMessage": {
        errorType : "InternalServerError",
        httpStatus : 500,
        requestId : context.awsRequestId,
        trace : {
            "function": "abc()",
            "line": 123,
            "file": "abc.js"
        }
    }
}
```

Depending on your API requirements, you may need to pass some or all of the custom error properties as method response header parameters. You can achieve this by applying the custom error mappings from the integration response body to the method response headers.

For example, the following OpenAPI extension defines a mapping from the `errorMessage.errorType`, `errorMessage.httpStatus`, `errorMessage.trace.function`, and `errorMessage.trace` properties to the `error_type`, `error_status`, `error_trace_function`, and `error_trace` headers, respectively.

```
"x-amazon-apigateway-integration": {
    "responses": {
        "default": {
            "statusCode": "200",
            "responseParameters": {
                "method.response.header.error_trace_function": "integration.response.body.errorMessage.trace.function",
                "method.response.header.error_trace": "integration.response.body.errorMessage.trace",
                "method.response.header.error_status": "integration.response.body.errorMessage.httpStatus",
                "method.response.header.error_type": "integration.response.body.errorMessage.errorType"
            }
        }
    }
}
```
"method.response.header.error_status": "integration.response.body.errorMessage.httpStatus",
"method.response.header.error_type": "integration.response.body.errorMessage.errorType",
"method.response.header.error_trace": "integration.response.body.errorMessage.trace"
}
{
...
}
}

At runtime, API Gateway deserializes the integration.response.body parameter when performing header mappings. However, this deserialization applies only to body-to-header mappings for Lambda custom error responses and does not apply to body-to-body mappings using $input.body. With these custom-error-body-to-header mappings, the client receives the following headers as part of the method response, provided that the error_status, error_trace, error_trace_function, and error_type headers are declared in the method request.

"error_status":"500",
"error_trace": "{\"function\":\"abc()\",\"line\":123,\"file\":\"abc.js\"\"},
"error_trace_function":"abc()",
"error_type":"InternalServerError"

The errorMessage.trace property of the integration response body is a complex property. It is mapped to the error_trace header as a JSON string.

Set up HTTP Integrations in API Gateway

You can integrate an API method with an HTTP endpoint using the HTTP proxy integration or the HTTP custom integration.

API Gateway supports the following endpoint ports: 80, 443 and 1024-65535.

With proxy integration, setup is simple. You only need to set the HTTP method and the HTTP endpoint URI, according to the backend requirements, if you are not concerned with content encoding or caching.

With custom integration, setup is more involved. In addition to the proxy integration setup steps, you need to specify how the incoming request data is mapped to the integration request and how the resulting integration response data is mapped to the method response.

Topics
- Set up HTTP Proxy Integrations in API Gateway (p. 239)
- Set up HTTP Custom Integrations in API Gateway (p. 243)

Set up HTTP Proxy Integrations in API Gateway

To set up a proxy resource with the HTTP proxy integration type, create an API resource with a greedy path parameter (for example, /parent/{proxy+}) and integrate this resource with an HTTP backend endpoint (for example, https://petstore-demo-endpoint.execute-api.com/petstore/ {proxy}) on the ANY method. The greedy path parameter must be at the end of the resource path.

As with a non-proxy resource, you can set up a proxy resource with the HTTP proxy integration by using the API Gateway console, importing an OpenAPI definition file, or calling the API Gateway REST API directly. For detailed instructions about using the API Gateway console to configure a proxy resource with the HTTP integration, see TUTORIAL: Build an API with HTTP Proxy Integration (p. 51).

The following OpenAPI definition file shows an example of an API with a proxy resource that is integrated with the PetStore website.
OpenAPI 3.0

```json
{
  "openapi": "3.0.0",
  "info": {
    "version": "2016-09-12T23:19:28Z",
    "title": "PetStoreWithProxyResource"
  },
  "paths": {
    "/{proxy+}": {
      "x-amazon-apigateway-any-method": {
        "parameters": [
          {
            "name": "proxy",
            "in": "path",
            "required": true,
            "schema": {
              "type": "string"
            }
          }
        ],
        "responses": {},
        "x-amazon-apigateway-integration": {
          "responses": {
            "default": {
              "statusCode": "200"
            }
          },
          "requestParameters": {
            "integration.request.path.proxy": "method.request.path.proxy"
          },
          "url": "http://petstore-demo-endpoint.execute-api.com/petstore/{proxy}\",
          "passthroughBehavior": "when_no_match",
          "httpMethod": "ANY",
          "cacheNamespace": "rbftud",
          "cacheKeyParameters": [
            "method.request.path.proxy"
          ],
          "type": "http_proxy"
        }
      }
    }
  },
  "servers": [
    {
      "url": "https://4z9giyi2c1.execute-api.us-east-1.amazonaws.com/{basePath}\",
      "variables": {
        "basePath": {
          "default": "/test"
        }
      }
    }
  ]
}
```

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "version": "2016-09-12T23:19:28Z",
    "title": "PetStoreWithProxyResource"
  },
  "host": "4z9giyi2c1.execute-api.us-east-1.amazonaws.com",
  "schemes": [
    "https"
  ]
}
```
In this example, a cache key is declared on the `method.request.path.proxy` path parameter of the proxy resource. This is the default setting when you create the API using the API Gateway console. The API's base path (`/test`, corresponding to a stage) is mapped to the website's PetStore page (`/petstore`). The single integration request mirrors the entire PetStore website using the API's greedy path variable and the catch-all `ANY` method. The following examples illustrate this mirroring.

- **Set ANY as GET and `{proxy+}` as pets**

  Method request initiated from the frontend:

  ```
  GET https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test/pets HTTP/1.1
  ```

  Integration request sent to the backend:

  ```
  GET http://petstore-demo-endpoint.execute-api.com/petstore/pets HTTP/1.1
  ```

  The run-time instances of the `ANY` method and proxy resource are both valid. The call returns a 200 OK response with the payload containing the first batch of pets, as returned from the backend.
• **Set ANY as GET and \( \{proxy+\} \) as pets?type=dog**

```
GET https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test/pets?type=dog HTTP/1.1
```

Integration request sent to the backend:

```
GET http://petstore-demo-endpoint.execute-api.com/petstore/pets?type=dog HTTP/1.1
```

The run-time instances of the \( \text{ANY} \) method and proxy resource are both valid. The call returns a \( 200 \) \( \text{OK} \) response with the payload containing the first batch of specified dogs, as returned from the backend.

• **Set ANY as GET and \( \{proxy+\} \) as pets/{petId}**

Method request initiated from the frontend:

```
GET https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test/pets/1 HTTP/1.1
```

Integration request sent to the backend:

```
GET http://petstore-demo-endpoint.execute-api.com/petstore/pets/1 HTTP/1.1
```

The run-time instances of the \( \text{ANY} \) method and proxy resource are both valid. The call returns a \( 200 \) \( \text{OK} \) response with the payload containing the specified pet, as returned from the backend.

• **Set ANY as POST and \( \{proxy+\} \) as pets**

Method request initiated from the frontend:

```
POST https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test/pets HTTP/1.1
Content-Type: application/json
Content-Length: ...

{  
  "type" : "dog",
  "price" : 1001.00
}
```

Integration request sent to the backend:

```
POST http://petstore-demo-endpoint.execute-api.com/petstore/pets HTTP/1.1
Content-Type: application/json
Content-Length: ...

{  
  "type" : "dog",
  "price" : 1001.00
}
```

The run-time instances of the \( \text{ANY} \) method and proxy resource are both valid. The call returns a \( 200 \) \( \text{OK} \) response with the payload containing the newly created pet, as returned from the backend.

• **Set ANY as GET and \( \{proxy+\} \) as pets/cat**

Method request initiated from the frontend:

```
GET https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test/pets/cat
```

242
Integration request sent to the backend:

```
GET http://petstore-demo-endpoint.execute-api.com/petstore/pets/cat
```

The run-time instance of the proxy resource path does not correspond to a backend endpoint and the resulting request is invalid. As a result, a 400 Bad Request response is returned with the following error message.

```
{
  "errors": [
    {
      "key": "Pet2.type",
      "message": "Missing required field"
    },
    {
      "key": "Pet2.price",
      "message": "Missing required field"
    }
  ]
}
```

- **Set ANY as GET and (proxy+) as null**

Method request initiated from the frontend:

```
GET https://4z9giyi2c1.execute-api.us-west-2.amazonaws.com/test
```

Integration request sent to the backend:

```
GET http://petstore-demo-endpoint.execute-api.com/petstore/pets
```

The targeted resource is the parent of the proxy resource, but the run-time instance of the ANY method is not defined in the API on that resource. As a result, this GET request returns a 403 Forbidden response with the Missing Authentication Token error message as returned by API Gateway. If the API exposes the ANY or GET method on the parent resource (/), the call returns a 404 Not Found response with the Cannot GET /petstore message as returned from the backend.

For any client request, if the targeted endpoint URL is invalid or the HTTP verb is valid but not supported, the backend returns a 404 Not Found response. For an unsupported HTTP method, a 403 Forbidden response is returned.

**Set up HTTP Custom Integrations in API Gateway**

With the HTTP custom integration, you have more control of which data to pass between an API method and an API integration and how to pass the data. You do this using data mappings.

As part of the method request setup, you set the `requestParameters` property on a `Method` resource. This declares which method request parameters, which are provisioned from the client, are to be mapped to integration request parameters or applicable body properties before being dispatched to the backend. Then, as part of the integration request setup, you set the `requestParameters` property on the corresponding `Integration` resource to specify the parameter-to-parameter mappings. You also set the `requestTemplates` property to specify mapping templates, one for each supported content type. The mapping templates map method request parameters, or body, to the integration request body.

Similarly, as part of the method response setup, you set the `responseParameters` property on the `MethodResponse` resource. This declares which method response parameters, to be dispatched to the
client, are to be mapped from integration response parameters or certain applicable body properties that were returned from the backend. Then, as part of the integration response setup, you set the responseParameters property on the corresponding IntegrationResponse resource to specify the parameter-to-parameter mappings. You also set the responseTemplates map to specify mapping templates, one for each supported content type. The mapping templates map integration response parameters, or integration response body properties, to the method response body.

For more information about setting up mapping templates, see Set up Data Mappings. (p. 259)

Set up API Gateway Private Integrations

The API Gateway private integration makes it simple to expose your HTTP/HTTPS resources behind an Amazon VPC for access by clients outside of the VPC. To extend access to your private VPC resources beyond the VPC boundaries, you can create an API with private integration for open access or controlled access. You can do this by using IAM permissions, a Lambda authorizer, or an Amazon Cognito user pool.

The private integration uses an API Gateway resource of VpcLink to encapsulate connections between API Gateway and targeted VPC resources. As an owner of a VPC resource, you are responsible for creating a network load balancer in your VPC and adding a VPC resource as a target of a network load balancer's listener. As an API developer, to set up an API with the private integration, you are responsible for creating a VpcLink targeting specified network load balancers and then treating the VpcLink as an effective integration endpoint.

With the API Gateway private integration, you can enable access to HTTP/HTTPS resources within a VPC without detailed knowledge of private network configurations or technology-specific appliances.

Topics

- Set up a Network Load Balancer for API Gateway Private Integrations (p. 244)
- Grant Permissions to Create a VPC Link (p. 245)
- Set up an API Gateway API with Private Integrations Using the API Gateway Console (p. 245)
- Set up an API Gateway API with Private Integrations Using the AWS CLI (p. 245)
- Set up API with Private Integrations Using OpenAPI (p. 249)

Set up a Network Load Balancer for API Gateway Private Integrations

The following procedure outlines the steps to set up a network load balancer (NLB) for API Gateway private integrations using the Amazon EC2 console and provides references for detailed instructions for each step.

For each VPC you have resources in, you only need to configure one NLB and one VPCLink. The NLB supports multiple listeners and target groups per NLB. You can configure each service as a specific listener on the NLB and use a single VPCLink to connect to the NLB. When creating the private integration in API Gateway you then define each service using the specific port that is assigned for each service. For more information, see the section called “TUTORIAL: Build an API with Private Integration” (p. 85).

To create a network load balancer for private integration using the API Gateway console

1. Sign in to the Amazon EC2 console at https://console.aws.amazon.com/ec2/ and choose a region; for example, us-east-1, on the navigation bar.
2. Set up a web server on an Amazon EC2 instance. For an example setup, see Installing a LAMP Web Server on Amazon Linux.
3. Create a network load balancer, register the EC2 instance with a target group, and add the target group to a listener of the network load balancer. For details, follow the instructions in Getting Started with Network Load Balancers.
After the network load balancer is created, note its ARN. You will need it to create a VPC link in API Gateway for integrating the API with the VPC resources behind the network load balancer.

Grant Permissions to Create a VPC Link

For you or a user in your account to create and maintain a VPC link, you or the user must have permissions to create, delete, and view VPC endpoint service configurations, change VPC endpoint service permissions, and examine load balancers. To grant such permissions, use the following steps.

To grant permissions to create and update a VpcLink

1. Create an IAM policy similar to the following:

   ```json
   {
     "Version":"2012-10-17",
     "Statement":[
       {
         "Effect":"Allow",
         "Action":[
           "ec2:CreateVpcEndpointServiceConfiguration",
           "ec2:DeleteVpcEndpointServiceConfigurations",
           "ec2:DescribeVpcEndpointServiceConfigurations",
           "ec2:ModifyVpcEndpointServicePermissions"
         ],
         "Resource":"*"
       },
       {
         "Effect":"Allow",
         "Action":[
           "elasticloadbalancing:DescribeLoadBalancers"
         ],
         "Resource":"*"
       }
     ]
   }
   ```

2. Create or choose an IAM role and attach the preceding policy to the role.
3. Assign the IAM role to you or a user in your account who is creating VPC links.

Set up an API Gateway API with Private Integrations Using the API Gateway Console

For instructions using the API Gateway Console to set up an API with private integration, see TUTORIAL: Build an API with API Gateway Private Integration (p. 85).

Set up an API Gateway API with Private Integrations Using the AWS CLI

Before creating an API with the private integration, you must have your VPC resource set up and a network load balancer created and configured with your VPC source as the target. If the requirements are not met, follow Set up a Network Load Balancer for API Gateway Private Integrations (p. 244) to install the VPC resource, create a NLB, set the VPC resource as a target of the network load balancer.

For you to be able to create and manage a VpcLink, you must also have the appropriate permissions configured. For more information, see Grant Permissions to Create a VPC Link (p. 245).

**Note**

You only need the permissions to create a VpcLink in your API. You do not need the permissions to use the VpcLink.
After the network load balancer is created, note its ARN. You need it to create a VPC link for the private integration.

**To set up an API with the private integration using AWS CLI**

1. Create a `VpcLink` targeting the specified network load balancer.

   For this discussion, we assume the ARN of the network load balancer is

   ```bash
   aws apigateway create-vpc-link 
   --name my-test-vpc-link 
   --target-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/my-vpclink-test-nlb/1f8df693cd094a72 
   --endpoint-url https://apigateway.us-east-1.amazonaws.com 
   --region us-east-1
   ``

   If the AWS configuration uses `us-east-1` as the default region, you can skip the `endpoint-url` and `region` parameters in the preceding input.

   The preceding command immediately returns the following response, acknowledging the receipt of the request, and showing the `PENDING` status for the `VpcLink` being created.

   ```json
   {
   "status": "PENDING",
   "targetArns": [
   "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/my-vpclink-test-nlb/1f8df693cd094a72"
   ],
   "id": "gim7c3",
   "name": "my-test-vpc-link"
   }
   ``

   It takes 2-4 minutes for API Gateway to finish creating the `VpcLink`. When the operation finishes successfully, the status is `AVAILABLE`. You can verify this by calling the following CLI command:

   ```bash
   aws apigateway get-vpc-link --vpc-link-id gim7c3
   ```

   If the operation fails, you get a `FAILED` status, with the `statusMessage` containing the error message. For example, if you attempt to create a `VpcLink` with a network load balancer that is already associated with a VPC endpoint, you get the following on the `statusMessage` property:

   ```json
   "NLB is already associated with another VPC Endpoint Service"
   ``

   Only after the `VpcLink` is created successfully are we ready to create the API and integrate it with the VPC resource through the `VpcLink`.

   Note the `id` value of the newly created `VpcLink` (gim7c3 in the preceding output). You need it to set up the private integration.

2. Set up an API by creating an API Gateway `RestApi` resource:

   ```bash
   aws apigateway create-rest-api --name 'My VPC Link Test'
   ```

   We have dropped the input parameters of `endpoint-url` and `region` to use the default region as specified in the AWS configuration.
Note the RestApi's id value in the returned result. In this example, we assume it is 6j4m3244we. You need this value to perform further operations on the API, including setting up methods and integrations.

For illustration purposes, we will create an API with only a GET method on the root resource (/) and integrate the method with the VpcLink.

3. Set up the GET / method. First get the identifier of the root resource (/):

```bash
aws apigateway get-resources --rest-api-id 6j4m3244we
```

In the output, note the id value of the / path. In this example, we assume it to be skpp60rab7.

Set up the method request for the API method of GET /:

```bash
aws apigateway put-method
  --rest-api-id 6j4m3244we
  --resource-id skpp60rab7
  --http-method GET
  --authorization-type "NONE"
```

To use the IAM permissions, a Lambda authorizer, or an Amazon Cognito user pool to authenticate the caller, set the authorization-type to AWS_IAM, CUSTOM, or COGNITO_USER_POOLS, respectively.

If you do not use the proxy integration with the VpcLink, you must also set up at least a method response of the 200 status code. We will use the proxy integration here.

4. Set up the private integration of the HTTP_PROXY type and call the put-integration command as follows:

```bash
aws apigateway put-integration
  --rest-api-id 6j4m3244we
  --resource-id skpp60rab7
  --uri 'http://myApi.example.com'
  --http-method GET
  --type HTTP_PROXY
  --integration-http-method GET
  --connection-type VPC_LINK
  --connection-id gim7c3
```

For a private integration, you must set connection-type to VPC_LINK and set connection-id to either your VpcLink's identifier or a stage variable referencing your VpcLink ID. The uri parameter is not used for routing requests to your endpoint, but is used for setting the Host header and for certificate validation.

If successful, the command returns the following output:

```json
{
    "passthroughBehavior": "WHEN_NO_MATCH",
    "timeoutInMillis": 29000,
    "connectionId": "gim7c3",
    "uri": "http://myApi.example.com",
    "httpMethod": "GET",
    "connectionType": "VPC_LINK",
    "cacheNamespace": "skpp60rab7",
    "type": "HTTP_PROXY",
    "cacheKeyParameters": []
}
```
Using a stage variable, you set the `connectionId` property when creating the integration:

```bash
aws apigateway put-integration \
  --rest-api-id 6j4m3244we \
  --resource-id skpp60rab7 \
  --uri 'http://myApi.example.com' \
  --http-method GET \
  --type HTTP_PROXY \
  --integration-http-method GET \
  --connection-type VPC_LINK \
  --connection-id "\${stageVariables.vpcLinkId}"
```

Make sure to double-quote the stage variable expression (`${stageVariables.vpcLinkId}`) and escape the `$` character.

Alternatively, you can update the integration to reset the `connectionId` value with a stage variable:

```bash
aws apigateway update-integration \
  --rest-api-id 6j4m3244we \
  --resource-id skpp60rab7 \
  --http-method GET \
  --patch-operations '[["op":"replace","path":"/connectionId","value":"\${stageVariables.vpcLinkId}"]]'
```

Make sure to use a stringified JSON list as the `patch-operations` parameter value.

Using a stage variable to set the `connectionId` value has the advantage of having the same API integrated with different VpcLinks by resetting the stage variable value. This is useful for switching your API to a different VPC link to migrate to a different network load balancer or a different VPC.

Because we used the private proxy integration, the API is now ready for deployment and for test runs. With the non-proxy integration, you must also set up the method response and integration response, just as you would when setting up an API with HTTP custom integrations (p. 57).

5. To test the API, deploy the API. This is necessary if you have used the stage variable as a placeholder of the VpcLink ID. To deploy the API with a stage variable, call the `create-deployment` command as follows:

```bash
aws apigateway create-deployment \
  --rest-api-id 6j4m3244we \
  --stage-name test \
  --variables vpcLinkId=gim7c3
```

To update the stage variable with a different VpcLink ID (e.g., asf9d7), call the `update-stage` command:

```bash
aws apigateway update-stage \
  --rest-api-id 6j4m3244we \
  --stage-name test \
  --patch-operations op=replace,path='/variables/vpcLinkId',value='asf9d7'
```

To test the API, invoke it using the following cURL command:

```bash
curl -X GET https://6j4m3244we.beta.execute-api.us-east-1.amazonaws.com/test
```

Alternatively, you can type the API's invoke-URL in a web browser to view the result.
When you hardcode the connection-id property with the VpcLink ID literal, you can also call test-invoke-method to test invoking the API before it is deployed.

Set up API with Private Integrations Using OpenAPI

You can set up an API with the private integration by importing the API's OpenAPI file. The settings are similar to the OpenAPI definitions of an API with HTTP integrations, with the following exceptions:

- You must explicitly set connectionType to VPC_LINK.
- You must explicitly set connectionId to the ID of a VpcLink or to a stage variable referencing the ID of a VpcLink.
- The uri parameter in the private integration points to an HTTP/HTTPS endpoint in the VPC, but is used instead to set up the integration request's Host header.
- The uri parameter in the private integration with an HTTPS endpoint in the VPC is used to verify the stated domain name against the one in the certificate installed on the VPC endpoint.

You can use a stage variable to reference the VpcLink ID. Or you can assign the ID value directly to connectionId.

The following JSON-formatted OpenAPI file shows an example of an API with a VPC link as referenced by a stage variable (stageVariables.vpcLinkId):

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "version": "2017-11-17T04:40:23Z",
    "title": "MyApiWithVpcLink"
  },
  "host": "p3wocvip9a.execute-api.us-west-2.amazonaws.com",
  "basePath": "/test",
  "schemes": ["https"],
  "paths": {
    
    "/": {
      "get": {
        "Produces": [
          "application/json"
        ],
        "responses": {
          "200": {
            "description": "200 response",
            "schema": {
              "$ref": "#/definitions/Empty"
            }
          }
        }
      },
      "x-amazon-apigateway-integration": {
        "responses": {
          "default": {
            "statusCode": "200"
          }
        },
        "uri": "http://myApi.example.com",
        "passthroughBehavior": "when_no_match",
        "connectionType": "VPC_LINK",
        "connectionId": "stageVariables.vpcLinkId"
      }
    }
  }
}
```
Set up Mock Integrations in API Gateway

Amazon API Gateway supports mock integrations for API methods. This feature enables API developers to generate API responses from API Gateway directly, without the need for an integration backend. As an API developer, you can use this feature to unblock dependent teams that need to work with an API before the project development is complete. You can also use this feature to provision a landing page for your API, which can provide an overview of and navigation to your API. For an example of such a landing page, see the integration request and response of the GET method on the root resource of the example API discussed in TUTORIAL: Create a REST API by Importing an Example (p. 42).

As an API developer, you decide how API Gateway responds to a mock integration request. For this, you configure the method's integration request and integration response to associate a response with a given status code. For a method with the mock integration to return a 200 response, configure the integration request body mapping template to return the following.

```
{"statusCode": 200}
```

Configure a 200 integration response to have the following body mapping template, for example:

```
{
   "statusCode": 200,
   "message": "Go ahead without me."
}
```

Similarly, for the method to return, for example, a 500 error response, set up the integration request body mapping template to return the following.

```
{"statusCode": 500}
```

Set up a 500 integration response with, for example, the following mapping template:

```
{
   "statusCode": 500,
   "message": "The invoked method is not supported on the API resource."
}
```

Alternatively, you can have a method of the mock integration return the default integration response without defining the integration request mapping template. The default integration response is the one with an undefined HTTP status regex. Make sure appropriate passthrough behaviors are set.

**Note**
Mock integrations aren't intended to support large response templates. If you need them for your use case, you should consider using a Lambda integration instead.
Using an integration request mapping template, you can inject application logic to decide which mock integration response to return based on certain conditions. For example, you could use a `scope` query parameter on the incoming request to determine whether to return a successful response or an error response:

```json
{
    //if( $input.params('scope') == "internal" )
    "statusCode": 200
    //else
    //  "statusCode": 500
    //end
}
```

This way, the method of the mock integration lets internal calls to go through while rejecting other types of calls with an error response.

In this section, we describe how to use the API Gateway console to enable the mock integration for an API method.

**Topics**

- Enable Mock Integration Using the API Gateway Console (p. 251)

### Enable Mock Integration Using the API Gateway Console

You must have the method available in API Gateway. Follow the instructions in TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).

1. Choose an API resource and create a method. In the method **Setup** pane, choose **Mock** for **Integration type**, and then choose **Save**.
2. Choose **Method Request** from **Method Execution**. Expand **URL Query String Parameters**. Choose **Add query string** to add a `scope` query parameter. This determines if the caller is internal or otherwise.
3. Choose **Integration Request** from **Method Execution**. Expand **Body Mapping Templates**. Choose or add an **application/json** mapping template. Type the following in the template editor:

```json
{
    //if( $input.params('scope') == "internal" )
    "statusCode": 200
    //else
    //  "statusCode": 500
    //end
}
```

Choose **Save**.

4. Choose **Integration Response** from **Method Execution**. Expand the **200** response and then the **Body Mapping Templates** section. Choose or add an application/json mapping template and type the following response body mapping template in the template editor:

```json
{
    "statusCode": 200,
    "message": "Go ahead without me"
}
```

Choose **Save**.

5. Scroll to **Integration Response**. Choose **Add integration response** to add a 500 response. Type `5\d{2}` in **HTTP status regex**. Expand **Body Mapping Templates** and choose **Add mapping**.
template. Type application/json for Content-Type and then choose the check mark icon to save the setting. In the template editor, type the following integration response body mapping template:

```json
{
  "statusCode": 500,
  "message": "The invoked method is not supported on the API resource."
}
```

Choose Save.

6. Choose Test from Method Execution. Do the following:

a. Type internal under scope. Choose Test. The test result shows:

```
Request: /?scope=internal
Status: 200
Latency: 26 ms
Response Body
{
  "statusCode": 200,
  "message": "Go ahead without me"
}
Response Headers
{"Content-Type":"application/json"}
```

b. Type public under scope or leave it blank. Choose Test. The test result shows:

```
Request: /
Status: 500
Latency: 16 ms
Response Body
{
  "statusCode": 500,
  "message": "The invoked method is not supported on the API resource."
}
Response Headers
{"Content-Type":"application/json"}
```

You can also return headers in a mock integration response by first adding a header to the method response and then setting up a header mapping in the integration response. In fact, this is how the API Gateway console enables CORS support by returning CORS required headers.

**Set up Gateway Responses to Customize Error Responses**

If API Gateway fails to process an incoming request, it returns to the client an error response without forwarding the request to the integration backend. By default, the error response contains a short descriptive error message. For example, if you attempt to call an operation on an undefined API resource, you receive an error response with the

```
{
  "message": "Missing Authentication Token"
}
```
message. If you are new to API Gateway, you may find it difficult to understand what actually went wrong.

For some of the error responses, API Gateway allows customization by API developers to return the responses in different formats. For the Missing Authentication Token example, you can add a hint to the original response payload with the possible cause, as in this example: {"message":"Missing Authentication Token", "hint":"The HTTP method or resources may not be supported."}.

When your API mediates between an external exchange and the AWS cloud, you use VTL mapping templates for integration request or integration response to map the payload from one format to another. However, the VTL mapping templates work only for valid requests with successful responses. For invalid requests, API Gateway bypasses the integration altogether and returns an error response. You must use the customization to render the error responses in an exchange-compliant format. Here, the customization is rendered in a non-VTL mapping template supporting only simple variable substitutions.

Generalizing the API Gateway-generated error response to any responses generated by API Gateway, we refer to them as gateway responses. This distinguishes API Gateway-generated responses from the integration responses. A gateway response mapping template can access $context variable values and $stageVariables property values, as well as method request parameters, in the form of method.request.param-position.param-name. For more information about $context variables, see $context Variables for Data Models, Authorizers, Mapping Templates, and CloudWatch Access Logging (p. 293). For more information about $stageVariables, see $stageVariables (p. 302). For more information about method request parameters, see Request parameters accessible by a mapping template (p. 289).

Topics
- Gateway Responses in API Gateway (p. 253)
- Gateway Response Types (p. 253)
- Set up a Gateway Response Using the API Gateway Console (p. 257)
- Set up a Gateway Response Using the API Gateway REST API (p. 258)
- Set up Gateway Response Customization in OpenAPI (p. 259)

Gateway Responses in API Gateway

A gateway response is identified by a response type defined by API Gateway. The response consists of an HTTP status code, a set of additional headers that are specified by parameter mappings, and a payload that is generated by a non-VTL mapping template.

In the API Gateway REST API, a gateway response is represented by the GatewayResponse. In OpenAPI, a GatewayResponse instance is described by the x-amazon-apigateway-gateway- responses.gatewayResponse (p. 583) extension.

To enable a gateway response, you set up a gateway response for a supported response type (p. 253) at the API level. Whenever API Gateway returns a response of the type, the header mappings and payload mapping templates defined in the gateway response are applied to return the mapped results to the API caller.

In the following section, we show how to set up gateway responses using the API Gateway console and the API Gateway REST API.

Gateway Response Types

API Gateway exposes the following gateway responses for customization by API developers.
<table>
<thead>
<tr>
<th>Gateway response type</th>
<th>Default status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_DENIED</td>
<td>403</td>
<td>The gateway response for authorization failure; for example, when access is denied by a custom or Amazon Cognito authorizer. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>API_CONFIGURATION_ERROR</td>
<td>500</td>
<td>The gateway response for invalid API configuration, including invalid endpoint address submitted, Base64 decoding failed on binary data when binary support is enacted, or integration response mapping cannot match any template and no default template is configured. If the response type is unspecified, this response defaults to the DEFAULT_5XX type.</td>
</tr>
<tr>
<td>AUTHORIZER_CONFIGURATION_ERROR</td>
<td></td>
<td>The gateway response for failing to connect to a custom or Amazon Cognito authorizer. If the response type is unspecified, this response defaults to the DEFAULT_5XX type.</td>
</tr>
<tr>
<td>AUTHORIZER_FAILURE</td>
<td>500</td>
<td>The gateway response when a custom or Amazon Cognito authorizer failed to authenticate the caller. If the response type is unspecified, this response defaults to the DEFAULT_5XX type.</td>
</tr>
<tr>
<td>BAD_REQUEST_PARAMETERS</td>
<td>400</td>
<td>The gateway response when the request parameter cannot be validated according to an enabled request validator. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>BAD_REQUEST_BODY</td>
<td>400</td>
<td>The gateway response when the request body cannot be validated according to an enabled request validator. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>DEFAULT_4XX</td>
<td>Null</td>
<td>The default gateway response for an unspecified response type.</td>
</tr>
<tr>
<td>Gateway response type</td>
<td>Default status code</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DEFAULT_4XX</td>
<td>403</td>
<td>The gateway response for an invalid API key submitted for a method requiring an API key. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>INTEGRATION_FAILURE</td>
<td>504</td>
<td>The gateway response for an integration failed error. If the response type is unspecified, this response defaults to the DEFAULT_5XX type.</td>
</tr>
<tr>
<td>INTEGRATION_TIMEOUT</td>
<td>504</td>
<td>The gateway response for an integration timed out error. If the response type is unspecified, this response defaults to the DEFAULT_5XX type.</td>
</tr>
<tr>
<td>INVALID_API_KEY</td>
<td>403</td>
<td>The gateway response for an invalid API key submitted for a method requiring an API key. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>INVALID_SIGNATURE</td>
<td>403</td>
<td>The gateway response for an invalid AWS signature error. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>EXPIRED_TOKEN</td>
<td>403</td>
<td>The gateway response for an AWS authentication token expired error. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>DEFAULT_5XX</td>
<td>Null</td>
<td>The default gateway response for an unspecified response type with a status code of 5XX. Changing the status code of this fallback gateway response changes the status codes of all other 5XX responses to the new value. Resetting this status code to null reverts the status codes of all other 5XX responses to their original values.</td>
</tr>
</tbody>
</table>

With the status code of 4XX. Changing the status code of this fallback gateway response changes the status codes of all other 4XX responses to the new value. Resetting this status code to null reverts the status codes of all other 4XX responses to their original values.
<table>
<thead>
<tr>
<th>Gateway response type</th>
<th>Default status code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MISSING_AUTHENTICATION_TOKEN</td>
<td>403</td>
<td>The gateway response for a missing authentication token error, including the cases when the client attempts to invoke an unsupported API method or resource. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>QUOTA_EXCEEDED</td>
<td>429</td>
<td>The gateway response for the usage plan quota exceeded error. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>REQUEST_TOO_LARGE</td>
<td>413</td>
<td>The gateway response for the request too large error. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>RESOURCE_NOT_FOUND</td>
<td>404</td>
<td>The gateway response when API Gateway cannot find the specified resource after an API request passes authentication and authorization, except for API key authentication and authorization. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>THROTTLED</td>
<td>429</td>
<td>The gateway response when usage plan-, method-, stage-, or account-level throttling limits exceeded. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
<tr>
<td>UNAUTHORIZED</td>
<td>401</td>
<td>The gateway response when the custom or Amazon Cognito authorizer failed to authenticate the caller.</td>
</tr>
<tr>
<td>UNSUPPORTED_MEDIA_TYPE</td>
<td>415</td>
<td>The gateway response when a payload is of an unsupported media type, if strict passthrough behavior is enabled. If the response type is unspecified, this response defaults to the DEFAULT_4XX type.</td>
</tr>
</tbody>
</table>
Set up a Gateway Response Using the API Gateway Console

To customize a gateway response using the API Gateway console

1. Sign in to the API Gateway console.
2. Choose your existing API or create a new one.
3. Expand the API in the primary navigation pane and choose Gateway Responses under the API.
4. In the Gateway Responses pane, choose a response type. In this walkthrough, we use Missing Authentication Token (403) as an example.
5. You can change the API Gateway-generated Status Code to return a different status code that meets your API's requirements. In this example, the customization changes the status code from the default (403) to 404 because this error message occurs when a client calls an unsupported or invalid resource that can be thought of as not found.
6. To return custom headers, choose Add Header under Response Headers. For illustration purposes, we add the following custom headers:

   - Access-Control-Allow-Origin:'a.b.c'
   - x-request-id:method.request.header.x-amzn-RequestId
   - x-request-path:method.request.path.petId
   - x-request-query:method.request.querystring.q

   In the preceding header mappings, a static domain name ('a.b.c') is mapped to the Allow-Control-Allow-Origin header to allow CORS access to the API; the input request header of x-amzn-RequestId is mapped to request-id in the response; the petId path variable of the incoming request is mapped to the request-path header in the response; and the q query parameter of the original request is mapped to the request-query header of the response.
7. Under Body Mapping Templates, leave application/json for Content Type and type the following body mapping template in the Body Mapping Template editor:

   ```json
   {
       "message":"$context.error.messageString",
       "type": "$context.error.responseType",
       "statusCode": "404",
       "stage": "$context.stage",
       "resourcePath": "$context.resourcePath",
       "stageVariables.a": "$stageVariables.a"
   }
   ```

   This example shows how to map $context and $stageVariables properties to properties of the gateway response body.
8. Choose Save.
9. Deploy the API to a new or existing stage.
10. Test it by calling the following CURL command, assuming the corresponding API method's Invoke URL is `https://o81lxisefl.execute-api.us-east-1.amazonaws.com/custErr/pets/{petId}:

```
curl -v -H 'x-amzn-RequestId:123344566' https://o81lxisefl.execute-api.us-east-1.amazonaws.com/custErr/pets/5/type?q=1
```

Because the extra query string parameter `q=1` is not compatible with the API, An error is returned to trigger the specified gateway response. You should get a gateway response similar to the following:

```
> GET /custErr/pets/5?q=1 HTTP/1.1
Host: o81lxisefl.execute-api.us-east-1.amazonaws.com
User-Agent: curl/7.51.0
Accept: */*

HTTP/1.1 404 Not Found
Content-Type: application/json
Content-Length: 334
Connection: keep-alive
Date: Tue, 02 May 2017 03:15:47 GMT
x-amzn-RequestId: a2be05a4-2ee5-11e7-bbf2-df131ec50ae6
Access-Control-Allow-Origin: a.b.c
x-amzn-ErrorType: MissingAuthenticationTokenException
header-1: static
x-request-query: 1
x-request-path: 5
x-request-body: 
X-Cache: Error from cloudfront
Via: 1.1 441811a054e8d055b893175754ef0c3.cloudfront.net (CloudFront)
X-Amz-Cf-Id: nNDR-fX4csbRoAgTQ16u0rTDBz9FZWT-Mk93KgoxnfsDltUlh3f1mzA==

{
  "message":"Missing Authentication Token",
  "type": "MISSING_AUTHENTICATION_TOKEN",
  "statusCode": "404",
  "stage": "custErr",
  "resourcePath": "/pets/{petId}"
}
```

The preceding example assumes that the API backend is Pet Store and the API has a stage variable, `a`, defined.

**Set up a Gateway Response Using the API Gateway REST API**

Before customizing a gateway response using the API Gateway REST API, you must have already created an API and have obtained its identifier. To retrieve the API identifier, you can follow `restapi:gateway-responses` link relation and examine the result.

**To customize a gateway response using the API Gateway REST API**

1. To overwrite an entire `GatewayResponse` instance, call the `gatewayresponse:put` action, specifying a desired `responseType` in the URL path parameter and supplying in the request payload the `statusCode`, `responseParameters` and `responseTemplates` mappings.

2. To update part of a `GatewayResponse` instance, call the `gatewayresponse:update` action, specifying a desired `responseType` in the URL path parameter and supplying in the request payload desired individual `GatewayResponse` properties, for example, the `responseParameters` or the `responseTemplates` mapping.
Set up Gateway Response Customization in OpenAPI

You can use the x-amazon-apigateway-gateway-responses extension at the API root level to customize gateway responses in OpenAPI. The following OpenAPI definition shows an example for customizing the GatewayResponse of the MISSING_AUTHENTICATION_TOKEN type.

```
"x-amazon-apigateway-gateway-responses": {
    "MISSING_AUTHENTICATION_TOKEN": {
        "statusCode": 404,
        "responseParameters": {
            "gatewayresponse.header.x-request-path": "method.input.params.petId",
            "gatewayresponse.header.x-request-query": "method.input.params.q",
            "gatewayresponse.header.Access-Control-Allow-Origin": "'a.b.c'",
            "gatewayresponse.header.x-request-header": "method.input.params.Accept"
        },
        "responseTemplates": {
            "application/json": "{\n                "message": $context.error.messageString,
                "type": "$context.error.responseType",
                "stage": "$context.stage",
                "resourcePath": "$context.resourcePath",
                "$stageVariables.a": "$stageVariables.a",
                "statusCode": "'404'"\n            }\n        }
    }
}
```

In this example, the customization changes the status code from the default (403) to 404. It also adds to the gateway response four header parameters and one body mapping template for the application/json media type.

Set up API Gateway Request and Response Data Mappings

**Topics**
- Set up Request and Response Data Mappings Using the API Gateway Console (p. 259)
- Create Models and Mapping Templates for Request and Response Mappings (p. 262)
- Amazon API Gateway API Request and Response Data Mapping Reference (p. 289)
- API Gateway Mapping Template and Access Logging Variable Reference (p. 293)

Set up Request and Response Data Mappings Using the API Gateway Console

To use the API Gateway console to define the API's integration request/response, follow these instructions.

**Note**
These instructions assume you have already completed the steps in Set up an API Integration Request Using the API Gateway Console (p. 216).

1. With the method selected in the **Resources** pane, in the **Method Execution** pane, choose **Integration Request**.
2. For an HTTP proxy or an AWS service proxy, to associate a path parameter, a query string parameter, or a header parameter defined in the integration request with a corresponding path parameter, query string parameter, or header parameter in the method request of the HTTP proxy or AWS service proxy, do the following:
a. Choose the arrow next to **URL Path Parameters, URL Query String Parameters, or HTTP Headers** respectively, and then choose **Add path, Add query string, or Add header**, respectively.

b. For **Name**, type the name of the path parameter, query string parameter, or header parameter in the HTTP proxy or AWS service proxy.

c. For **Mapped from**, type the mapping value for the path parameter, query string parameter, or header parameter. Use one of the following formats:

   - **method.request.path.**parameter-name for a path parameter named parameter-name as defined in the Method Request page.
   - **method.request.querystring.**parameter-name for a query string parameter named parameter-name as defined in the Method Request page.
   - **method.request.multivaluequerystring.**parameter-name for a multi-valued query string parameter named parameter-name as defined in the Method Request page.
   - **method.request.header.**parameter-name for a header parameter named parameter-name as defined in the Method Request page.

   Alternatively, you can set a literal string value (enclosed by a pair of single quotes) to an integration header.

   - **method.request.multivalueheader.**parameter-name for a multi-valued header parameter named parameter-name as defined in the Method Request page.

d. Choose **Create**. (To delete a path parameter, query string parameter, or header parameter, choose **Cancel** or **Remove** next to the parameter you want to delete.)

3. In the **Body Mapping Templates** area, choose an option for **Request body passthrough** to configure how the method request body of an unmapped content type will be passed through the integration request without transformation to the Lambda function, HTTP proxy, or AWS service proxy. There are three options:

   - Choose **When no template matches the request Content-Type header** if you want the method request body to pass through the integration request to the backend without transformation when the method request content type does not match any content types associated with the mapping templates, as defined in the next step.

     **Note**
     When calling the API Gateway API, you choose this option by setting **WHEN_NO_MATCH** as the `passthroughBehavior` property value on the Integration resource.

   - Choose **When there are no templates defined (recommended)** if you want the method request body to pass through the integration request to the backend without transformation when no mapping template is defined in the integration request. If a template is defined when this option is selected, the method request of an unmapped content type will be rejected with an HTTP 415 Unsupported Media Type response.

     **Note**
     When calling the API Gateway API, you choose this option by setting **WHEN_NO_TEMPLATE** as the `passthroughBehavior` property value on the Integration resource.

   - Choose **Never** if you do not want the method request to pass through when either the method request content type does not match any content type associated with the mapping templates defined in the integration request or no mapping template is defined in the integration request. The method request of an unmapped content type will be rejected with an HTTP 415 Unsupported Media Type response.

     **Note**
     When calling the API Gateway API, you choose this option by setting **NEVER** as the `passthroughBehavior` property value on the Integration resource.
For more information about the integration passthrough behaviors, see Integration Passthrough Behaviors (p. 292).

4. To define a mapping template for an incoming request, choose Add mapping template under Content-Type. Type a content type (e.g., application/json) in the input text box and then choose the check mark icon to save the input. Then, type the mapping template manually or choose Generate template to create one from a model template. For more information, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

5. You can map an integration response from the backend to a method response of the API returned to the calling app. This includes returning to the client selected response headers from the available ones from the backend, transforming the data format of the backend response payload to an API-specified format. You can specify such mapping by configuring Method Response and Integration Response from the Method Execution page.

a. In the Method Execution pane, choose Integration Response. Choose either the arrow next to 200 to specify settings for a 200 HTTP response code from the method, or choose Add integration response to specify settings for any other HTTP response status code from the method.

b. For Lambda error regex (for a Lambda function) or HTTP status regex (for an HTTP proxy or AWS service proxy), type a regular expression to specify which Lambda function error strings (for a Lambda function) or HTTP response status codes (for an HTTP proxy or AWS service proxy) map to this output mapping. For example, to map all 2xx HTTP response status codes from an HTTP proxy to this output mapping, type "^2\d{2}" for HTTP status regex. To return an error message containing "Invalid Request" from a Lambda function to a 400 Bad Request response, type ".*Invalid request.*" as the Lambda error regex expression. On the other hand, to return 400 Bad Request for all unmapped error messages from Lambda, type "((\n.|.)+)" in Lambda error regex. This last regular expression can be used for the default error response of an API.

Note
API Gateway uses Java pattern-style regexes for response mapping. For more information, see Pattern in the Oracle documentation.

The error patterns are matched against the entire string of the errorMessage property in the Lambda response, which is populated by callback(errorMessage) in Node.js or by throw new MyException(errorMessage) in Java. Also, escaped characters are unescaped before the regular expression is applied.

If you use ".+" as the selection pattern to filter responses, be aware that it may not match a response containing a newline (\n) character.

c. If enabled, for Method response status, choose the HTTP response status code you defined in the Method Response page.

d. For Header Mappings, for each header you defined for the HTTP response status code in the Method Response page, specify a mapping value by choosing Edit. For Mapping value, use one of the following formats:

- integration.response.multivalueheaders.header-name
- integration.response.header.header-name

For example, to return the backend response's Date header as an API method's response's Timestamp header, the Response header column will contain a Timestamp entry, and the associated Mapping value should be set to integration.response.multivalueheaders.Date.

For example, to return the backend response's Date header as an API method's response's Timestamp header, the Response header column will contain a Timestamp entry, and the associated Mapping value should be set to integration.response.header.Date.
e. In the Template Mappings area, next to Content type, choose Add. In the Content type box, type the content type of the data that will be passed from the Lambda function, HTTP proxy, or AWS service proxy to the method. Choose Update.

f. Select Output passthrough if you want the method to receive, but not modify, the data from the Lambda function, HTTP proxy, or AWS service proxy.

g. If Output passthrough is cleared, for Output mapping, specify the output mapping template you want the Lambda function, HTTP proxy, or AWS service proxy to use to send data to the method. You can either type the mapping template manually or choose a model from Generate template from model.

h. Choose Save.

Create Models and Mapping Templates for Request and Response Mappings

In API Gateway, an API's method request can take a payload in a different format from the corresponding integration request payload, as required in the backend. Similarly, the backend may return an integration response payload different from the method response payload, as expected by the frontend. API Gateway lets you use mapping templates to map the payload from a method request to the corresponding integration request and from an integration response to the corresponding method response.

A mapping template is a script expressed in Velocity Template Language (VTL) and applied to the payload using JSONPath expressions.

The payload can have a data model according to the JSON schema draft 4. You must define the model in order to have API Gateway to generate a SDK or to enable basic request validation for your API. You do not have to define any model to create a mapping template. However, a model can help you create a template because API Gateway will generate a template blueprint based on a provided model.

The section explains how to map the API request and response payload using models and mapping templates.

Topics
- Models (p. 262)
- Mapping Templates (p. 266)
- Tasks for Models and Mapping Templates (p. 268)
- Create a Model in API Gateway (p. 268)
- View a List of Models in API Gateway (p. 269)
- Use a Mapping Template to Override an API's Request and Response Parameters and Status Codes (p. 269)
- Delete a Model in API Gateway (p. 273)
- Photos Example (API Gateway Models and Mapping Templates) (p. 273)
- News Article Example (API Gateway Models and Mapping Templates) (p. 277)
- Sales Invoice Example (API Gateway Models and Mapping Templates) (p. 280)
- Employee Record Example (API Gateway Models and Mapping Templates) (p. 284)

Models

In API Gateway, a model defines the data structure of a payload. In API Gateway models are defined using the JSON schema draft 4.
The following JSON object describes a sample data describing the fruit or vegetable inventory in the produce department of a likely supermarket:

Suppose we have an API for managing fruit and vegetable inventory in the produce department of a supermarket. When a manager queries the backend for the current inventory, the server sends back the following response payload:

```json
{
  "department": "produce",
  "categories": [
    "fruit",
    "vegetables"
  ],
  "bins": [
    {
      "category": "fruit",
      "type": "apples",
      "price": 1.99,
      "unit": "pound",
      "quantity": 232
    },
    {
      "category": "fruit",
      "type": "bananas",
      "price": 0.19,
      "unit": "each",
      "quantity": 112
    },
    {
      "category": "vegetables",
      "type": "carrots",
      "price": 1.29,
      "unit": "bag",
      "quantity": 57
    }
  ]
}
```

The JSON object has three properties:

- The department property has a string value (produce).
- The categories property is an array of two strings: fruit and vegetables.
- The bins property is an array of objects, each having the string- or number-valued properties of category, type, price, unit and quantity.

We can use the following JSON Schema to define the model for the above data:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "GroceryStoreInputModel",
  "type": "object",
  "properties": {
    "department": { "type": "string" },
    "categories": { "type": "array", "items": { "type": "string" } }
  },
  "bins": { "type": "array", "items": { "type": "object", "properties": { "category": "string", "type": "string", "price": "number", "unit": "string", "quantity": "number" } } }
}
```
In the preceding example model:

- The $schema object represents a valid JSON Schema version identifier. In this example, it refers to JSON Schema, draft v4.
- The title object is a human-readable identifier for the model. In this example, it is GroceryStoreInputModel.
- The top-level, or root, construct in the JSON data is an object.
- The root object in the JSON data contains department, categories, and bins properties.
- The department property is a string object in the JSON data.
- The categories property is an array in the JSON data. The array contains string values in the JSON data.
- The bins property is an array in the JSON data. The array contains objects in the JSON data. Each of these objects in the JSON data contains a category string, a type string, a price number, a unit string, and a quantity integer (a number without a fraction or exponent part).

Alternatively, you could include part of this schema, for example, the item definition of the bins array, in a separate section of the same file and use the $ref primitive to reference this reusable definition in other parts of the schema. Using $ref, the above model definition file can be expressed as follows:

```json
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "GroceryStoreInputModel",
    "type": "object",
    "properties": {
        "department": { "type": "string" },
        "categories": { "type": "array", "items": { "type": "string" } },
        "bins": { "type": "array", "items": { "$ref": "#/definitions/Bin" } }
    },
    "definitions": {
        "Bin": { "type": "object", "properties": { "category": { "type": "string" }, "type": { "type": "string" }, "price": { "type": "number" }, "unit": { "type": "string" }, "quantity": { "type": "integer" } } }
    }
}
```
The definitions section contains the schema definition of the Bin item that is referenced in the bins array with "$ref": "#/definitions/Bin". Using reusable definitions this way makes your model definition easier to read.

In addition, you can also reference another model schema defined in an external model file by setting that model's URL as the value of the $ref property: "$ref": "https://apigateway.amazonaws.com/restapis/{restapi_id}/models/{model_name}". For example, supposed you have the following full-fledged model named Bin created under an API with an identifier of fugvjdxtri:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "GroceryStoreInputModel",
  "type": "object",
  "properties": {
    "Bin": {
      "type": "object",
      "properties": {
        "category": { "type": "string" },
        "type": { "type": "string" },
        "price": { "type": "number" },
        "unit": { "type": "string" },
        "quantity": { "type": "integer" }
      }
    }
  }
}
```

You can then reference it from the GroceryStoreInputModel from the same API, as shown as follows:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "GroceryStoreInputModel",
  "type": "object",
  "properties": {
    "department": { "type": "string" },
    "categories": {
      "type": "array",
      "items": { "type": "string" }
    },
    "bins": {
      "type": "array",
      "items": {
        "$ref": "https://apigateway.amazonaws.com/restapis/fugvjdxtri/models/Bin2"
      }
    }
  }
}
```

The referencing and referenced models must be from the same API.

The examples do not use advanced JSON Schema features, such as specifying required items; minimum and maximum allowed string lengths, numeric values, and array item lengths; regular expressions; and more. For more information, see Introducing JSON and JSON schema draft 4.

For more complex JSON data formats and their models, see the following examples:

- Input Model (Photos Example) (p. 274) and Output Model (Photos Example) (p. 276) in the Photos Example (p. 273)
• Input Model (News Article Example) (p. 277) and Output Model (News Article Example) (p. 279) in the News Article Example (p. 277)
• Input Model (Sales Invoice Example) (p. 281) and Output Model (Sales Invoice Example) (p. 283) in the Sales Invoice Example (p. 280)
• Input Model (Employee Record Example) (p. 285) and Output Model (Employee Record Example) (p. 287) in the Employee Record Example (p. 284)

To experiment with models in API Gateway, follow the instructions in Map Response Payload (p. 74), specifically Step 1: Create Models (p. 76).

Mapping Templates

When the backend returns the query results (shown in the Models (p. 262) section), the manager of the produce department may be interested in reading them as follows:

```json
{
    "choices": [
        {
            "kind": "apples",
            "suggestedPrice": "1.99 per pound",
            "available": 232
        },
        {
            "kind": "bananas",
            "suggestedPrice": "0.19 per each",
            "available": 112
        },
        {
            "kind": "carrots",
            "suggestedPrice": "1.29 per bag",
            "available": 57
        }
    ]
}
```

To enable this, we need to provide API Gateway a mapping template to translate the data from the backend format. The following mapping template will do just that.

```java
#set($inputRoot = $input.path(''))
{
    "choices": [
        #foreach($elem in $inputRoot.bins)
            {
                "kind": "$elem.type",
                "suggestedPrice": "$elem.price per $elem.unit",
                "available": $elem.quantity
            }#if($foreach.hasNext),#end
        #end
    ]
}
```

Let us now examine some details of the preceding output mapping template:

• The $inputRoot variable represents the root object in the original JSON data from the previous section. The variables in an output mapping template map to the original JSON data, not the desired transformed JSON data schema.
• The choices array in the output mapping template is mapped from the bins array with the root object in the original JSON data ($inputRoot.bins).
• In the output mapping template, each of the objects in the `choices` array (represented by `$elem`) are mapped from the corresponding objects in the `bins` array within the root object in the original JSON data.

• In the output mapping template, for each of objects in the `choices` object, the values of the `kind` and `available` objects (represented by `$elem.type` and `$elem.quantity`) are mapped from the corresponding values of the `type` and `value` objects in each of the objects in the original JSON data's `bins` array, respectively.

• In the output mapping template, for each of objects in the `choices` object, the value of the `suggestedPrice` object is a concatenation of the corresponding value of the `price` and `unit` objects in each of the objects in the original JSON data, respectively, with each value separated by the word `per`.

For more information about the Velocity Template Language, see Apache Velocity - VTL Reference. For more information about JSONPath, see JSONPath - XPath for JSON.

The mapping template assumes that the underlying data is of a JSON object. It does not require that a model be defined for the data. As an API developer, you know the data formats at both the front and backends. That knowledge can guide you to define the necessary mappings without ambiguity.

To have an SDK generated for the API, the above data will be returned as a language-specific object. For strongly typed languages, such as Java, Objective-C or Swift, the object corresponds to a user-defined data type (UDT). API Gateway will create such a UDT if you provide it with a data model. For the method response example above, you can define the following payload model in the integration response:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "GroceryStoreOutputModel",
  "type": "object",
  "properties": {
    "choices": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "kind": { "type": "string" },
          "suggestedPrice": { "type": "string" },
          "available": { "type": "integer" }
        }
      }
    }
  }
}
```

In this model, the JSON schema is expressed as follows:

• The `$schema` object represents a valid JSON Schema version identifier. In this example, it refers to JSON Schema, draft v4.

• The `title` object is a human-readable identifier for the model. In this example, it is `GroceryStoreOutputModel`.

• The top-level, or root, construct in the JSON data is an object.

• The root object in the JSON data contains an array of objects.

• Each object in the array of objects contains a `kind` string, a `suggestedPrice` string, and an `available` integer (a number without a fraction or exponent part).

With this model, you can call an SDK to retrieve the `kind`, `suggestedPrice` and `available` property values by reading the `GroceryStoreOutputModel[i].kind`,
To explore more complex mapping templates, see the following examples:

- Input Mapping Template (Photos Example) (p. 275) and Output Mapping Template (Photos Example) (p. 276) in the Photos Example (p. 273)
- Input Mapping Template (News Article Example) (p. 278) and Output Mapping Template (News Article Example) (p. 279) in the News Article Example (p. 277)
- Input Mapping Template (Sales Invoice Example) (p. 282) and Output Mapping Template (Sales Invoice Example) (p. 283) in the Sales Invoice Example (p. 280)
- Input Mapping Template (Employee Record Example) (p. 286) and Output Mapping Template (Employee Record Example) (p. 288) in the Employee Record Example (p. 284)

To experiment with mapping templates in API Gateway, follow the instructions in Map Response Payload (p. 74), specifically Step 5: Set up and Test the Methods (p. 80).

Tasks for Models and Mapping Templates

For additional things you can do with models and mapping templates, see the following:

- Create a Model (p. 268)
- View a List of Models (p. 269)
- Delete a Model (p. 273)

Create a Model in API Gateway

Use the API Gateway console to create a model for an API.

Topics

- Prerequisites (p. 268)
- Create a Model With the API Gateway Console (p. 268)

Prerequisites

- You must have an API available in API Gateway. Follow the instructions in Creating a REST API in Amazon API Gateway (p. 177).

Create a Model With the API Gateway Console

2. In the box that contains the name of the API where you want to create the model, choose Models.
3. Choose Create.
4. For Model Name, type a name for the model.
5. For Content Type, type the model's content type (for example, application/json for JSON).
6. (Optional) For Model description, type a description for the model.
7. For Model schema, type the model's schema. For more information about model schemas, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).
8. Choose Create model.
View a List of Models in API Gateway

Use the API Gateway console to view a list of models.

Topics

- Prerequisites (p. 269)
- View a List of Models with the API Gateway Console (p. 269)

Prerequisites

- You must have at least one model in API Gateway. Follow the instructions in Create a Model (p. 268).

View a List of Models with the API Gateway Console

2. In the box that contains the name of the API, choose Models.

Use a Mapping Template to Override an API's Request and Response Parameters and Status Codes

Standard API Gateway parameter and response code mapping templates (p. 262) allow you to map parameters one-to-one and map a family of integration response status codes (matched by a regular expression) to a single response status code. Mapping template overrides provides you with the flexibility to perform many-to-one parameter mappings; override parameters after standard API Gateway mappings have been applied; conditionally map parameters based on body content or other parameter values; programmatically create new parameters on the fly; and override status codes returned by your integration endpoint. Any type of request parameter, response header, or response status code may be overridden.

Following are example uses for a mapping template override:

- To create a new header (or overwrite an existing header) as a concatenation of two parameters
- To override the response code to a success or failure code based on the contents of the body
- To conditionally remap a parameter based on its contents or the contents of some other parameter
- To iterate over the contents of a json body and remap key value pairs to headers or query strings

To create a mapping template override, use one or more of the following $context variables (p. 293) in a mapping template (p. 262):

<table>
<thead>
<tr>
<th>Request Body Mapping Template</th>
<th>Response Body Mapping Template</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.requestOverride.header.header_name</td>
<td>$context.responseOverride.header.header_name</td>
</tr>
<tr>
<td>$context.requestOverride.path.path_name</td>
<td>$context.responseOverride.status</td>
</tr>
<tr>
<td>$context.requestOverride.querystring.querystring_name</td>
<td></td>
</tr>
</tbody>
</table>

Note

Mapping template overrides cannot be used with proxy integration endpoints, which lack data mappings. For more information about integration types, see Choose an API Gateway API Integration Type (p. 214).
Important
Overrides are final. An override may only be applied to each parameter once. Trying to override the same parameter multiple times will result in 5XX responses from Amazon API Gateway. If you must override the same parameter multiple times throughout the template, we recommend creating a variable and applying the override at the end of the template. Note that the template is applied only after the entire template is parsed. See Tutorial: Override an API's Request Parameters and Headers with the API Gateway Console (p. 271).

The following tutorials show how to create and test a mapping template override in the API Gateway console. These tutorials use the PetStore sample API (p. 42) as a starting point. Both tutorials assume that you have already created the PetStore sample API (p. 42).

Topics
- Tutorial: Override an API's Response Status Code with the API Gateway Console (p. 270)
- Tutorial: Override an API's Request Parameters and Headers with the API Gateway Console (p. 271)
- Examples: Override an API's Request Parameters and Headers with the API Gateway CLI (p. 272)
- Example: Override an API's Request Parameters and Headers Using the SDK for JavaScript (p. 273)

Tutorial: Override an API's Response Status Code with the API Gateway Console

To retrieve a pet using the PetStore sample API, you use the API method request of GET /pets/{petId}, where {petId} is a path parameter that can take a number at run time.

In this tutorial, you'll override this GET method's response code by creating a mapping template that maps $context.responseOverride.status to 400 when an error condition is detected.

2. Under APIs, choose the PetStore API.
3. In the Resources column, choose the GET method under /{petId}.
4. In the Client box, choose Test.
5. Type -1 for {petId} and choose Test.

In the results, you'll notice two things:

First, the Response Body indicates an out-of-range error:

```json
{
  "errors": [
    {
      "key": "GetPetRequest.petId",
      "message": "The value is out of range."
    }
  ]
}
```

Second, the last line under Logs box ends with: Method completed with status: 200.

6. Go back to Method Execution. Choose Integration Response, and then choose the arrow next to 200.
7. In the Mapping Templates section, choose Add mapping template.
8. For Content Type, type application/json, and then choose the check mark icon to save the choice.
9. Copy the following code into the template area:

```java
#set($inputRoot = $input.path('$.'))
```
10. Choose Save.
11. Go back to Method Execution
12. In the Client box, choose Test.
13. Type -1 for {petId} and choose Test.

In the results, the Response Body indicates an out-of-range error:

```
{
  "errors": [
    {
      "key": "GetPetRequest.petId",
      "message": "The value is out of range."
    }
  ]
}
```

However, the last line under Logs box now ends with: Method completed with status: 400.

**Tutorial: Override an API's Request Parameters and Headers with the API Gateway Console**

In this tutorial, you'll override the GET method's request header code by creating a mapping template that maps $context.requestOverride.header.**header_name** to a new header that combines two other headers.

2. Under APIs, choose the PetStore API.
3. In the Resources column, choose the GET method under /pets.
5. Create a parameter as follows:
   a. Expand HTTP Request Headers.
   b. Choose Add header.
   c. Under Name, type header1.
   d. Choose the check mark icon to save your choice.

Repeat the process to create a second header called header2.

6. Go back to Method Execution
7. Choose Integration Request.
8. Expand HTTP Headers. You’ll see the two headers you created, header1 and header2, along with their default mappings (under Mapped from).
10. Choose Add mapping template.
11. For Content Type, type application/json, and then choose the check mark icon to save the choice.
12. A popup will appear that says, Note: This template can map headers and body.

Choose Yes, secure this integration.
13. Copy the following code into the template area:

```
#set($header1Override = "foo")
#set($header3Value = "$input.params('header1')$input.params('header2')")
$input.json("$")
#set($context.requestOverride.header.header3 = $header3Value)
#set($context.requestOverride.header.header1 = $header1Override)
#set($context.requestOverride.header.multivalueheader=[$header1Override,
$header3Value])
```

14. Choose Save.
15. Go back to Method Execution
16. In the Client box, choose Test.
17. Under Headers for (pets), copy the following code:

```
header1:header1Val
header2:header2Val
```

18. Choose Test.

In the Logs, you should see an entry that includes this text:

```
Endpoint request headers: {header3=header1Valheader2Val,
header2=header2Val, header1=foo, x-amzn-apigateway-api-id=<api-id>,
Accept=application/json, multivalueheader=foo,header1Valheader2Val}
```

Examples: Override an API's Request Parameters and Headers with the API Gateway CLI

The following CLI example shows how to use the put-integration command to override a response code:

```
aws apigateway put-integration --rest-api-id <API_ID> --resource-id <PATH_TO_RESOURCE_ID>
--http-method <METHOD> --type <INTEGRATION_TYPE> --request-templates <REQUEST_TEMPLATE_MAP>
```

where `<REQUEST_TEMPLATE_MAP>` is a map from content type to a string of the template to apply. The structure of that map is as follows:

```
Content_type1=template_string,Content_type2=template_string
```

or, in JSON syntax:

```
{"content_type1": "template_string"
...}
```

The following example shows how to use the put-integration-response command to override an API's response code:

```
aws apigateway put-integration-response --rest-api-id <API_ID> --resource-id <PATH_TO_RESOURCE_ID>
--http-method <METHOD> --status-code <STATUS_CODE> --response-templates <RESPONSE_TEMPLATE_MAP>
```

where `<RESPONSE_TEMPLATE_MAP>` has the same format as `<REQUEST_TEMPLATE_MAP>` above.
Example: Override an API's Request Parameters and Headers Using the SDK for JavaScript

The following example shows how to use the `put-integration` command to override a response code:

**Request:**

```
var params = {
    httpMethod: 'STRING_VALUE', /* required */
    resourceId: 'STRING_VALUE', /* required */
    restApiId: 'STRING_VALUE', /* required */
    type: HTTP | AWS | MOCK | HTTP_PROXY | AWS_PROXY, /* required */
    requestTemplates: {
        '<Content_type>': 'TEMPLATE_STRING',
        /* '<String>': ... */
    },
};
apigateway.putIntegration(params, function(err, data) {
    if (err) console.log(err, err.stack); // an error occurred
    else console.log(data); // successful response
});
```

**Response:**

```
var params = {
    httpMethod: 'STRING_VALUE', /* required */
    resourceId: 'STRING_VALUE', /* required */
    restApiId: 'STRING_VALUE', /* required */
    statusCode: 'STRING_VALUE', /* required */
    responseTemplates: {
        '<Content_type>': 'TEMPLATE_STRING',
        /* '<String>': ... */
    },
};
apigateway.putIntegrationResponse(params, function(err, data) {
    if (err) console.log(err, err.stack); // an error occurred
    else console.log(data); // successful response
});
```

Delete a Model in API Gateway

Use the API Gateway console to delete a model.

**Warning**

Deleting a model may cause part or all of the corresponding API to become unusable by API callers. Deleting a model cannot be undone.

**Delete a Model with the API Gateway Console**

2. In the box that contains the name of the API for the model, choose Models.
3. In the Models pane, choose the model you want to delete, and then choose Delete Model.
4. When prompted, choose Delete.

Photos Example (API Gateway Models and Mapping Templates)

The following sections provide examples of models and mapping templates that could be used for a sample photo API in API Gateway. For more information about models and mapping templates in API Gateway, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).
Original Data (Photos Example)

The following is the original JSON data for the photos example:

```json
{
  "photos": {
    "page": 1,
    "pages": "1234",
    "perpage": 100,
    "total": "123398",
    "photo": [
      {
        "id": "12345678901",
        "owner": "23456789@A12",
        "secret": "abc123d456",
        "server": "1234",
        "farm": 1,
        "title": "Sample photo 1",
        "ispublic": 1,
        "isfriend": 0,
        "isfamily": 0
      },
      {
        "id": "23456789012",
        "owner": "34567890@B23",
        "secret": "bcd234e567",
        "server": "2345",
        "farm": 2,
        "title": "Sample photo 2",
        "ispublic": 1,
        "isfriend": 0,
        "isfamily": 0
      }
    ]
  }
}
```

Input Model (Photos Example)

The following is the input model that corresponds to the original JSON data for the photos example:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "PhotosInputModel",
  "type": "object",
  "properties": {
    "photos": {
      "type": "object",
      "properties": {
        "page": { "type": "integer" },
        "pages": { "type": "string" },
        "perpage": { "type": "integer" }
      }
    }
  }
}
```
Input Mapping Template (Photos Example)

The following is the input mapping template that corresponds to the original JSON data for the photos example:

```plaintext
#set($inputRoot = $input.path($))
{
  "photos": {
    "page": $inputRoot.photos.page,
    "pages": "$inputRoot.photos.pages",
    "perpage": $inputRoot.photos.perpage,
    "total": "$inputRoot.photos.total",
    "photo": [
      #foreach($elem in $inputRoot.photos.photo)
        {
          "id": "$elem.id",
          "owner": "$elem.owner",
          "secret": "$elem.secret",
          "server": "$elem.server",
          "farm": "$elem.farm",
          "title": "$elem.title",
          "ispublic": "$elem.ispublic",
          "isfriend": "$elem.isfriend",
          "isfamily": "$elem.isfamily"
        }
      #if($foreach.hasNext),
    #end
    #end
  ]
}
```

Transformed Data (Photos Example)

The following is one example of how the original photos example JSON data could be transformed for output:

```plaintext
{
  "photos": [
    {
      "id": "12345678901",
```
Output Model (Photos Example)

The following is the output model that corresponds to the transformed JSON data format:

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "PhotosOutputModel",
    "type": "object",
    "properties": {
        "photos": {
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "id": { "type": "string" },
                    "owner": { "type": "string" },
                    "title": { "type": "string" },
                    "ispublic": { "type": "integer" },
                    "isfriend": { "type": "integer" },
                    "isfamily": { "type": "integer" }
                }
            }
        }
    }
}
```

Output Mapping Template (Photos Example)

The following is the output mapping template that corresponds to the transformed JSON data format. The template variables here are based on the original, not transformed, JSON data format:

```
#set($inputRoot = $input.path($'))
{
    "photos": [
    #foreach($elem in $inputRoot.photos.photo)
        {
            "id": "$elem.id",
            "owner": "$elem.owner",
            "title": "$elem.title",
            "ispublic": "$elem.ispublic",
            "isfriend": "$elem.isfriend",
            "isfamily": "$elem.isfamily"
        }#if($foreach.hasNext),#end
    #end
}
```
News Article Example (API Gateway Models and Mapping Templates)

The following sections provide examples of models and mapping templates that could be used for a sample news article API in API Gateway. For more information about models and mapping templates in API Gateway, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

Topics

- Original Data (News Article Example) (p. 277)
- Input Model (News Article Example) (p. 277)
- Input Mapping Template (News Article Example) (p. 278)
- Transformed Data (News Article Example) (p. 279)
- Output Model (News Article Example) (p. 279)
- Output Mapping Template (News Article Example) (p. 279)

Original Data (News Article Example)

The following is the original JSON data for the news article example:

```json
{
   "count": 1,
   "items": [
      {
         "last_updated_date": "2015-04-24",
         "expire_date": "2016-04-25",
         "author_first_name": "John",
         "description": "Sample Description",
         "creation_date": "2015-04-20",
         "title": "Sample Title",
         "allow_comment": "1",
         "author": {
            "last_name": "Doe",
            "email": "johndoe@example.com",
            "first_name": "John"
         },
         "body": "Sample Body",
         "publish_date": "2015-04-25",
         "version": "1",
         "author_last_name": "Doe",
         "parent_id": 2345678901,
         "article_url": "http://www.example.com/articles/3456789012"
      }
   ],
   "version": 1
}
```

Input Model (News Article Example)

The following is the input model that corresponds to the original JSON data for the news article example:

```json
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "title": "NewsArticleInputModel",
   "type": "object",
   "properties": {
      "count": { "type": "integer" }
   }
}
```
"items": {
  "type": "array",
  "items": {
    "type": "object",
    "properties": {
      "last_updated_date": { "type": "string" },
      "expire_date": { "type": "string" },
      "author_first_name": { "type": "string" },
      "description": { "type": "string" },
      "creation_date": { "type": "string" },
      "title": { "type": "string" },
      "allow_comment": { "type": "string" },
      "author": {
        "type": "object",
        "properties": {
          "last_name": { "type": "string" },
          "email": { "type": "string" },
          "first_name": { "type": "string" }
        }
      },
      "body": { "type": "string" },
      "publish_date": { "type": "string" },
      "version": { "type": "string" },
      "author_last_name": { "type": "string" },
      "parent_id": { "type": "integer" },
      "article_url": { "type": "string" }
    }
  }
},
"version": { "type": "integer" }
}

Input Mapping Template (News Article Example)

The following is the input mapping template that corresponds to the original JSON data for the news article example:

```java
#set($inputRoot = $input.path('$.')
{
  "count": $inputRoot.count,
  "items": [
    #foreach($elem in $inputRoot.items)
    {
      "last_updated_date": "$elem.last_updated_date",
      "expire_date": "$elem.expire_date",
      "author_first_name": "$elem.author_first_name",
      "description": "$elem.description",
      "creation_date": "$elem.creation_date",
      "title": "$elem.title",
      "allow_comment": "$elem.allow_comment",
      "author": {
        "last_name": "$elem.author.last_name",
        "email": "$elem.author.email",
        "first_name": "$elem.author.first_name"
      },
      "body": "$elem.body",
      "publish_date": "$elem.publish_date",
      "version": "$elem.version",
      "author_last_name": "$elem.author_last_name",
      "parent_id": $elem.parent_id,
      "article_url": "$elem.article_url"
    }#if($foreach.hasNext),#end
  ]
})
```

278
# Set up Data Mappings

### Transformed Data (News Article Example)

The following is one example of how the original news article example JSON data could be transformed for output:

```json
{
  "count": 1,
  "items": [
    {
      "creation_date": "2015-04-20",
      "title": "Sample Title",
      "author": "John Doe",
      "body": "Sample Body",
      "publish_date": "2015-04-25",
      "article_url": "http://www.example.com/articles/3456789012"
    }
  ],
  "version": 1
}
```

### Output Model (News Article Example)

The following is the output model that corresponds to the transformed JSON data format:

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "NewsArticleOutputModel",
  "type": "object",
  "properties": {
    "count": { "type": "integer" },
    "items": {
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "creation_date": { "type": "string" },
          "title": { "type": "string" },
          "author": { "type": "string" },
          "body": { "type": "string" },
          "publish_date": { "type": "string" },
          "article_url": { "type": "string" }
        }
      }
    },
    "version": { "type": "integer" }
  }
}
```

### Output Mapping Template (News Article Example)

The following is the output mapping template that corresponds to the transformed JSON data format. The template variables here are based on the original, not transformed, JSON data format:

```template
#set($inputRoot = $input.path('/'))
{
  "count": $inputRoot.count,
  "items": [
    {
      "creation_date": $inputRoot.creation_date,
      "title": $inputRoot.title,
      "author": $inputRoot.author,
      "body": $inputRoot.body,
      "publish_date": $inputRoot.publish_date,
      "article_url": $inputRoot.article_url
    }
  ],
  "version": $inputRoot.version
}
```
"items": [
  #foreach($elem in $inputRoot.items)
    {
      "creation_date": "$elem.creation_date",
      "title": "$elem.title",
      "author": "$elem.author.first_name $elem.author.last_name",
      "body": "$elem.body",
      "publish_date": "$elem.publish_date",
      "article_url": "$elem.article_url"
    }#if($foreach.hasNext),#end
  #end
],
"version": $inputRoot.version
}

Sales Invoice Example (API Gateway Models and Mapping Templates)

The following sections provide examples of models and mapping templates that could be used for a sample sales invoice API in API Gateway. For more information about models and mapping templates in API Gateway, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

**Topics**
- Original Data (Sales Invoice Example) (p. 280)
- Input Model (Sales Invoice Example) (p. 281)
- Input Mapping Template (Sales Invoice Example) (p. 282)
- Transformed Data (Sales Invoice Example) (p. 283)
- Output Model (Sales Invoice Example) (p. 283)
- Output Mapping Template (Sales Invoice Example) (p. 283)

**Original Data (Sales Invoice Example)**

The following is the original JSON data for the sales invoice example:

```json
{
  "DueDate": "2013-02-15",
  "Balance": 1990.19,
  "DocNumber": "SAMP001",
  "Status": "Payable",
  "Line": [
    {
      "Description": "Sample Expense",
      "Amount": 500,
      "DetailType": "ExpenseDetail",
      "ExpenseDetail": {
        "Customer": {
          "value": "ABC123",
          "name": "Sample Customer"
        },
        "Ref": {
          "value": "DEF234",
          "name": "Sample Construction"
        },
        "Account": {
          "value": "EFG345",
          "name": "Fuel"
        },
        "LineStatus": "Billable"
      }
    }
  ]
}
```
Input Model (Sales Invoice Example)

The following is the input model that corresponds to the original JSON data for the sales invoice example:

```json
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "InvoiceInputModel",
    "type": "object",
    "properties": {
        "DueDate": { "type": "string" },
        "Balance": { "type": "number" },
        "DocNumber": { "type": "string" },
        "Status": { "type": "string" },
        "Line": { "type": "array", "items": { "type": "object", "properties": { "Description": { "type": "string" }, "Amount": { "type": "integer" }, "DetailType": { "type": "string" }, "ExpenseDetail": { "type": "object", "properties": { "Customer": { "type": "object", "properties": { "value": { "type": "string" }, "name": { "type": "string" } } }, "Ref": { "type": "object", "properties": { "value": { "type": "string" }, "name": { "type": "string" } } }, "Account": { "type": "object", "properties": { "value": { "type": "string" }, "name": { "type": "string" } } }, "LineStatus": { "type": "string" } } } } }, "Vendor": { "value": "GHI456", "name": "Sample Bank" }, "APRef": { "value": "HIJ567", "name": "Accounts Payable" }, "TotalAmt": 1990.19 } 
```
"Vendor": {  
    "type": "object",  
    "properties": {  
        "value": { "type": "string" },  
        "name": { "type": "string" }  
    }  
},  
"APRef": {  
    "type": "object",  
    "properties": {  
        "value": { "type": "string" },  
        "name": { "type": "string" }  
    }  
},  
"TotalAmt": { "type": "number" }  
}  

---

**Input Mapping Template (Sales Invoice Example)**

The following is the input mapping template that corresponds to the original JSON data for the sales invoice example:

```java
#set($inputRoot = $input.path(''))
{
    "DueDate": "$inputRoot.DueDate",
    "Balance": $inputRoot.Balance,
    "DocNumber": "$inputRoot.DocNumber",
    "Status": "$inputRoot.Status",
    "Line": [
        #foreach($elem in $inputRoot.Line)
            {
                "Description": "$elem.Description",
                "Amount": $elem.Amount,
                "DetailType": "$elem.DetailType",
                "ExpenseDetail": {
                    "Customer": {
                        "value": "$elem.ExpenseDetail.Customer.value",
                        "name": "$elem.ExpenseDetail.Customer.name"
                    },
                    "Ref": {
                        "value": "$elem.ExpenseDetail.Ref.value",
                        "name": "$elem.ExpenseDetail.Ref.name"
                    },
                    "Account": {
                        "value": "$elem.ExpenseDetail.Account.value",
                        "name": "$elem.ExpenseDetail.Account.name"
                    },
                    "LineStatus": "$elem.ExpenseDetail.LineStatus"
                }
            },
        #if($foreach.hasNext),
        #end
        #end
    ],
    "Vendor": {
        "value": "$inputRoot.Vendor.value",
        "name": "$inputRoot.Vendor.name"
    },
    "APRef": {
        "value": "$inputRoot.APRef.value",
        "name": "$inputRoot.APRef.name"
    },
    "TotalAmt": $inputRoot.TotalAmt
}  
```

---

282
Transformed Data (Sales Invoice Example)

The following is one example of how the original sales invoice example JSON data could be transformed for output:

```
{
    "DueDate": "2013-02-15",
    "Balance": 1990.19,
    "DocNumber": "SAMP001",
    "Status": "Payable",
    "Line": [
        {
            "Description": "Sample Expense",
            "Amount": 500,
            "DetailType": "ExpenseDetail",
            "Customer": "ABC123 (Sample Customer)",
            "Ref": "DEF234 (Sample Construction)",
            "Account": "EFG345 (Fuel)",
            "LineStatus": "Billable"
        }
    ],
    "TotalAmt": 1990.19
}
```

Output Model (Sales Invoice Example)

The following is the output model that corresponds to the transformed JSON data format:

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "InvoiceOutputModel",
    "type": "object",
    "properties": {
        "DueDate": { "type": "string" },
        "Balance": { "type": "number" },
        "DocNumber": { "type": "string" },
        "Status": { "type": "string" },
        "Line": {
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "Description": { "type": "string" },
                    "Amount": { "type": "integer" },
                    "DetailType": { "type": "string" },
                    "Customer": { "type": "string" },
                    "Ref": { "type": "string" },
                    "Account": { "type": "string" },
                    "LineStatus": { "type": "string" }
                }
            }
        },
        "TotalAmt": { "type": "number" }
    }
}
```

Output Mapping Template (Sales Invoice Example)

The following is the output mapping template that corresponds to the transformed JSON data format. The template variables here are based on the original, not transformed, JSON data format:

```
#set($inputRoot = $input.path(''))
{"..."
```
Employee Record Example (API Gateway Models and Mapping Templates)

The following sections provide examples of models and mapping templates that can be used for a sample employee record API in API Gateway. For more information about models and mapping templates in API Gateway, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

Topics
- Original Data (Employee Record Example) (p. 284)
- Input Model (Employee Record Example) (p. 285)
- Input Mapping Template (Employee Record Example) (p. 286)
- Transformed Data (Employee Record Example) (p. 286)
- Output Model (Employee Record Example) (p. 287)
- Output Mapping Template (Employee Record Example) (p. 288)

Original Data (Employee Record Example)

The following is the original JSON data for the employee record example:

```json
{
  "maxResults": "1",
  "startPosition": "1",
  "Employee": {
    "Organization": "false",
    "Title": "Mrs.",
    "GivenName": "Jane",
    "MiddleName": "Lane",
    "FamilyName": "Doe",
    "DisplayName": "Jane Lane Doe",
    "PrintOnCheckName": "Jane Lane Doe",
    "Active": "true",
    "PrimaryPhone": {
      "FreeFormNumber": "505.555.9999"
    },
    "PrimaryEmailAddr": {
      "Address": "janedoe@example.com"
    },
    "EmployeeType": "Regular",
    "status": "Synchronized",
    "Id": "ABC123",
    "SyncToken": "1",
    "MetaData": {
      "DueDate": "$inputRoot.DueDate",
      "Balance": $inputRoot.Balance,
      "DocNumber": "$inputRoot.DocNumber",
      "Status": "$inputRoot.Status",
      "Line": [
        #foreach($elem in $inputRoot.Line)
          {
            "Description": "$elem.Description",
            "Amount": $elem.Amount,
            "DetailType": "$elem.DetailType",
            "Ref": "$elem.ExpenseDetail.Ref.value ($elem.ExpenseDetail.Ref.name)",
            "LineStatus": "$elem.ExpenseDetail.LineStatus"
          }#if($foreach.hasNext),#end
        #end
      ],
      "TotalAmt": $inputRoot.TotalAmt
    }
  }
}
```
Input Model (Employee Record Example)

The following is the input model that corresponds to the original JSON data for the employee record example:

```json
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "title": "EmployeeInputModel",
   "type": "object",
   "properties": {
      "QueryResponse": {
         "type": "object",
         "properties": {
            "maxResults": { "type": "string" },
            "startPosition": { "type": "string" },
            "Employee": {
               "type": "object",
               "properties": {
                  "Organization": { "type": "string" },
                  "Title": { "type": "string" },
                  "GivenName": { "type": "string" },
                  "MiddleName": { "type": "string" },
                  "FamilyName": { "type": "string" },
                  "DisplayName": { "type": "string" },
                  "PrintOnCheckName": { "type": "string" },
                  "Active": { "type": "string" },
                  "PrimaryPhone": {
                     "type": "object",
                     "properties": {
                        "FreeFormNumber": { "type": "string" }
                     }
                  },
                  "PrimaryEmailAddr": {
                     "type": "object",
                     "properties": {
                        "Address": { "type": "string" }
                     }
                  },
                  "EmployeeType": { "type": "string" },
                  "status": { "type": "string" },
                  "Id": { "type": "string" },
                  "SyncToken": { "type": "string" },
                  "MetaData": {
                     "type": "object",
                     "properties": {
                        "CreateTime": { "type": "string" },
                        "LastUpdatedTime": { "type": "string" }
                     }
                  }
               }
            }
         }
      }
   }
}
```
Input Mapping Template (Employee Record Example)

The following is the input mapping template that corresponds to the original JSON data for the employee record example:

```java
#set($inputRoot = $input.path('/'))
{
  "QueryResponse": {
    "maxResults": "$inputRoot.QueryResponse.maxResults",
    "startPosition": "$inputRoot.QueryResponse.startPosition",
    "Employee": {
      "Title": "$inputRoot.QueryResponse.Employee.Title",
      "GivenName": "$inputRoot.QueryResponse.Employee.GivenName",
      "MiddleName": "$inputRoot.QueryResponse.Employee.MiddleName",
      "FamilyName": "$inputRoot.QueryResponse.Employee.FamilyName",
      "DisplayName": "$inputRoot.QueryResponse.Employee.DisplayName",
      "PrintOnCheckName": "$inputRoot.QueryResponse.Employee.PrintOnCheckName",
      "Active": "$inputRoot.QueryResponse.Employee.Active",
      "PrimaryPhone": { "FreeFormNumber": "$inputRoot.QueryResponse.Employee.PrimaryPhone.FreeFormNumber" },
      "PrimaryEmailAddr": { "Address": "$inputRoot.QueryResponse.Employee.PrimaryEmailAddr.Address" },
      "EmployeeType": "$inputRoot.QueryResponse.Employee.EmployeeType",
      "status": "$inputRoot.QueryResponse.Employee.status",
      "Id": "$inputRoot.QueryResponse.Employee.Id",
      "SyncToken": "$inputRoot.QueryResponse.Employee.SyncToken",
      "MetaData": {
        "LastUpdatedTime": "$inputRoot.QueryResponse.Employee.MetaData.LastUpdatedTime"
      },
      "PrimaryAddr": {
        "Line1": "$inputRoot.QueryResponse.Employee.PrimaryAddr.Line1",
        "City": "$inputRoot.QueryResponse.Employee.PrimaryAddr.City",
      }
    }
  },
  "time": "$inputRoot.time"
}
```

Transformed Data (Employee Record Example)

The following is one example of how the original employee record example JSON data could be transformed for output:
Output Model (Employee Record Example)

The following is the output model that corresponds to the transformed JSON data format:

```json
{
"$schema": "http://json-schema.org/draft-04/schema#",
"title": "EmployeeOutputModel",
"type": "object",
"properties": {
"QueryResponse": {
"type": "object",
"properties": {
"maxResults": { "type": "string" },
"startPosition": { "type": "string" },
"Employees": {
"type": "array",
"items": {
"type": "object",
"properties": {
"Title": { "type": "string" },
"GivenName": { "type": "string" },
"MiddleName": { "type": "string" },
"FamilyName": { "type": "string" },
"DisplayName": { "type": "string" },
"PrintOnCheckName": { "type": "string" },
"Active": { "type": "string" },
"PrimaryPhone": { "type": "string" },
"PrimaryAddr": {
"type": "object",
"properties": {
"Line1": { "type": "string" },
"City": { "type": "string" },
"CountrySubDivisionCode": { "type": "string" },
"PostalCode": { "type": "string" }
}
}
}
}
}
"time": "2015-04-27T22:12:32.012Z"
}
```
Output Mapping Template (Employee Record Example)

The following is the output mapping template that corresponds to the transformed JSON data format. The template variables here are based on the original, not transformed, JSON data format:

```java
#set($inputRoot = $input.path(''))

Amazon API Gateway API Request and Response Data Mapping Reference

This section explains how to set up data mappings from an API's method request data, including other data stored in context (p. 293), stage (p. 302), or util (p. 302) variables, to the corresponding integration request parameters and from an integration response data, including the other data, to the method response parameters. The method request data includes request parameters (path, query string, headers) and the body. The integration response data includes response parameters (headers) and the body. For more information about using the stage variables, see Amazon API Gateway Stage Variables Reference (p. 519).

Topics
- Map Method Request Data to Integration Request Parameters (p. 289)
- Map Integration Response Data to Method Response Headers (p. 290)
- Map Request and Response Payloads between Method and Integration (p. 291)
- Integration Passthrough Behaviors (p. 292)

Map Method Request Data to Integration Request Parameters

Integration request parameters, in the form of path variables, query strings or headers, can be mapped from any defined method request parameters and the payload.

In the following table, PARAM_NAME is the name of a method request parameter of the given parameter type. It must match the regular expression ‘^[a-zA-Z0-9._$-]+$’ and must have been defined before it can be referenced. JSONPath_EXPRESSION is a JSONPath expression for a JSON field of the body of a request or response.

**Note**
The "$" prefix is omitted in this syntax.

Integration request data mapping expressions

<table>
<thead>
<tr>
<th>Mapped data source</th>
<th>Mapping expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Method request path</td>
<td>method.request.path.$PARAM_NAME</td>
</tr>
<tr>
<td>Method request query string</td>
<td>method.request.querystring.$PARAM_NAME</td>
</tr>
<tr>
<td>Multi-value method request query string</td>
<td>method.request.multivaluequerystring.$PARAM_NAME</td>
</tr>
<tr>
<td>Method request header</td>
<td>method.request.header.$PARAM_NAME</td>
</tr>
<tr>
<td>Multi-value method request header</td>
<td>method.request.multivalueheader.$PARAM_NAME</td>
</tr>
<tr>
<td>Method request body</td>
<td>method.request.body</td>
</tr>
<tr>
<td>Method request body (JsonPath)</td>
<td>method.request.body.$JSONPath_EXPRESSION</td>
</tr>
<tr>
<td>Stage variables</td>
<td>stageVariables.$VARIABLE_NAME</td>
</tr>
<tr>
<td>Context variables</td>
<td>context.$VARIABLE_NAME that must be one of the supported context variables (p. 293).</td>
</tr>
<tr>
<td>Static value</td>
<td>$STATIC_VALUE. The STATIC_VALUE is a string literal and must be enclosed within a pair of single quotes.</td>
</tr>
</tbody>
</table>
Example mappings from method request parameter in OpenAPI

The following example shows an OpenAPI snippet that maps:

- the method request's header, named `methodRequestHeaderParam`, into the integration request path parameter, named `integrationPathParam`
- the multi-value method request query string, named `methodRequestQueryParam`, into the integration request query string, named `integrationQueryParam`

```json
...  
"requestParameters" : {
  "integration.request.path.integrationPathParam" : "method.request.header.methodRequestHeaderParam",
  "integration.request.querystring.integrationQueryParam" : "method.request.multivaluequerystring.methodRequestQueryParam"
}
...  
```

Integration request parameters can also be mapped from fields in the JSON request body using a JSONPath expression. The following table shows the mapping expressions for a method request body and its JSON fields.

Example mapping from method request body in OpenAPI

The following example shows an OpenAPI snippet that maps 1) the method request body to the integration request header, named `body-header`, and 2) a JSON field of the body, as expressed by a JSON expression (`petstore.pets[0].name`, without the `$.` prefix).

```json
...  
"requestParameters" : {
  "integration.request.header.body-header" : "method.request.body",
  "integration.request.path.pet-name" : "method.request.body.petstore.pets[0].name",
}
...  
```

Map Integration Response Data to Method Response Headers

Method response header parameters can be mapped from any integration response header or integration response body, `$context` variables, or static values.

<table>
<thead>
<tr>
<th>Mapped Data Source</th>
<th>Mapping expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration response header</td>
<td><code>integration.response.header.PARAM_NAME</code></td>
</tr>
<tr>
<td>Integration response header</td>
<td><code>integration.response.multivalueheader.PARAM_NAME</code></td>
</tr>
<tr>
<td>Integration response body</td>
<td><code>integration.response.body</code></td>
</tr>
</tbody>
</table>
Set up Data Mappings

<table>
<thead>
<tr>
<th>Mapped Data Source</th>
<th>Mapping expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration response body (JsonPath)</td>
<td>integration.response.body.JSONPath_EXPRESSION</td>
</tr>
<tr>
<td>Stage variable</td>
<td>stageVariables.VARIABLE_NAME</td>
</tr>
<tr>
<td>Context variable</td>
<td>context.VARIABLE_NAME</td>
</tr>
<tr>
<td>Static value</td>
<td>'STATIC_VALUE'. The STATIC_VALUE is a string literal and must be enclosed within a pair of single quotes.</td>
</tr>
</tbody>
</table>

**Example data mapping from integration response in OpenAPI**

The following example shows an OpenAPI snippet that maps 1) the integration response's redirect.url, JSONPath field into the request response's location header; and 2) the integration response's x-app-id header to the method response's id header.

```json
...
"responseParameters" : {
    "method.response.header.location" : "integration.response.body.redirect.url",
    "method.response.header.id" : "integration.response.header.x-app-id",
    "method.response.header.items" : "integration.response.multivalueheader.item",
}
...
```

**Map Request and Response Payloads between Method and Integration**

API Gateway uses Velocity Template Language (VTL) engine to process body mapping templates (p. 266) for the integration request and integration response. The mapping templates translate method request payloads to the corresponding integration request payloads and translate integration response bodies to the method response bodies.

The VTL templates use JSONPath expressions, other parameters such as calling contexts and stage variables, and utility functions to process the JSON data.

If a model is defined to describe the data structure of a payload, API Gateway can use the model to generate a skeletal mapping template for an integration request or integration response. You can use the skeletal template as an aid to customize and expand the mapping VTL script. However, you can create a mapping template from scratch without defining a model for the payload's data structure.

**Select a VTL Mapping Template**

API Gateway uses the following logic to select a mapping template, in Velocity Template Language (VTL), to map the payload from a method request to the corresponding integration request or to map the payload from an integration response to the corresponding method response.

For a request payload, API Gateway uses the request's Content-Type header value as the key to select the mapping template for the request payload. For a response payload, API Gateway uses the incoming request's Accept header value as the key to select the mapping template.

When the Content-Type header is absent in the request, API Gateway assumes that its default value is application/json. For such a request, API Gateway uses application/json as the default key.
to select the mapping template, if one is defined. When no template matches this key, API Gateway passes the payload through unmapped if the `passthroughBehavior` property is set to `WHEN_NO_MATCH` or `WHEN_NO_TEMPLATES`.

When the `Accept` header is not specified in the request, API Gateway assumes that its default value is `application/json`. In this case, API Gateway selects an existing mapping template for `application/json` to map the response payload. If no template is defined for `application/json`, API Gateway selects the first existing template and uses it as the default to map the response payload. Similarly, API Gateway uses the first existing template when the specified `Accept` header value does not match any existing template key. If no template is defined, API Gateway simply passes the response payload through unmapped.

For example, suppose that an API has a `application/json` template defined for a request payload and has a `application/xml` template defined for the response payload. If the client sets the “Content-Type : application/json”, and "Accept : application/xml" headers in the request, both the request and response payloads will be processed with the corresponding mapping templates. If the Accept:application/xml header is absent, the application/xml mapping template will be used to map the response payload. To return the response payload unmapped instead, you must set up an empty template for `application/json`.

Only the MIME type is used from the `Accept` and `Content-Type` headers when selecting a mapping template. For example, a header of "Content-Type: application/json; charset=UTF-8" will have a request template with the `application/json` key selected.

### Integration Passthrough Behaviors

With non-proxy integrations, when a method request carries a payload and either the Content-Type header does not match any specified mapping template or no mapping template is defined, you can choose to pass the client-supplied request payload through the integration request to the backend without transformation. The process is known as integration passthrough.

For proxy integrations (p. 215), API Gateway passes the entire request through to your backend, and you do not have the option to modify the passthrough behaviors.

The actual passthrough behavior of an incoming request is determined by the option you choose for a specified mapping template, during integration request set-up (p. 259), and the Content Type header that a client set in the incoming request. The following examples illustrate the possible passthrough behaviors.

**Example 1:** One mapping template is defined in the integration request for the `application/json` content type.

<table>
<thead>
<tr>
<th>Content-Type header \Selected passthrough option</th>
<th>WHEN_NO_MATCH</th>
<th>WHEN_NO TEMPLATE</th>
<th>NEVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (default to application/json)</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
</tr>
<tr>
<td>application/json</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
</tr>
<tr>
<td>application/xml</td>
<td>The request payload is not transformed and is sent to the backend as-is.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
</tr>
</tbody>
</table>
Example 2: One mapping template is defined in the integration request for the application/xml content type.

<table>
<thead>
<tr>
<th>Content-Type header \Selected passthrough option</th>
<th>WHEN_NO_MATCH</th>
<th>WHEN_NO_TEMPLATE</th>
<th>NEVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (default to application/json)</td>
<td>The request payload is not transformed and is sent to the backend as-is.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
</tr>
<tr>
<td>application/json</td>
<td>The request payload is not transformed and is sent to the backend as-is.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
<td>The request is rejected with an HTTP 415 Unsupported Media Type response.</td>
</tr>
<tr>
<td>application/xml</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
<td>The request payload is transformed using the template.</td>
</tr>
</tbody>
</table>

**API Gateway Mapping Template and Access Logging Variable Reference**

This section provides reference information for the variables and functions that Amazon API Gateway defines for use with data models, authorizers, mapping templates, and CloudWatch access logging. For detailed information about how to use these variables and functions, see the section called “Create Models and Mapping Templates” (p. 262).

**Topics**

- $context Variables for Data Models, Authorizers, Mapping Templates, and CloudWatch Access Logging (p. 293)
- $context Variable Template Example (p. 298)
- $context Variables for CloudWatch Access Logging Only (p. 298)
- $input Variables (p. 299)
- $input Variable Template Examples (p. 300)
- $stageVariables (p. 302)
- $util Variables (p. 302)

**Note**

For $method and $integration variables, see the section called “Request and Response Data Mapping Reference” (p. 289).

**$context Variables for Data Models, Authorizers, Mapping Templates, and CloudWatch Access Logging**

The following $context variables can be used in data models, authorizers, mapping templates, and CloudWatch access logging.

For $context variables that can be used only in CloudWatch access logging, see the section called “$context Variables for CloudWatch Access Logging Only” (p. 298).
### Parameter | Description
--- | ---
$context.accountId | The API owner's AWS account ID.
$context.apiId | The identifier API Gateway assigns to your API.
$context.authorizer.claims.property | A property of the claims returned from the Amazon Cognito user pool after the method caller is successfully authenticated. For more information, see the section called "Use Cognito User Pool as Authorizer for a REST API" (p. 397).
| Note: Calling $context.authorizer.claims returns null.
$context.authorizer.principalId | The principal user identification associated with the token sent by the client and returned from an API Gateway Lambda authorizer (formerly known as a custom authorizer). For more information, see the section called "Use Lambda Authorizers" (p. 380).
$context.authorizer.property | The stringified value of the specified key-value pair of the context map returned from an API Gateway Lambda authorizer function. For example, if the authorizer returns the following context map:

```
"context" : {
   "key": "value",
   "numKey": 1,
   "boolKey": true
}
```
calling $context.authorizer.key returns the "value" string, calling $context.authorizer.numKey returns the "1" string, and calling $context.authorizer.boolKey returns the "true" string.
For more information, see the section called "Use Lambda Authorizers" (p. 380).
$context.awsEndpointRequestId | The AWS endpoint's request ID.
$context.domainName | The full domain name used to invoke the API. This should be the same as the incoming Host header.
$context.domainPrefix | The first label of the $context.domainName. This is often used as a caller/customer identifier.
$context.error.message | A string containing an API Gateway error message. This variable can only be used for simple variable substitution in a GatewayResponse body-mapping template, which is not processed by the Velocity Template Language engine, and in access logging. For more information, see the section...
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.error.messageString</td>
<td>The quoted value of $context.error.message, namely &quot;$context.error.message&quot;.</td>
</tr>
<tr>
<td>$context.error.responseType</td>
<td>A type of GatewayResponse. This variable can only be used for simple variable substitution in a GatewayResponse body-mapping template, which is not processed by the Velocity Template Language engine, and in access logging. For more information, see the section called “Monitor WebSocket API Execution with CloudWatch” (p. 617) and the section called “Set up Gateway Responses” (p. 252).</td>
</tr>
<tr>
<td>$context.error.validationErrorString</td>
<td>A string containing a detailed validation error message.</td>
</tr>
<tr>
<td>$context.extendedRequestId</td>
<td>The extended ID that API Gateway assigns to the API request, which contains more useful information for debugging/troubleshooting.</td>
</tr>
<tr>
<td>$context.httpMethod</td>
<td>The HTTP method used. Valid values include: DELETE, GET, HEAD, OPTIONS, PATCH, POST, and PUT.</td>
</tr>
<tr>
<td>$context.identity.accountId</td>
<td>The AWS account ID associated with the request.</td>
</tr>
<tr>
<td>$context.identity.apiKey</td>
<td>For API methods that require an API key, this variable is the API key associated with the method request. For methods that don't require an API key, this variable is null. For more information, see the section called “Use Usage Plans with API Keys” (p. 432).</td>
</tr>
<tr>
<td>$context.identity.apiKeyId</td>
<td>The API key ID associated with an API request that requires an API key.</td>
</tr>
<tr>
<td>$context.identity.caller</td>
<td>The principal identifier of the caller making the request.</td>
</tr>
<tr>
<td>$context.identity.cognitoAuthenticationProvider</td>
<td>The Amazon Cognito authentication provider used by the caller making the request. Available only if the request was signed with Amazon Cognito credentials. For information, see Using Federated Identities in the Amazon Cognito Developer Guide.</td>
</tr>
<tr>
<td>$context.identity.cognitoAuthenticationType</td>
<td>The Amazon Cognito authentication type of the caller making the request. Available only if the request was signed with Amazon Cognito credentials.</td>
</tr>
<tr>
<td>$context.identity.cognitoIdentityId</td>
<td>The Amazon Cognito identity ID of the caller making the request. Available only if the request was signed with Amazon Cognito credentials.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$context.identity.cognitoIdentityPoolId</td>
<td>The Amazon Cognito identity pool ID of the caller making the request. Available only if the request was signed with Amazon Cognito credentials.</td>
</tr>
<tr>
<td>$context.identity.principalOrgId</td>
<td>The AWS organization ID.</td>
</tr>
<tr>
<td>$context.identity.sourceIp</td>
<td>The source IP address of the TCP connection making the request to API Gateway.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning</strong></td>
</tr>
<tr>
<td></td>
<td>You should not trust this value if there is any chance that the X-Forwarded-For header could be forged.</td>
</tr>
<tr>
<td>$context.identity.user</td>
<td>The principal identifier of the user making the request. Used in Lambda authorizers. For more information, see the section called “Output from an Amazon API Gateway Lambda Authorizer” (p. 391).</td>
</tr>
<tr>
<td>$context.identity.userAgent</td>
<td>The User-Agent header of the API caller.</td>
</tr>
<tr>
<td>$context.identity.userArn</td>
<td>The Amazon Resource Name (ARN) of the effective user identified after authentication. For more information, see <a href="https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html">https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html</a>.</td>
</tr>
<tr>
<td>$context.path</td>
<td>The request path. For example, for a non-proxy request URL of https://{rest-api-id.execute-api.{region}.amazonaws.com/{stage}/root/child, the $context.path value is {stage}/root/child.</td>
</tr>
<tr>
<td>$context.protocol</td>
<td>The request protocol, for example, HTTP/1.1.</td>
</tr>
<tr>
<td>$context.requestId</td>
<td>The ID that API Gateway assigns to the API request.</td>
</tr>
<tr>
<td>$context.requestOverride.header.header_name</td>
<td>The request header override. If this parameter is defined, it contains the headers to be used instead of the HTTP Headers that are defined in the Integration Request pane. For more information, see Use a Mapping Template to Override an API’s Request and Response Parameters and Status Codes (p. 269).</td>
</tr>
<tr>
<td>$context.requestOverride.path.path_name</td>
<td>The request path override. If this parameter is defined, it contains the request path to be used instead of the URL Path Parameters that are defined in the Integration Request pane. For more information, see Use a Mapping Template to Override an API’s Request and Response Parameters and Status Codes (p. 269).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>$context.requestOverride.querystring.querystring_name</td>
<td>The request query string override. If this parameter is defined, it contains the request query strings to be used instead of the URL Query String Parameters that are defined in the Integration Request pane. For more information, see Use a Mapping Template to Override an API's Request and Response Parameters and Status Codes (p. 269).</td>
</tr>
<tr>
<td>$context.responseOverride.header.header_name</td>
<td>The response header override. If this parameter is defined, it contains the header to be returned instead of the Response header that is defined as the Default mapping in the Integration Response pane. For more information, see Use a Mapping Template to Override an API's Request and Response Parameters and Status Codes (p. 269).</td>
</tr>
<tr>
<td>$context.responseOverride.status</td>
<td>The response status code override. If this parameter is defined, it contains the status code to be returned instead of the Method response status that is defined as the Default mapping in the Integration Response pane. For more information, see Use a Mapping Template to Override an API's Request and Response Parameters and Status Codes (p. 269).</td>
</tr>
<tr>
<td>$context.requestTime</td>
<td>The CLF-formatted request time (dd/MMM/yyyy:HH:mm:ss +hhmm).</td>
</tr>
<tr>
<td>$context.requestTimeEpoch</td>
<td>The Epoch-formatted request time.</td>
</tr>
<tr>
<td>$context.resourceId</td>
<td>The identifier that API Gateway assigns to your resource.</td>
</tr>
<tr>
<td>$context.resourcePath</td>
<td>The path to your resource. For example, for the non-proxy request URI of https://{rest-api-id.execute-api.{region}.amazonaws.com/{stage}/root/child, The $context.resourcePath value is /root/child. For more information, see TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).</td>
</tr>
<tr>
<td>$context.stage</td>
<td>The deployment stage of the API request (for example, Beta or Prod).</td>
</tr>
<tr>
<td>$context.wafResponseCode</td>
<td>The response received from AWS WAF: WAF_ALLOW or WAF_BLOCK. Will not be set if the stage is not associated with a web ACL. For more information, see the section called &quot;Use AWS WAF to Protect Your API from Common Web Exploits&quot; (p. 430).</td>
</tr>
</tbody>
</table>
Set up Data Mappings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.webaclArn</td>
<td>The complete ARN of the web ACL that is used to decide whether to allow or block the request. Will not be set if the stage is not associated with a web ACL. For more information, see the section called “Use AWS WAF to Protect Your API from Common Web Exploits” (p. 430).</td>
</tr>
<tr>
<td>$context.xrayTraceId</td>
<td>The trace ID for the X-Ray trace. For more information, see the section called “Setting Up AWS X-Ray” (p. 559).</td>
</tr>
</tbody>
</table>

$context Variable Template Example

You may want to use $context variables in a mapping template if your API method passes structured data to a backend that requires the data to be in a particular format.

The following example shows a mapping template that maps incoming $context variables to backend variables with slightly different names in an integration request payload:

**Note**

Note that one of the variables is an API key. This example assumes that the method has "require API key" enabled.

```json
{
    "stage": "$context.stage",
    "request_id": "$context.requestId",
    "http_method": "$context.httpMethod",
    "source_ip": "$context.identity.sourceIp",
    "user_agent": "$context.identity.userAgent",
    "account_id": "$context.identity.accountId",
    "api_key": "$context.identity.apiKey",
    "caller": "$context.identity.caller",
    "user": "$context.identity.user",
    "user_arn": "$context.identity.userArn"
}
```

$context Variables for CloudWatch Access Logging Only

The following $context variables are available only for CloudWatch access logging. For more information, see the section called “Set Up CloudWatch API Logging” (p. 510). (For WebSocket APIs, see the section called “Monitor WebSocket API Execution with CloudWatch” (p. 617).)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.authorizer.integrationLatency</td>
<td>The authorizer latency in ms.</td>
</tr>
<tr>
<td>$context.integrationLatency</td>
<td>The integration latency in ms.</td>
</tr>
<tr>
<td>$context.integrationStatus</td>
<td>For Lambda proxy integration, this parameter represents the status code returned from AWS Lambda, not from the backend Lambda function.</td>
</tr>
<tr>
<td>$context.responseLatency</td>
<td>The response latency in ms.</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.responseLength</td>
<td>The response payload length.</td>
</tr>
<tr>
<td>$context.status</td>
<td>The method response status.</td>
</tr>
</tbody>
</table>

### "$input" Variables

The "$input" variable represents the method request payload and parameters to be processed by a mapping template. It provides four functions:

<table>
<thead>
<tr>
<th>Variable and Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$input.body</td>
<td>Returns the raw request payload as a string.</td>
</tr>
<tr>
<td>$input.json(x)</td>
<td>This function evaluates a JSONPath expression and returns the results as a JSON string. For example, $input.json('$.pets') returns a JSON string representing the pets structure. For more information about JSONPath, see JSONPath or JSONPath for Java.</td>
</tr>
<tr>
<td>$input.params()</td>
<td>Returns a map of all the request parameters.</td>
</tr>
<tr>
<td>$input.params(x)</td>
<td>Returns the value of a method request parameter from the path, query string, or header value (searched in that order), given a parameter name string x.</td>
</tr>
<tr>
<td>$input.path(x)</td>
<td>Takes a JSONPath expression string (x) and returns a JSON object representation of the result. This allows you to access and manipulate elements of the payload natively in Apache Velocity Template Language (VTL). For example, if the expression $input.path('$.pets') returns an object like this:</td>
</tr>
</tbody>
</table>

```json
[
  {
    "id": 1,
    "type": "dog",
    "price": 249.99
  },
  {
    "id": 2,
    "type": "cat",
    "price": 124.99
  },
  {
    "id": 3,
    "type": "fish",
    "price": 0.99
  }
]
```
<table>
<thead>
<tr>
<th>Variable and Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$input.path('$.pets').count()</td>
<td>would return &quot;3&quot;.</td>
</tr>
<tr>
<td></td>
<td>For more information about JSONPath, see JSONPath or JSONPath for Java.</td>
</tr>
</tbody>
</table>

### $input Variable Template Examples

#### Parameter Mapping Template Example

The following parameter-mapping example passes all parameters, including path, querystring, and header, through to the integration endpoint via a JSON payload:

```
#set($allParams = $input.params())
{
  "params" : {
    #foreach($type in $allParams.keySet())
    #set($params = $allParams.get($type))
    "$type" : {
      #foreach($paramName in $params.keySet())
      "$paramName" : "$util.escapeJavaScript($params.get($paramName))"
      #if($foreach.hasNext),#end
    }#if($foreach.hasNext),#end
    #end
    #if($foreach.hasNext),#end
  }#if($foreach.hasNext),#end
}
```

In effect, this mapping template outputs all the request parameters in the payload as outlined as follows:

```
{
  "parameters" : {
    "path" : {
      "path_name" : "path_value",
      ...
    }
    "header" : {
      "header_name" : "header_value",
      ...
    }
    "querystring" : {
      "querystring_name" : "querystring_value",
      ...
    }
  }
}
```

You may want to use the $input variable to get query strings and the request body with or without using models. You may also want to get the parameter and the payload, or a subsection of the payload, into your Lambda function. The following examples show how to do this.

#### Example JSON Mapping Template Using $input

The following example shows how to use a mapping to read a name from the query string and then include the entire POST body in an element:

```
"name" : "$input.params('name')",
"body" : $input.json('$')
}

If the JSON input contains unescaped characters that cannot be parsed by JavaScript, a 400 response may be returned. Applying $util.escapeJavaScript($input.json('$')) above will ensure that the JSON input can be parsed properly.

Example Mapping Template Using $input

The following example shows how to pass a JSONPath expression to the json() method. You could also read a specific property of your request body object by using a period (.), followed by your property name:

```
{
    "name" : "$input.params('name')",
    "body" : $input.json('$.mykey')
}
```

If a method request payload contains unescaped characters that cannot be parsed by JavaScript, you may get 400 response. In this case, you need to call $util.escapeJavaScript() function in the mapping template, as shown as follows:

```
{
    "name" : "$input.params('name')",
    "body" : $util.escapeJavaScript($input.json('$.mykey'))
}
```

Example Request and Response Using $input

Here's an example that uses all three functions:

**Request Template:**

Resource: /things/{id}

With input template:

```
{
    "id" : "$input.params('id')",
    "count" : "$input.path('$.things').size()",
    "things" : $util.escapeJavaScript($input.json('$.things'))
}
```

POST /things/abc
```
{
    "things" : {
        "1" : {},
        "2" : {},
        "3" : {}
    }
}
```

**Response:**

```
{
    "id": "abc",
    "count": "3",
    "things": {
        "1": {},
        "2": {}
    }
}
"3": {}  
}  
}  

For more mapping examples, see Create Models and Mapping Templates for Request and Response Mappings (p. 262).

$stageVariables

Stage variables can be used in parameter mapping and mapping templates and as placeholders in ARNs and URLs used in method integrations. For more information, see the section called “Set up Stage Variables for a REST API” (p. 514).

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$stageVariables.&lt;variable_name&gt;</td>
<td>&lt;variable_name&gt; represents a stage variable name.</td>
</tr>
<tr>
<td>$stageVariables['&lt;variable_name&gt;']</td>
<td>&lt;variable_name&gt; represents any stage variable name.</td>
</tr>
<tr>
<td>${stageVariables['&lt;variable_name&gt;']}</td>
<td>&lt;variable_name&gt; represents any stage variable name.</td>
</tr>
</tbody>
</table>

$util Variables

The $util variable contains utility functions for use in mapping templates.

**Note**

Unless otherwise specified, the default character set is UTF-8.

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
</table>
| $util.escapeJavaScript() | Escapes the characters in a string using JavaScript string rules.  
**Note**  
This function will turn any regular single quotes (‘) into escaped ones (\’). However, the escaped single quotes are not valid in JSON. Thus, when the output from this function is used in a JSON property, you must turn any escaped single quotes (\’) back to regular single quotes (‘). This is shown in the following example:  
```javascript  
$util.escapeJavaScript(data).replaceAll("\"", \\
"\", \\
")  
``` |
| $util.parseJson() | Takes "stringified" JSON and returns an object representation of the result. You can use the result from this function to access and manipulate elements of the payload natively in Apache Velocity Template Language (VTL). For example, if you have the following payload:
Support Binary Payloads in API Gateway

In API Gateway, the API request and response can have a text or binary payload. A text payload is a UTF-8-encoded JSON string, and a binary payload is anything other than a text payload. The binary payload can be, for example, a JPEG file, a GZip file, or an XML file.

By default, API Gateway treats the message body as a text payload and applies any preconfigured mapping template to transform the JSON string. If no mapping template is specified, API Gateway can pass the text payload through to or from the integration endpoint without modification, provided that the passthrough behavior is enabled on the API method. For a binary payload, API Gateway simply passes through the body as-is.

For API Gateway to pass binary payloads, you add the media types to the binaryMediaTypes list of the RestApi resource or set the contentHandling properties on the Integration and the IntegrationResponse resources. The contentHandling value can be CONVERT_TO_BINARY, CONVERT_TO_TEXT, or undefined. Depending on the contentHandling value, and whether the Content-Type header of the response or the Accept header of the incoming request matches an entry in the binaryMediaTypes list, API Gateway can encode the raw binary bytes as a Base64-encoded string, decode a Base64-encoded string back to its raw bytes, or pass the body through without modification.

You must configure the API as follows to support binary payloads for your API in API Gateway:

- Add the desired binary media types to the binaryMediaTypes list on the RestApi resource. If this property and the contentHandling property are not defined, the payloads are handled as UTF-8 encoded JSON strings.
• Set the `contentHandling` property of the `Integration` resource to `CONVERT_TO_BINARY` to have the request payload converted from a Base64-encoded string to its binary blob, or set the property to `CONVERT_TO_TEXT` to have the request payload converted from a binary blob to a Base64-encoded string. If this property is not defined, API Gateway passes the payload through without modification. This occurs when the `Content-Type` header value matches one of the `binaryMediaTypes` entries and the `passThroughBehaviors` (p. 292) are also enabled for the API.

• Set the `contentHandling` property of the `IntegrationResponse` resource to `CONVERT_TO_BINARY` to have the response payload converted from a Base64-encoded string to its binary blob, or set the property to `CONVERT_TO_TEXT` to have the response payload converted from a binary blob to a Base64-encoded string. If `contentHandling` is not defined, and if the `Content-Type` header of the response and the `Accept` header of the original request match an entry of the `binaryMediaTypes` list, API Gateway passes through the body. This occurs when the `Content-Type` header and the `Accept` header are the same; otherwise, API Gateway converts the response body to the type specified in the `Accept` header.

**Tip**
When a request contains multiple media types in its `Accept` header, API Gateway only honors the first `Accept` media type. In the situation where you cannot control the order of the `Accept` media types and the media type of your binary content is not the first in the list, you can add the first `Accept` media type in the `binaryMediaTypes` list of your API, API Gateway will return your content as binary. For example, to send a JPEG file using an `<img>` element in a browser, the browser might send `Accept:image/webp,image/*,*/*;q=0.8` in a request. By adding `image/webp` to the `binaryMediaTypes` list, the endpoint will receive the JPEG file as binary.

**Topics**
- Content Type Conversions in API Gateway (p. 304)
- Enable Binary Support Using the API Gateway Console (p. 306)
- Enable Binary Support Using API Gateway REST API (p. 310)
- Import and Export Content Encodings (p. 314)
- Examples of Binary Support (p. 314)

**Content Type Conversions in API Gateway**

The following table shows how API Gateway converts the request payload for specific configurations of a request's `Content-Type` header, the `binaryMediaTypes` list of a `RestApi` resource, and the `contentHandling` property value of the `Integration` resource.

**API Request Content Type Conversions in API Gateway**

<table>
<thead>
<tr>
<th>Method request payload</th>
<th>Request Content-Type header</th>
<th>binaryMediaTypes</th>
<th>contentHandling</th>
<th>Integration request payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text data</td>
<td>Any data type</td>
<td>Undefined</td>
<td>Undefined</td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Text data</td>
<td>Any data type</td>
<td>Undefined</td>
<td><code>CONVERT_TO_BINARY</code></td>
<td>Base64-decoded binary blob</td>
</tr>
<tr>
<td>Text data</td>
<td>Any data type</td>
<td>Undefined</td>
<td><code>CONVERT_TO_TEXT</code></td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Text data</td>
<td>A text data type</td>
<td>Set with matching media types</td>
<td>Undefined</td>
<td>Text data</td>
</tr>
</tbody>
</table>
The following table shows how API Gateway converts the response payload for specific configurations of a request's Accept header, the binaryMediaTypes list of a RestApi resource, and the contentHandling property value of the IntegrationResponse resource.

### API Gateway Response Content Type Conversions

<table>
<thead>
<tr>
<th>Integration response payload</th>
<th>Request Accept header</th>
<th>binaryMediaTypes</th>
<th>contentHandling</th>
<th>Method response payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text or binary data</td>
<td>A text type</td>
<td>Undefined</td>
<td>Undefined</td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Text or binary data</td>
<td>A text type</td>
<td>Undefined</td>
<td>CONVERT_TO_BINARY</td>
<td>Base64-decoded blob</td>
</tr>
<tr>
<td>Text or binary data</td>
<td>A text type</td>
<td>Undefined</td>
<td>CONVERT_TO_TEXT</td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Text data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>Undefined</td>
<td>Text data</td>
</tr>
<tr>
<td>Text data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_BINARY</td>
<td>Base64-decoded blob</td>
</tr>
<tr>
<td>Text data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_TEXT</td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Text data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>Undefined</td>
<td>Base64-decoded blob</td>
</tr>
<tr>
<td>Text data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_BINARY</td>
<td>Base64-decoded blob</td>
</tr>
<tr>
<td>Text data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_TEXT</td>
<td>UTF8-encoded string</td>
</tr>
<tr>
<td>Binary data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>Undefined</td>
<td>Base64-encoded string</td>
</tr>
<tr>
<td>Binary data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_BINARY</td>
<td>Base64-decoded blob</td>
</tr>
<tr>
<td>Binary data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_TEXT</td>
<td>UTF8-encoded string</td>
</tr>
</tbody>
</table>
Support Binary Payloads

<table>
<thead>
<tr>
<th>Integration response payload</th>
<th>Request Accept header</th>
<th>binaryMediaTypes</th>
<th>contentHandling</th>
<th>Method response payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binary data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_BINARY</td>
<td>Binary data</td>
</tr>
<tr>
<td>Binary data</td>
<td>A text type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_TEXT</td>
<td>Base64-encoded string</td>
</tr>
<tr>
<td>Binary data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>Undefined</td>
<td>Binary data</td>
</tr>
<tr>
<td>Binary data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_BINARY</td>
<td>Binary data</td>
</tr>
<tr>
<td>Binary data</td>
<td>A binary type</td>
<td>Set with matching media types</td>
<td>CONVERT_TO_TEXT</td>
<td>Base64-encoded string</td>
</tr>
</tbody>
</table>

Tip
When a request contains multiple media types in its Accept header, API Gateway only honors the first Accept media type. In the situation where you cannot control the order of the Accept media types and the media type of your binary content is not the first in the list, you can add the first Accept media type in the binaryMediaTypes list of your API, API Gateway will return your content as binary. For example, to send a JPEG file using an <img> element in a browser, the browser might send Accept: image/webp, image/*,*/*;q=0.8 in a request. By adding image/webp to the binaryMediaTypes list, the endpoint will receive the JPEG file as binary.

When converting a text payload to a binary blob, API Gateway assumes that the text data is a Base64-encoded string and outputs the binary data as a Base64-decoded blob. If the conversion fails, it returns a 500 response indicating an API configuration error. You do not provide a mapping template for such a conversion, although you must enable the passthrough behaviors (p. 292) on the API.

When converting a binary payload to a text string, API Gateway always applies a Base64 encoding on the binary data. You can define a mapping template for such a payload, but can only access the Base64-encoded string in the mapping template through $input.body, as shown in the following excerpt of an example mapping template.

```json
{
  "data": "$input.body"
}
```

To have the binary payload passed through without modification, you must enable the passthrough behaviors (p. 292) on the API.

Enable Binary Support Using the API Gateway Console

The section explains how to enable binary support using the API Gateway console. As an example, we use an API integrated with Amazon S3. We focus on the tasks to set the supported media types and to specify how the payload should be handled. For detailed information on how to create an API integrated with Amazon S3, see TUTORIAL: Create a REST API as an Amazon S3 Proxy in API Gateway (p. 111).

To enable binary support using the API Gateway console

1. Set binary media types for the API:
   a. Create a new API or choose an existing API. For this example, we name the API FileMan.
b. Under the selected API in the primary navigation panel, choose Settings.

c. In the Settings pane, choose Add Binary Media Type in the Binary Media Types section.

d. Type a required media type, for example, image/png, in the input text field. If needed, repeat this step to add more media types. To support all binary media types, specify /.

e. Choose Save Changes.

2. Set how message payloads are handled for the API method:

   a. Create a new or choose an existing resource in the API. For this example, we use the / {folder}/{item} resource.

   b. Create a new or choose an existing method on the resource. As an example, we use the GET / {folder}/{item} method integrated with the Object GET action in Amazon S3.

   c. In Content Handling, choose an option.
Choose **Passthrough** if you do not want to convert the body when the client and backend accepts the same binary format. Choose **Convert to text (if needed)** to convert the binary body to a Base64-encoded string when, for example, the backend requires that a binary request payload is passed in as a JSON property. And choose **Convert to binary (if needed)** when the client submits a Base64-encoded string and the backend requires the original binary format, or when the endpoint returns a Base64-encoded string and the client accepts only the binary output.

d. Preserve the incoming request's `Accept` header in the integration request. You should do this if you've set `contentHandling` to `passthrough` and want to override that setting at run time.
e. Enable the passthrough behavior on the request body.

f. For conversion to text, define a mapping template to put the Base64-encoded binary data into the required format.
Support Binary Payloads

The format of this mapping template depends on the endpoint requirements of the input.

Enable Binary Support Using API Gateway REST API

The following tasks show how to enable binary support using the API Gateway REST API calls.

Topics

- Add and Update Supported Binary Media Types to an API (p. 310)
- Configure Request Payload Conversions (p. 311)
- Configure Response Payload Conversions (p. 311)
- Convert Binary Data to Text Data (p. 312)
- Convert Text Data to a Binary Payload (p. 312)
- Pass through a Binary Payload (p. 313)

Add and Update Supported Binary Media Types to an API

To enable API Gateway to support a new binary media type, you must add the binary media type to the binaryMediaTypes list of the RestApi resource. For example, to have API Gateway handle JPEG images, submit a PATCH request to the RestApi resource:
Support Binary Payloads

PATCH /restapis/<restapi_id>/
{
  "patchOperations" : [ {
    "op" : "add",
    "path" : "/binaryMediaTypes/image~1jpeg"
  }
]
}

The MIME type specification of image/jpeg that is part of the path property value is escaped as image~1jpeg.

To update the supported binary media types, replace or remove the media type from the binaryMediaTypes list of the RestApi resource. For example, to change binary support from JPEG files to raw bytes, submit a PATCH request to the RestApi resource, as follows.

PATCH /restapis/<restapi_id>/
{
  "patchOperations" : [ {
    "op" : "replace",
    "path" : "/binaryMediaTypes/image~1jpeg",
    "value" : "application/octet-stream"
  },
  { "op" : "remove",
    "path" : "/binaryMediaTypes/image~1jpeg"
  }
]
}

Configure Request Payload Conversions

If the endpoint requires a binary input, set the contentHandling property of the Integration resource to CONVERT_TO_BINARY. To do so, submit a PATCH request, as shown next:

PATCH /restapis/<restapi_id>/resources/<resource_id>/methods/<http_method>/integration
{
  "patchOperations" : [ {
    "op" : "replace",
    "path" : "/contentHandling",
    "value" : "CONVERT_TO_BINARY"
  }
]
}

Configure Response Payload Conversions

If the client accepts the result as a binary blob instead of a Base64-encoded payload returned from the endpoint, set the contentHandling property of the IntegrationResponse resource to CONVERT_TO_BINARY by submitting a PATCH request, as shown next:

PATCH /restapis/<restapi_id>/resources/<resource_id>/methods/<http_method>/integration/responses/<status_code>
{
  "patchOperations" : [ {
    "op" : "replace",
    "path" : "/contentHandling",
    "value" : "CONVERT_TO_BINARY"
  }
]
**Convert Binary Data to Text Data**

To send binary data as a JSON property of the input to AWS Lambda or Kinesis through API Gateway, do the following:

1. Enable the binary payload support of the API by adding the new binary media type of `application/octet-stream` to the API's `binaryMediaTypes` list.

   ```json
   PATCH /restapis/<restapi_id>
   {
       "patchOperations" : [ {
           "op" : "add",
           "path" : "/binaryMediaTypes/application/octet-stream"
       }]
   }
   
   2. Set `CONVERT_TO_TEXT` on the `contentHandling` property of the `Integration` resource and provide a mapping template to assign the Base64-encoded string of the binary data to a JSON property. In the following example, the JSON property is `body` and `$input.body` holds the Base64-encoded string.

   ```json
   PATCH /restapis/<restapi_id>/resources/<resource_id>/methods/<http_method>/integration
   {
       "patchOperations" : [
           {
               "op" : "replace",
               "path" : "/contentHandling",
               "value" : "CONVERT_TO_TEXT"
           },
           {
               "op" : "add",
               "path" : "/requestTemplates/application/octet-stream",
               "value" : "{\"body\": \"$input.body\"}"
           }
       ]
   }
   
**Convert Text Data to a Binary Payload**

Suppose a Lambda function returns an image file as a Base64-encoded string. To pass this binary output to the client through API Gateway, do the following:

1. Update the API's `binaryMediaTypes` list by adding the binary media type of `application/octet-stream` if it is not already in the list.

   ```json
   PATCH /restapis/<restapi_id>
   {
       "patchOperations" : [ {
           "op" : "add",
           "path" : "/binaryMediaTypes/application/octet-stream",
       }]
   }
   ```
2. Set the `contentHandling` property on the Integration resource to `CONVERT_TO_BINARY`. Do not define a mapping template. When you do not define a mapping template, API Gateway invokes the passthrough template to return the Base64-decoded binary blob as the image file to the client.

```json
PATCH /restapis/<restapi_id>/resources/<resource_id>/methods/<http_method>/integration/responses/<status_code>
{
    "patchOperations" : [
        {
            "op" : "replace",
            "path" : "/contentHandling",
            "value" : "CONVERT_TO_BINARY"
        }
    ]
}
```

**Pass through a Binary Payload**

To store an image in an Amazon S3 bucket using API Gateway, do the following:

1. Update the API's `binaryMediaTypes` list by adding the binary media type of `application/octet-stream`, if it is not already in the list.

```json
PATCH /restapis/<restapi_id>
{
    "patchOperations" : [
        {
            "op" : "add",
            "path" : "/binaryMediaTypes/application/octet-stream"
        }
    ]
}
```

2. On the `contentHandling` property of the Integration resource, set `CONVERT_TO_BINARY`. Set `WHEN_NO_MATCH` as the `passthroughBehavior` property value without defining a mapping template. This enables API Gateway to invoke the passthrough template.

```json
PATCH /restapis/<restapi_id>/resources/<resource_id>/methods/<http_method>/integration
{
    "patchOperations" : [
        {
            "op" : "replace",
            "path" : "/contentHandling",
            "value" : "CONVERT_TO_BINARY"
        },
        {
            "op" : "replace",
            "path" : "/passthroughBehaviors",
            "value" : "WHEN_NO_MATCH"
        }
    ]
}
```
Import and Export Content Encodings

To import the `binaryMediaTypes` list on a RestApi, use the following API Gateway extension to the API's OpenAPI definition file. The extension is also used to export the API settings.

- `x-amazon-apigateway-binary-media-types` Property (p. 582)

To import and export the `contentHandling` property value on an Integration or IntegrationResponse resource, use the following API Gateway extensions to the OpenAPI definitions:

- `x-amazon-apigateway-integration` Object (p. 586)
- `x-amazon-apigateway-integration.response` Object (p. 592)

Examples of Binary Support

The following example demonstrates how to access a binary file in Amazon S3 or AWS Lambda through an API Gateway API. The sample API is presented in an OpenAPI file. The code example uses the API Gateway REST API calls.

Topics
- Access Binary Files in Amazon S3 through an API Gateway API (p. 314)
- Access Binary Files in Lambda Using an API Gateway API (p. 319)

Access Binary Files in Amazon S3 through an API Gateway API

The following examples show the OpenAPI file used to access images in Amazon S3, how to download an image from Amazon S3, and how to upload an image to Amazon S3.

Topics
- OpenAPI File of a Sample API to Access Images in Amazon S3 (p. 314)
- Download an Image from Amazon S3 (p. 318)
- Upload an Image to Amazon S3 (p. 319)

OpenAPI File of a Sample API to Access Images in Amazon S3

The following OpenAPI file shows a sample API that illustrates downloading an image file from Amazon S3 and uploading an image file to Amazon S3. This API exposes the `GET /s3?key={file-name}` and `PUT /s3?key={file-name}` methods for downloading and uploading a specified image file. The `GET` method returns the image file as a Base64-encoded string as part of a JSON output, following the supplied mapping template, in a 200 OK response. The `PUT` method takes a raw binary blob as input and returns a 200 OK response with an empty payload.

OpenAPI 3.0

```json
{
  "openapi": "3.0.0",
  "info": {
    "version": "2016-10-21T17:26:28Z",
    "title": "ApiName"
  },
  "paths": {
    "/s3": {
      "get": {
        "parameters": [
```
Support Binary Payloads

```
{
  "name": "key",
  "in": "query",
  "required": false,
  "schema": {
    "type": "string"
  }
}
```

```
"200": {
  "description": "200 response",
  "content": {
    "application/json": {
      "schema": {
        "$ref": "#/components/schemas/Empty"
      }
    }
  }
},
"500": {
  "description": "500 response"
}
```

```
x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/binarySupportRole",
  "responses": {
    "default": {
      "statusCode": "500"
    },
    "$\{\d(2)\}$": {
      "statusCode": "200"
    }
  },
  "requestParameters": {
    "integration.request.path.key": "method.request.querystring.key"
  },
  "uri": "arn:aws:apigateway:us-west-2:s3:path/{key}",
  "passthroughBehavior": "when_no_match",
  "httpMethod": "GET",
  "type": "aws"
}
```

```
"put": {
  "parameters": [
    {
      "name": "key",
      "in": "query",
      "required": false,
      "schema": {
        "type": "string"
      }
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "content": {
        "application/json": {
          "schema": {
            "$ref": "#/components/schemas/Empty"
          }
        },
        "application/octet-stream": {
          "schema": {
            "$ref": "#/components/schemas/Empty"
          }
        }
      }
    }
  }
}
```
Support Binary Payloads

```json
OpenAPI 2.0

{
    "swagger": "2.0",
    "info": {
        "version": "2016-10-21T17:26:28Z",
        "title": "ApiName"
    },
    "host": "abcdefghi.execute-api.us-east-1.amazonaws.com",
    "basePath": "/v1",
    "schemes": [
        "https"
    ],
    "paths": {
        "}
    "}
```

"https",
"paths": {
  "/s3": {
    "get": {
      "produces": [
        "application/json"
      ],
      "parameters": [
        {
          "name": "key",
          "in": "query",
          "required": false,
          "type": "string"
        }
      ],
      "responses": {
        "200": {
          "description": "200 response",
          "schema": {
            "$ref": "#/definitions/Empty"
          }
        },
        "500": {
          "description": "500 response"
        }
      },
      "x-amazon-apigateway-integration": {
        "credentials": "arn:aws:iam::123456789012:role/binarySupportRole",
        "responses": {
          "default": {
            "statusCode": "500"
          },
          "2\d{2}\": {
            "statusCode": "200"
          }
        },
        "requestParameters": {
          "integration.request.path.key": "method.request.querystring.key"
        },
        "uri": "arn:aws:apigateway:us-west-2:s3:path/{key}'",
        "passthroughBehavior": "when_no_match",
        "httpMethod": "GET",
        "type": "aws"
      }
    },
    "put": {
      "produces": [
        "application/json", "application/octet-stream"
      ],
      "parameters": [
        {
          "name": "key",
          "in": "query",
          "required": false,
          "type": "string"
        }
      ],
      "responses": {
        "200": {
          "description": "200 response",
          "schema": {
            "$ref": "#/definitions/Empty"
          }
        },
        "500": {
          "description": "500 response"
        }
      }
    }
  }
}
Download an Image from Amazon S3

To download an image file (image.jpg) as a binary blob from Amazon S3:

GET /v1/s3?key=image.jpg HTTP/1.1
Host: abcdefghi.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/octet-stream

The successful response looks like this:

200 OK HTTP/1.1
[raw bytes]

The raw bytes are returned because the Accept header is set to a binary media type of application/octet-stream and binary support is enabled for the API.

Alternatively, to download an image file (image.jpg) as a Base64-encoded string, formatted as a JSON property, from Amazon S3, add a response template to the 200 integration response like this, as shown in the bold-faced OpenAPI definition block below:

```
"x-amazon-apigateway-integration": {
  "credentials": "arn:aws:iam::123456789012:role/binarySupportRole",
  "responses": {
    "default": {
      "statusCode": "500"
    },
    "200": {
      "statusCode": "200"
    }
  },
  "requestParameters": {
    "integration.request.path.key": "method.request.querystring.key"
  },
  "uri": "arn:aws:apigateway:us-west-2:s3:path/{key}",
  "passthroughBehavior": "when_no_match",
  "httpMethod": "PUT",
  "type": "aws",
  "contentHandling": "CONVERT_TO_BINARY"
}
```

"x-amazon-apigateway-binary-media-types" : ["application/octet-stream", "image/jpeg"],
"definitions": {
  "Empty": {
    "type": "object",
    "title": "Empty Schema"
  }
}
<table>
<thead>
<tr>
<th>Support Binary Payloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>The request to download the image file looks like this:</td>
</tr>
<tr>
<td>GET /v1/s3?key=image.jpg HTTP/1.1</td>
</tr>
<tr>
<td>Host: abcdefghi.execute-api.us-east-1.amazonaws.com</td>
</tr>
<tr>
<td>Content-Type: application/json</td>
</tr>
<tr>
<td>Accept: application/json</td>
</tr>
<tr>
<td>The successful response looks like this:</td>
</tr>
<tr>
<td>200 OK HTTP/1.1</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;image&quot;: &quot;W3JhdyBieXRlc10=&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>

**Upload an Image to Amazon S3**

To upload an image file (image.jpg) as a binary blob to Amazon S3:

| PUT /v1/s3?key=image.jpg HTTP/1.1 |
| Host: abcdefghi.execute-api.us-east-1.amazonaws.com |
| Content-Type: application/octet-stream |
| Accept: application/json |
| [raw bytes] |
| The successful response looks like this: |
| 200 OK HTTP/1.1 |

To upload an image file (image.jpg) as a Base64-encoded string to Amazon S3:

| PUT /v1/s3?key=image.jpg HTTP/1.1 |
| Host: abcdefghi.execute-api.us-east-1.amazonaws.com |
| Content-Type: application/json |
| Accept: application/json |
| W3JhdyBieXRlc10= |

Notice that the input payload must be a Base64-encoded string, because the Content-Type header value is set to application/json. The successful response looks like this:

| 200 OK HTTP/1.1 |

**Access Binary Files in Lambda Using an API Gateway API**

The following example demonstrates how to access a binary file in AWS Lambda through an API Gateway API. The sample API is presented in an OpenAPI file. The code example uses the API Gateway REST API calls.
Topics

- OpenAPI File of a Sample API to Access Images in Lambda (p. 320)
- Download an Image from Lambda (p. 324)
- Upload an Image to Lambda (p. 324)

OpenAPI File of a Sample API to Access Images in Lambda

The following OpenAPI file shows an example API that illustrates downloading an image file from Lambda and uploading an image file to Lambda.

OpenAPI 3.0

```json
{
   "openapi": "3.0.0",
   "info": {
      "version": "2016-10-21T17:26:28Z",
      "title": "ApiName"
   },
   "paths": {
      "/lambda": {
         "get": {
            "parameters": [
               {
                  "name": "key",
                  "in": "query",
                  "required": false,
                  "schema": {
                     "type": "string"
                  }
               }
            ],
            "responses": {
               "200": {
                  "description": "200 response",
                  "content": {
                     "application/json": {
                        "schema": {
                           "$ref": "#/components/schemas/Empty"
                        }
                     }
                  }
               },
               "500": {
                  "description": "500 response"
               }
            }
         }
      }
   }
}
```


Support Binary Payloads

"application/json": "{"image": "$input.body"}"

"put": {
"parameters": [
{
"name": "key",
"in": "query",
"required": false,
"schema": {
"type": "string"
}
}
],
"responses": {
"200": {
"description": "200 response",
"content": {
"application/json": {
"schema": {
"$ref": "#/components/schemas/Empty"
}
},
"application/octet-stream": {
"schema": {
"$ref": "#/components/schemas/Empty"
}
}
}
},
"500": {
"description": "500 response"
}
},
"x-amazon-apigateway-integration": {
"type": "AWS",
"credentials": "arn:aws:iam::123456789012:role/Lambda",
"httpMethod": "POST",
"contentHandling": "CONVERT_TO_TEXT",
"requestTemplates": {
"application/json": "{"imageKey": "$input.params('key')", "image": "$input.body"}"
},
"responses": {
"default": {
"statusCode": "500"
},
"2\d{2}": {
"statusCode": "200"
}
}
}
},
"x-amazon-apigateway-binary-media-types": [
"application/octet-stream",
"image/jpeg"
],
"servers": [
OpenAPI 2.0

```json
{
   "swagger": "2.0",
   "info": {
      "version": "2016-10-21T17:26:28Z",
      "title": "ApiName"
   },
   "host": "abcdefghi.execute-api.us-east-1.amazonaws.com",
   "basePath": "/v1",
   "schemes": [
      "https"
   ],
   "paths": {
      "/lambda": {
         "get": {
            "produces": ["application/json" района
                      "parameters": [
                         {"name": "key", "in": "query", "required": false, "type": "string"
                      }]
                     "responses": {
                        "200": {
                           "description": "200 response",
                           "schema": {
                              "$ref": "#/definitions/Empty"
                           }
                        },
                        "500": {
                           "description": "500 response"
                        }
                     },
                     "x-amazon-apigateway-integration": {
                        "type": "AWS",
                        "credentials": "arn:aws:iam::123456789012:role/Lambda",
                        "httpMethod": "POST",
                        "requestTemplates": {
                           "application/json": "\n                           
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
"responses": {
  "default": {
    "statusCode": "500"
  },
  "2\d{2}": {
    "statusCode": "200",
    "responseTemplates": {
      "application/json": "{\n        "image": "$input.body"\n      }"
    }
  }
},
"put": {
  "produces": [
    "application/json", "application/octet-stream"
  ],
  "parameters": [
    {
      "name": "key",
      "in": "query",
      "required": false,
      "type": "string"
    }
  ],
  "responses": {
    "200": {
      "description": "200 response",
      "schema": {
        "$ref": "#/definitions/Empty"
      }
    },
    "500": {
      "description": "500 response"
    }
  },
  "x-amazon-apigateway-integration": {
    "type": "AWS",
    "credentials": "arn:aws:iam::123456789012:role/Lambda",
    "httpMethod": "POST",
    "contentHandling": "CONVERT_TO_TEXT",
    "requestTemplates": {
      "application/json": "{\n        "imageKey": "$input.params('key')", "image": "$input.body"\n      }"
    },
    "responses": {
      "default": {
        "statusCode": "500"
      },
      "2\d{2}": {
        "statusCode": "200"
      }
    }
  }
},
"x-amazon-apigateway-binary-media-types": ["application/octet-stream", "image/jpeg"],
"definitions": {
  "Empty": {
    "type": "object",
    "title": "Empty Schema"
  }
}
Download an Image from Lambda

To download an image file (image.jpg) as a binary blob from Lambda:

```
GET /v1/lambda?key=image.jpg HTTP/1.1
Host: abcdefghi.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/octet-stream
```

The successful response looks like this:

```
200 OK HTTP/1.1
[
]
```

To download an image file (image.jpg) as a Base64-encoded string, formatted as a JSON property, from Lambda:

```
GET /v1/lambda?key=image.jpg HTTP/1.1
Host: abcdefghi.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```

The successful response looks like this:

```
200 OK HTTP/1.1

{
    "image": "W3JhdyBieXRlc10=
}
```

Upload an Image to Lambda

To upload an image file (image.jpg) as a binary blob to Lambda:

```
PUT /v1/lambda?key=image.jpg HTTP/1.1
Host: abcdefghi.execute-api.us-east-1.amazonaws.com
Content-Type: application/octet-stream
Accept: application/json
```

The successful response looks like this:

```
200 OK
```

To upload an image file (image.jpg) as a Base64-encoded string to Lambda:

```
PUT /v1/lambda?key=image.jpg HTTP/1.1
Host: abcdefghi.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```
Enable Payload Compression for an API

API Gateway allows your client to call your API with compressed payloads using one of the supported content codings (p. 326). By default, API Gateway supports decompression of the method request payload. However, you must configure your API to enable compression of the method response payload.

To enable compression on an API, set the `minimumCompressionsSize` property to a non-negative integer between 0 and 10485760 (10M bytes) when you create the API or after you've created the API. To disable compression on the API, set the `minimumCompressionSize` to null or remove it altogether. You can enable or disable compression for an API by using the API Gateway console, the AWS CLI, or the API Gateway REST API.

If you want the compression applied on a payload of any size, set the `minimumCompressionSize` value to zero. However, compressing data of a small size might actually increase the final data size. Furthermore, compression in API Gateway and decompression in the client might increase overall latency and require more computing times. You should run test cases against your API to determine an optimal value.

The client can submit an API request with a compressed payload and an appropriate `Content-Encoding` header for API Gateway to decompress the method request payload and apply applicable mapping templates, before passing the request to the integration endpoint. After the compression is enabled and the API is deployed, the client can receive an API response with a compressed payload if it specifies an appropriate `Accept-Encoding` header in the method request.

When the integration endpoint expects and returns uncompressed JSON payloads, any mapping template that's configured for an uncompressed JSON payload is applicable to the compressed payload. For a compressed method request payload, API Gateway decompresses the payload, applies the template, and passes the mapped request to the integration endpoint. For an uncompressed integration response payload, API Gateway applies the mapping template, compresses the mapped payload, and returns the compressed payload to the client.

**Topics**

- Enable Payload Compression for an API (p. 325)
- Call an API Method with a Compressed Payload (p. 327)
- Receive an API Response with a Compressed Payload (p. 327)

Enable Payload Compression for an API

You can enable compression for an API using the API Gateway console, the AWS CLI, or an AWS SDK.

For an existing API, you must deploy the API after enabling the compression in order for the change to take effect. For a new API, you can deploy the API after the API setup is complete.

**Note**

The highest-priority content encoding must be one supported by API Gateway. If it is not, compression is not applied to the response payload.

**Topics**
Enable Payload Compression for an API Using the API Gateway Console

The following procedure describes how to enable payload compression for an API.

To enable payload compression by using the API Gateway console

1. Sign in to the API Gateway console.
2. Choose an existing API or create a new one.
3. In the primary navigation pane, choose Settings under the API you chose or the one you created.
4. Under the Content Encoding section in the Settings pane, select the Content Encoding enabled option to enable payload compression. Type a number for the minimum compression size (in bytes) next to Minimum body size required for compression. To disable the compression, clear the Content Encoding enabled option.
5. Choose Save Changes.

Enable Payload Compression for an API Using AWS CLI

To use the AWS CLI to create a new API and enable compression, call the create-rest-api command as follows:

```bash
aws apigateway create-rest-api \
--name "My test API" \n--minimum-compression-size 0
```

To use the AWS CLI to enable compression on an existing API, call the update-rest-api command as follows:

```bash
aws apigateway update-rest-api \
--rest-api-id 1234567890 \n--patch-operations op=replace,path=/minimumCompressionSize,value=0
```

The minimumCompressionSize property has a non-negative integer value between 0 and 10485760 (10M bytes). It measures the compression threshold. If the payload size is smaller than this value, compression or decompression are not applied on the payload. Setting it to zero allows compression for any payload size.

To use the AWS CLI to disable compression, call the update-rest-api command as follows:

```bash
aws apigateway update-rest-api \
--rest-api-id 1234567890 \n--patch-operations op=replace,path=/minimumCompressionSize,value=
```

You can also set value to an empty string "" or omit the value property altogether in the preceding call.

Content Codings Supported by API Gateway

API Gateway supports the following content codings:

- deflate
Enable Payload Compression

- gzip
- identity

API Gateway also supports the following Accept-Encoding header format, according to the RFC 7231 specification:

- Accept-Encoding: deflate, gzip
- Accept-Encoding: *
- Accept-Encoding: deflate;q=0.5, gzip=1.0
- Accept-Encoding: gzip;q=1.0, identity;q=0.5, *;q=0

Call an API Method with a Compressed Payload

To make an API request with a compressed payload, the client must set the Content-Encoding header with one of the supported content codings (p. 326).

Suppose that you're an API client and want to call the PetStore API method (POST /pets). Don't call the method by using the following JSON output:

```json
POST /pets
Host: {petstore-api-id}.execute-api.{region}.amazonaws.com
Content-Length: ...
{
  "type": "dog",
  "price": 249.99
}
```

Instead, you can call the method with the same payload compressed by using the GZIP coding:

```json
POST /pets
Host: {petstore-api-id}.execute-api.{region}.amazonaws.com
Content-Encoding: gzip
Content-Length: ...
```

When API Gateway receives the request, it verifies if the specified content coding is supported. Then, it attempts to decompress the payload with the specified content coding. If the decompression is successful, it dispatches the request to the integration endpoint. If the specified coding isn't supported or the supplied payload isn't compressed with specified coding, API Gateway returns the 415 Unsupported Media Type error response. The error is not be logged to CloudWatch Logs, if it occurs in the early phase of decompression before your API and stage are identified.

Receive an API Response with a Compressed Payload

When making a request on a compression-enabled API, the client can choose to receive a compressed response payload of a specific format by specifying an Accept-Encoding header with a supported content coding (p. 326).

API Gateway only compresses the response payload when the following conditions are satisfied:

- The incoming request has the Accept-Encoding header with a supported content coding and format.
Note
If the header is not set, the default value is * as defined in RFC 7231. In such a case, API Gateway will not compress the payload. Some browser or client may add Accept-Encoding (for example, Accept-Encoding: gzip, deflate, br) automatically to compression-enabled requests. This can trigger the payload compression in API Gateway. Without an explicit specification of supported Accept-Encoding header values, API Gateway does not compress the payload.

- The minimumCompressionSize is set on the API to enable compression.
- The integration response doesn't have a Content-Encoding header.
- The size of an integration response payload, after the applicable mapping template is applied, is greater than or equal to the specified minimumCompressionSize value.

API Gateway applies any mapping template that's configured for the integration response before compressing the payload. If the integration response contains a Content-Encoding header, API Gateway assumes that the integration response payload is already compressed and skips the compression processing.

An example is the PetStore API example and the following request:

```plaintext
GET /pets
Host: {petstore-api-id}.execute-api.{region}.amazonaws.com
Accept: application/json
```

The backend responds to the request with an uncompressed JSON payload that's similar to the following:

```
200 OK
[
  {
    "id": 1,
    "type": "dog",
    "price": 249.99
  },
  {
    "id": 2,
    "type": "cat",
    "price": 124.99
  },
  {
    "id": 3,
    "type": "fish",
    "price": 0.99
  }
]
```

To receive this output as a compressed payload, your API client can submit a request as follows:

```plaintext
GET /pets
Host: {petstore-api-id}.execute-api.{region}.amazonaws.com
Accept-Encoding: gzip
```

The client receives the response with a Content-Encoding header and GZIP-encoded payload that are similar to the following:

```
200 OK
Content-Encoding:gzip
```
Enable Request Validation in API Gateway

You can configure API Gateway to perform basic validation of an API request before proceeding with the integration request. When the validation fails, API Gateway immediately fails the request, returns a 400 error response to the caller, and publishes the validation results in CloudWatch Logs. This reduces unnecessary calls to the backend. More importantly, it lets you focus on the validation efforts specific to your application.

Topics
- Overview of Basic Request Validation in API Gateway (p. 329)
- Set up Basic Request Validation in API Gateway (p. 329)
- Test Basic Request Validation in API Gateway (p. 335)
- OpenAPI Definitions of a Sample API with Basic Request Validation (p. 338)

Overview of Basic Request Validation in API Gateway

API Gateway can perform the basic validation. This enables you, the API developer, to focus on app-specific deep validation in the backend. For the basic validation, API Gateway verifies either or both of the following conditions:

- The required request parameters in the URI, query string, and headers of an incoming request are included and non-blank.
- The applicable request payload adheres to the configured JSON schema request model (p. 268) of the method.

To enable basic validation, you specify validation rules in a request validator, add the validator to the API's map of request validators, and assign the validator to individual API methods.

Note

Request body validation and request body passthrough (p. 292) are two separate issues. When a request payload cannot be validated because no model schema can be matched, you can choose to passthrough or block the original payload. For example, when you enable request validation with a mapping template for the application/json media type, you may want to pass an XML payload through to the backend even though the enabled request validation will fail. This may be the case if you expect to support the XML payload on the method in the future. To fail the request with an XML payload, you must explicitly choose the NEVER option for the content passthrough behavior.

Set up Basic Request Validation in API Gateway

You can set up request validators in an API's OpenAPI definition file and then import the OpenAPI definitions into API Gateway. You can also set them up in the API Gateway console or by calling the API Gateway REST API, AWS CLI, or one of the AWS SDKs. Here, we show how to do this with an OpenAPI file, in the console, and using the API Gateway REST API.

Topics
Enable Request Validation

- Set up Basic Request Validation by Importing OpenAPI Definition (p. 330)
- Set up Request Validators Using the API Gateway REST API (p. 333)
- Set up Basic Request Validation Using the API Gateway Console (p. 334)

Set up Basic Request Validation by Importing OpenAPI Definition

The following steps describe how to enable basic request validation by importing an OpenAPI file.

To enable request validation by importing an OpenAPI file into API Gateway

1. Declare request validators in OpenAPI by specifying a set of the `x-amazon-apigateway-request-validators` objects in the `x-amazon-apigateway-request-validators Object` map at the API level. For example, the sample API OpenAPI file (p. 338) contains the `x-amazon-apigateway-request-validators map`, with the validators’ names as the keys.

OpenAPI 3.0

```json
{
  "openapi": "3.0.0",
  "info": {
    "title": "ReqValidation Sample",
    "version": "1.0.0"
  },
  "servers": [
    {
      "url": "/{basePath}"
    }
  ],
  "x-amazon-apigateway-request-validators": {
    "all": {
      "validateRequestBody": true,
      "validateRequestParameters": true
    },
    "params-only": {
      "validateRequestBody": false,
      "validateRequestParameters": true
    }
  }
}
```

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "title": "ReqValidation Sample",
    "version": "1.0.0"
  },
  "schemes": ["https"],
  "basePath": "/v1",
  "produces": [
    "application/json"
  ],
  "x-amazon-apigateway-request-validators": {
```
Enable Request Validation

```
"all" : {
    "validateRequestBody" : true,
    "validateRequestParameters" : true
},
"params-only" : {
    "validateRequestBody" : false,
    "validateRequestParameters" : true
}
```

You select a validator's name when enabling the validator on the API or on a method, as shown in the next step.

2. To enable a request validator on all methods of an API, specify an `x-amazon-apigateway-request-validator` property at the API level of the OpenAPI definition file. To enable a request validator on an individual method, specify the `x-amazon-apigateway-request-validator` property at the method level. For example, the following `x-amazon-apigateway-request-validator` property enables the `params-only` validator on all API methods, unless otherwise overridden.

**OpenAPI 3.0**

```
{
    "openapi": "3.0.0",
    "info": {
        "title": "ReqValidation Sample",
        "version": "1.0.0"
    },
    "servers": [
        {
            "url": "/{basePath}",
            "variables": {
                "basePath": {
                    "default": "/v1"
                }
            }
        }
    ],
    "x-amazon-apigateway-request-validator": "params-only",
    ...
}
```

**OpenAPI 2.0**

```
{
    "swagger": "2.0",
    "info": {
        "title": "ReqValidation Sample",
        "version": "1.0.0"
    },
    "schemes": [
        "https"
    ],
    "basePath": "/v1",
    "produces": [
        "application/json"
    ],
    ...
    "x-amazon-apigateway-request-validator" : "params-only",
    ...
}
To enable a request validator on an individual method, specify the `x-amazon-apigateway-request-validator` property at the method level. For example, the following `x-amazon-apigateway-request-validator` property enables the `all` validator on the `POST /validation` method. This overrides the `params-only` validator that is inherited from the API.

**OpenAPI 3.0**

```json
{
  "openapi": "3.0.0",
  "info": {
    "title": "ReqValidation Sample",
    "version": "1.0.0"
  },
  "servers": [
    {
      "url": "/{basePath}"
    }
  ],
  "paths": {
    "/validation": {
      "post": {
        "x-amazon-apigateway-request-validator": "all",
        ...
      }
    }
  }
}
```

**OpenAPI 2.0**

```json
{
  "swagger": "2.0",
  "info": {
    "title": "ReqValidation Sample",
    "version": "1.0.0"
  },
  "schemes": ["https"],
  "basePath": "/v1",
  "produces": ["application/json"],
  ...
  "paths": {
    "/validation": {
      "post": {
        "x-amazon-apigateway-request-validator": "all",
        ...
      }
    }
  }
}
```
3. In API Gateway, create the API with request validators enabled by importing this sample OpenAPI definition (p. 338):

```plaintext
POST /restapis?mode=import&failonwarning=true HTTP/1.1
Content-Type: application/json
Host: apigateway.us-east-1.amazonaws.com
X-Amz-Date: 20170306T234936Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170306/us-east-1/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature={sig4_hash}

Copy the JSON object from this sample OpenAPI definition (p. 338) and paste it here.
```

4. Deploy the newly created API (fjd6crafxc) to a specified stage (testStage).

```plaintext
POST /restapis/fjd6crafxc/deployments HTTP/1.1
Content-Type: application/json
Host: apigateway.us-east-1.amazonaws.com
X-Amz-Date: 20170306T234936Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170306/us-east-1/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature={sig4_hash}

{
    "stageName" : "testStage",
    "stageDescription" : "Test stage",
    "description" : "First deployment",
    "cacheClusterEnabled" : "false"
}
```

For instructions on how to test the request validation using the API Gateway REST API, see Test Basic Request Validation Using the API Gateway REST API (p. 335). For instructions on how to test using the API Gateway console, see Test Basic Request Validation Using the API Gateway Console (p. 338).

Set up Request Validators Using the API Gateway REST API

In the API Gateway REST API, a request validator is represented by a RequestValidator resource. To have an API support the same request validators as the Sample API (p. 338), add to the RequestValidators collection a parameters-only validator with `params-only` as the key, and add a full validator with `all` as its key.

To enable the basic request validation using the API Gateway REST API

We assume that you have an API similar to the sample API (p. 338), but have not set up the request validators. If your API already has request validators enabled, call the appropriate `requestvalidator:update` or `method:put` action instead of `requestvalidator:create` or `method:put`.

1. To set up the `params-only` request validator, call the `requestvalidator:create` action as follows:

```plaintext
POST /restapis/restapi-id/requestvalidators HTTP/1.1
Content-Type: application/json
Host: apigateway.region.amazonaws.com
X-Amz-Date: 20170223T172652Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170223/region/apigateway/aws4_request, SignedHeaders=content-type;host;x-amz-date, Signature={sig4_hash}

{
}
```
Enable Request Validation

2. To set up the all request validator, call the requestvalidator:create action as follows:

```
POST /restapis/restapi-id/requestvalidators HTTP/1.1
Content-Type: application/json
Host: apigateway.region.amazonaws.com
X-Amz-Date: 20170223T172652Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170223/region/apigateway/ aws4_request, SignedHeaders=content-type;host;x-amz-date, Signature={sig4_hash}

{
    "name" : "all",
    "validateRequestBody" : "true",
    "validateRequestParameters" : "true"
}
```

If the preceding validator keys already exist in the RequestValidators map, call the requestvalidator:update action instead to reset the validation rules.

3. To apply the all request validator to the POST method, call method:put to enable the specified validator (as identified by the requestValidatorId property) or call method:update to update the enabled validator.

```
PUT /restapis/restapi-id/resources/resource-id/methods/POST HTTP/1.1
Content-Type: application/json
Host: apigateway.region.amazonaws.com
X-Amz-Date: 20170223T172652Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170223/region/apigateway/ aws4_request, SignedHeaders=content-type;host;x-amz-date, Signature={sig4_hash}

{
    "authorizationType" : "NONE",
    ...
    "requestValidatorId" : "all"
}
```

Set up Basic Request Validation Using the API Gateway Console

The API Gateway console lets you set up the basic request validation on a method using one of the three validators:

- **Validate body**: This is the body-only validator.
- **Validate query string parameters and headers**: This is the parameters-only validator.
- **Validate body, query string parameters, and headers**: This validator is for both body and parameters validation.

When you choose one of the above validators to enable it on an API method, the API Gateway console will add the validator to the API's RequestValidators map, if the validator has not already been added to the validators map of the API.

To enable a request validator on a method

1. Sign in to the API Gateway console, if not already logged in.
2. Create a new or choose an existing API.
Enable Request Validation

3. Create a new or choose an existing resource of the API.
4. Create a new or choose an existing method the resource.
5. Choose Method Request.
6. Choose the pencil icon of Request Validator under Settings.
7. Choose Validate body, Validate query string parameters and headers or Validate body, query string parameters, and headers from the Request Validator drop-down list and then choose the check mark icon to save your choice.

To test and use the request validator in the console, follow the instructions in Test Basic Request Validation Using the API Gateway Console (p. 338).

Test Basic Request Validation in API Gateway

Choose one of the following topics for instructions on testing the basic request validation against the sample API (p. 338).

Topics
- Test Basic Request Validation Using the API Gateway REST API (p. 335)
- Test Basic Request Validation Using the API Gateway Console (p. 338)

Test Basic Request Validation Using the API Gateway REST API

To see the invocation URL of the deployed API, you can export the API from the stage, making sure to include the Accept: application/json or Accept: application/yaml header:

```
GET /restapis/fjd6crafxc/stages/testStage/exports/swagger?extensions=validators HTTP/1.1
Accept: application/json
Content-Type: application/json
Host: apigateway.us-east-1.amazonaws.com
X-Amz-Date: 20170306T234936Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20170306/us-east-1/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature={sig4_hash}
```

You can ignore the ?extensions=validators query parameter, if you do not want to download the OpenAPI specifications related to the request validation.

To test request validation using the API Gateway REST API calls

1. Call GET /validation?q1=cat.
Enable Request Validation

```
GET /testStage/validation?q1=cat HTTP/1.1
Host: fjd6crafxc.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```

Because the required parameter of q1 is set and not blank, the request passes the validation. API Gateway returns the following 200 OK response:

```
{
  "id": 1,
  "type": "cat",
  "price": 249.99
},
{
  "id": 2,
  "type": "cat",
  "price": 124.99
},
{
  "id": 3,
  "type": "cat",
  "price": 0.99
}
```

2. Call `GET /validation`.

```
GET /testStage/validation HTTP/1.1
Host: fjd6crafxc.beta.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```

Because the required parameter of q1 is not set, the request fails to pass the validation. API Gateway returns the following 400 Bad Request response:

```
{
  "message": "Missing required request parameters: [q1]"
}
```

3. Call `GET /validation?q1=`.

```
GET /testStage/validation?q1= HTTP/1.1
Host: fjd6crafxc.beta.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```

Because the required parameter of q1 is blank, the request fails to pass the validation. API Gateway returns the same 400 Bad Request response as in the previous example.

4. Call `POST /validation`.

```
POST /testStage/validation HTTP/1.1
Host: fjd6crafxc.beta.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
```

Because the required parameter of q1 is blank, the request fails to pass the validation. API Gateway returns the same 400 Bad Request response as in the previous example.
Because the required header parameter of h1 is set and not blank and the payload format adheres to the RequestDataModel required properties and associated constraints, the request passes the validation. API Gateway returns the following successful response.

```json
{
  "pet": {
    "name": "Marco",
    "type": "dog",
    "price": 260
  },
  "message": "success"
}
```

5. Call POST /validation, without specifying the h1 header or setting its value blank.

```shell
POST /testStage/validation HTTP/1.1
Host: fjd6crafxc.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json

{
  "name": "Marco",
  "type": "dog",
  "price": 260
}
```

Because the required header parameter of h1 is missing or set to blank, the request fails to pass the validation. API Gateway returns the following 400 Bad Request response:

```json
{
  "message": "Missing required request parameters: [h1]"
}
```

6. Call POST /validation, setting the type property of the payload to bird.

```shell
POST /testStage/validation HTTP/1.1
Host: fjd6crafxc.execute-api.us-east-1.amazonaws.com
Content-Type: application/json
Accept: application/json
X-Amz-Date: 20170309T000215Z
h1: v1

{
  "name": "Molly",
  "type": "bird",
  "price": 269
}
```

Because the type property value is not a member of the enumeration of ["dog", "cat", "fish"], the request fails to pass the validation. API Gateway returns the following 400 Bad Request response:

```json
{
  "message": "Invalid request body"
}
```
Setting `price` to 501 violates the constraint on the property. This causes the validation to fail and the same 400 Bad Request response is returned.

**Test Basic Request Validation Using the API Gateway Console**

The following steps describe how to test basic request validation in the API Gateway console.

**To test the request validation on a method using TestInvoke in the API Gateway console**

While signed in to the API Gateway console, do the following:

1. Choose **Resources** for the API for which you have configured a request validators map.
2. Choose a method for which you have enabled the request validation with a specified request validator.
3. Under **Method Execution**, in the **Client** box, choose **Test**.
4. Try different values for required request parameter or applicable body, and then choose **Test** to see the response.

When the method call passes validation, you should get expected responses. If validation fails, the following error message returns if the payload is not the correct format:

```json
{
  "message": "Invalid request body"
}
```

If the request parameters are not valid, the following error message returns:

```json
{
  "message": "Missing required request parameters: [p1]"
}
```

**OpenAPI Definitions of a Sample API with Basic Request Validation**

The following OpenAPI definition defines a sample API with request validation enabled. The API is a subset of the PetStore API. It exposes a `POST` method to add a pet to the `pets` collection and a `GET` method to query pets by a specified type.

There are two request validators declared in the `x-amazon-apigateway-request-validators` map at the API level. The `params-only` validator is enabled on the API and inherited by the `GET` method. This validator allows API Gateway to verify that the required query parameter (`q1`) is included and not blank in the incoming request. The `all` validator is enabled on the `POST` method. This validator verifies that the required header parameter (`h1`) is set and not blank. It also verifies that the payload format adheres to the specified `RequestBodyModel` schema. This model requires that the input JSON object contains the `name`, `type`, and `price` properties. The `name` property can be any string, `type` must be one of the specified enumeration fields ("dog", "cat", "fish"), and `price` must range between 25 and 500. The `id` parameter is not required.

For more information about the behavior of this API, see Enable Request Validation in API Gateway (p. 329).
OpenAPI 2.0

{
    "swagger": "2.0",
    "info": {
        "title": "ReqValidators Sample",
        "version": "1.0.0"
    },
    "schemes": [ "https" ],
    "basePath": "/v1",
    "produces": [ "application/json" ],
    "x-amazon-apigateway-request-validators" : {
        "all" : {
            "validateRequestBody" : true,
            "validateRequestParameters" : true
        },
        "params-only" : {
            "validateRequestBody" : false,
            "validateRequestParameters" : true
        }
    },
    "x-amazon-apigateway-request-validator" : "params-only",
    "paths": {
        "/validation": {
            "post": {
                "x-amazon-apigateway-request-validator" : "all",
                "parameters": [
                    {
                        "in": "header",
                        "name": "hi",
                        "required": true
                    },
                    {
                        "in": "body",
                        "name": "RequestBodyModel",
                        "required": true,
                        "schema": {
                            "$ref": "#/definitions/RequestBodyModel"
                        }
                    }
                ],
                "responses": {
                    "200": {
                        "schema": {
                            "type": "array",
                            "items": {
                                "$ref": "#/definitions/Error"
                            }
                        },
                        "headers" : {
                            "test-method-response-header" : {
                                "type": "string"
                            }
                        }
                    }
                },
                "security" : [{
                    "api_key" : []
                }],
                "x-amazon-apigateway-auth" : {
                    "type" : "none"
                }
            }
        }
    }
}
"x-amazon-apigateway-integration": {
  "type": "http",
  "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets",
  "httpMethod": "POST",
  "requestParameters": {
    "integration.request.header.custom_h1": "method.request.header.h1"
  },
  "responses": {
    "2\d{2}": {
      "statusCode": "200"
    },
    "default": {
      "statusCode": "400",
      "responseParameters": {
        "method.response.header.test-method-response-header": "'static value'"
      },
      "responseTemplates": {
        "application/json": "json 400 response template",
        "application/xml": "xml 400 response template"
      }
    }
  }
},
"get": {
  "parameters": [
    {
      "name": "q1",
      "in": "query",
      "required": true
    }
  ],
  "responses": {
    "200": {
      "schema": {
        "type": "array",
        "items": {
          "$ref": "#/definitions/Error"
        }
      },
      "headers": {
        "test-method-response-header": {
          "type": "string"
        }
      }
    }
  },
  "security": [{
    "api_key": []
  }],
  "x-amazon-apigateway-auth": {
    "type": "none"
  },
  "x-amazon-apigateway-integration": {
    "type": "http",
    "uri": "http://petstore-demo-endpoint.execute-api.com/petstore/pets",
    "httpMethod": "GET",
    "requestParameters": {
      "integration.request.querystring.type": "method.request.querystring.q1"
    },
    "responses": {
      "2\d{2}": {
        "statusCode": "200"
      },
      "default": {

Import a REST API into API Gateway

You can use the API Gateway Import API feature to import a REST API from an external definition file into API Gateway. Currently, the Import API feature supports OpenAPI v2.0 and OpenAPI v3.0 definition files. You can update an API by overwriting it with a new definition, or merge a definition with an existing API. You specify the options using a mode query parameter in the request URL.

For a tutorial on using the Import API feature from the API Gateway console, see TUTORIAL: Create a REST API by Importing an Example (p. 42).

Topics
- Import an Edge-Optimized API into API Gateway (p. 341)
- Import a Regional API into API Gateway (p. 342)
- Import an OpenAPI File to Update an Existing API Definition (p. 343)
- Set the OpenAPI basePath Property (p. 344)
- Errors and Warnings during Import (p. 346)

Import an Edge-Optimized API into API Gateway

You can import an API's OpenAPI definition file to create a new edge-optimized API by specifying the EDGE endpoint type as an additional input, besides the OpenAPI file, to the import operation. You can do so using the API Gateway console, AWS CLI, or an AWS SDK.
For a tutorial on using the Import API feature from the API Gateway console, see TUTORIAL: Create a REST API by Importing an Example (p. 42).

Topics
- Import an Edge-Optimized API Using the API Gateway Console (p. 342)
- Import an Edge-Optimized API Using the AWS CLI (p. 342)

Import an Edge-Optimized API Using the API Gateway Console

To import an edge-optimized API using the API Gateway console, do the following:

1. Sign in to the API Gateway console and choose + Create API.
2. Select the Import from OpenAPI option under Create new API.
3. Copy an API's OpenAPI definition and paste it into the code editor, or choose Select OpenAPI File to load an OpenAPI file from a local drive.
4. Under Settings, for Endpoint Type, choose Edge optimized.
5. Choose Import to start importing the OpenAPI definitions.

Import an Edge-Optimized API Using the AWS CLI

To import an API from an OpenAPI definition file to create a new edge-optimized API using the AWS CLI, use the import-rest-api command as follows:

```
aws apigateway import-rest-api \
  --fail-on-warnings \
  --body 'file://path/to/API_OpenAPI_template.json'
```

or with an explicit specification of the endpointConfigurationTypes query string parameter to EDGE:

```
aws apigateway import-rest-api \
  --endpointConfigurationTypes=EDGE \
  --fail-on-warnings \
  --body 'file://path/to/API_OpenAPI_template.json'
```

Import a Regional API into API Gateway

When importing an API, you can choose the regional endpoint configuration for the API. You can use the API Gateway console, the AWS CLI, or an AWS SDK.

When you export an API, the API endpoint configuration is not included in the exported API definitions.

For a tutorial on using the Import API feature from the API Gateway console, see TUTORIAL: Create a REST API by Importing an Example (p. 42).

Topics
- Import a Regional API Using the API Gateway Console (p. 342)
- Import a Regional API Using the AWS CLI (p. 343)

Import a Regional API Using the API Gateway Console

To import an API of a regional endpoint using the API Gateway console, do the following:
1. Sign in to the API Gateway console and choose **Create API**.
2. Select the **Import from OpenAPI** option under **Create new API**.
3. Copy an API's OpenAPI definition and paste it into the code editor, or choose **Select OpenAPI File** to load an OpenAPI file from a local drive.
4. Under **Settings**, for **Endpoint Type**, choose **Regional**.
5. Choose **Import** to start importing the OpenAPI definitions.

**Import a Regional API Using the AWS CLI**

To import an API from an OpenAPI definition file using the AWS CLI, use the `import-rest-api` command:

```bash
aws apigateway import-rest-api \
  --endpointConfigurationTypes 'REGIONAL' \
  --fail-on-warnings \
  --body 'file://path/to/API_OpenAPI_template.json'
```

**Import an OpenAPI File to Update an Existing API Definition**

You can import API definitions only to update an existing API, without changing its endpoint configuration, as well as stages and stage variables, or references to API Keys.

The import-to-update operation can occur in two modes: merge or overwrite.

When an API (A) is merged into another (B), the resulting API retains the definitions of both A and B if the two APIs do not share any conflicting definitions. When conflicts arise, the method definitions of the merging API (A) overrides the corresponding method definitions of the merged API (B). For example, suppose B has declared the following methods to return 200 and 206 responses:

- GET /a
- POST /a

and A declares the following method to return 200 and 400 responses:

- GET /a

When A is merged into B, the resulting API will yield the following methods:

- GET /a

which will return 200 and 400 responses, and

- POST /a

which will return 200 and 206 responses.

Merging an API is useful when you have decomposed your external API definitions into multiple, smaller parts and only want to apply changes from one of those parts at a time. For example, this might occur if multiple teams are responsible for different parts of an API and have changes available at different rates. In this mode, items from the existing API that are not specifically defined in the imported definition will be left alone.
When an API (A) overwrites another API (B), the resulting API takes the definitions of the overwriting API (A). Overwriting an API is useful when an external API definition contains the complete definition of an API. In this mode, items from an existing API that are not specifically defined in the imported definition will be deleted.

To merge an API, submit a PUT request to https://apigateway.<region>.amazonaws.com/restapis/<restapi_id>?mode=merge. The restapi_id path parameter value specifies the API to which the supplied API definition will be merged.

The following code snippet shows an example of the PUT request to merge an OpenAPI API definition in JSON, as the payload, with the specified API already in API Gateway:

```
PUT /restapis/<restapi_id>?mode=merge
Host:apigateway.<region>.amazonaws.com
Content-Type: application/json
Content-Length: ...

An OpenAPI API definition in JSON (p. 107)
```

The merging update operation takes two complete API definitions and merges them together. For a small and incremental change, you can use the resource update operation.

To overwrite an API, submit a PUT request to https://apigateway.<region>.amazonaws.com/restapis/<restapi_id>?mode=overwrite. The restapi_id path parameter specifies the API that will be overwritten with the supplied API definitions.

The following code snippet shows an example of an overwriting request with the payload of a JSON-formatted OpenAPI definition:

```
PUT /restapis/<restapi_id>?mode=overwrite
Host:apigateway.<region>.amazonaws.com
Content-Type: application/json
Content-Length: ...

An OpenAPI API definition in JSON (p. 107)
```

When the mode query parameter is not specified, merge is assumed.

**Note**
The PUT operations are idempotent, but not atomic. That means if a system error occurs part way through processing, the API can end up in a bad state. However, repeating the operation will put the API into the same final state as if the first operation had succeeded.

### Set the OpenAPI **basePath** Property

In OpenAPI 2.0, you can use the `basePath` property to provide one or more path parts that precede each path defined in the `paths` property. Because API Gateway has several ways to express a resource's path, the Import API feature provides the following options for interpreting the `basePath` property during import: ignore, prepend, and split.

In OpenAPI 3.0, `basePath` is no longer a top-level property. Instead, API Gateway uses a server variable as a convention. The Import API feature provides the same options for interpreting the base path during import. The base path is identified as follows:
• If the API doesn’t contain any `basePath` variables, the Import API feature checks the `server.url` string to see if it contains a path beyond "/". If it does, that path is used as the base path.
• If the API contains only one `basePath` variable, the Import API feature uses it as the base path, even if it’s not referenced in the `server.url`.
• If the API contains multiple `basePath` variables, the Import API feature uses only the first one as the base path.

**ignore**

If the OpenAPI file has a `basePath` value of `/a/b/c` and the `paths` property contains `/e` and `/f`, the following POST or PUT request:

```plaintext
POST /restapis?mode=import&basepath=ignore

PUT /restapis/api_id?basepath=ignore
```

will result in the following resources in the API:

• /
• /e
• /f

The effect is to treat the `basePath` as if it was not present, and all of the declared API resources are served relative to the host. This can be used, for example, when you have a custom domain name with an API mapping that does not include a `Base Path` and a `Stage` value that refers to your production stage.

**Note**
API Gateway will automatically create a root resource for you, even if it is not explicitly declared in your definition file.

When unspecified, `basePath` takes `ignore` by default.

**prepend**

If the OpenAPI file has a `basePath` value of `/a/b/c` and the `paths` property contains `/e` and `/f`, the following POST or PUT request:

```plaintext
POST /restapis?mode=import&basepath=prepend

PUT /restapis/api_id?basepath=prepend
```

will result in the following resources in the API:

• /
• /a
• /b
• /a/b/c
• /a/b/c/e
• /a/b/c/f
The effect is to treat the `basePath` as specifying additional resources (without methods) and to add them to the declared resource set. This can be used, for example, when different teams are responsible for different parts of an API and the `basePath` could reference the path location for each team's API part.

**Note**

API Gateway will automatically create intermediate resources for you, even if they are not explicitly declared in your definition.

**split**

If the OpenAPI file has a `basePath` value of `/a/b/c` and the `paths` property contains `/e` and `/f`, the following POST or PUT request:

```text
POST /restapis?mode=import&basePath=split
```

```text
PUT /restapis/api_id?basePath=split
```

will result in the following resources in the API:

- `/`
- `/b`
- `/b/c`
- `/b/c/e`
- `/b/c/f`

The effect is to treat top-most path part, `/a`, as the beginning of each resource's path, and to create additional (no method) resources within the API itself. This could, for example, be used when `a` is a stage name that you want to expose as part of your API.

**Errors and Warnings during Import**

**Errors during Import**

During the import, errors can be generated for major issues like an invalid OpenAPI document. Errors are returned as exceptions (for example, `BadRequestException`) in an unsuccessful response. When an error occurs, the new API definition is discarded and no change is made to the existing API.

**Warnings during Import**

During the import, warnings can be generated for minor issues like a missing model reference. If a warning occurs, the operation will continue if the `failonwarnings=false` query expression is appended to the request URL. Otherwise, the updates will be rolled back. By default, `failonwarnings` is set to `false`. In such cases, warnings are returned as a field in the resulting `RestApi` resource. Otherwise, warnings are returned as a message in the exception.

**Controlling and Managing Access to a REST API in API Gateway**

API Gateway supports multiple mechanisms for controlling and managing access to your API.
The following mechanisms can be used for authentication and authorization:

- **Resource policies** let you create resource-based policies to allow or deny access to your APIs and methods from specified source IP addresses or VPC endpoints. For more information, see the section called "Use API Gateway Resource Policies" (p. 347).

- **Standard AWS IAM roles and policies** offer flexible and robust access controls that can be applied to an entire API or individual methods. IAM roles and policies can be used for controlling who can create and manage your APIs as well as who can invoke them. For more information, see the section called "Use IAM Permissions" (p. 362).

- **IAM tags** can be used together with IAM policies to control access. For more information, see the section called "Tag-Based Access Control" (p. 682).

- **Endpoint Policies for Interface VPC Endpoints** allow you to attach IAM resource policies to interface VPC endpoints to improve the security of your private APIs. For more information, see the section called "Use VPC Endpoint Policies for Private APIs" (p. 378).

- **Lambda authorizers** are Lambda functions that control access to REST API methods using bearer token authentication as well as information described by headers, paths, query strings, stage variables, or context variables request parameters. Lambda authorizers are used to control who can invoke REST API methods. For more information, see the section called "Use Lambda Authorizers" (p. 380).

- **Amazon Cognito user pools** let you create customizable authentication and authorization solutions for your REST APIs. Amazon Cognito user pools are used to control who can invoke REST API methods. For more information, see the section called "Use Cognito User Pool as Authorizer for a REST API" (p. 397).

The following mechanisms can be used for performing other tasks related to access control:

- **Cross-origin resource sharing (CORS)** lets you control how your REST API responds to cross-domain resource requests. For more information, see the section called "Enable CORS for a REST API Resource" (p. 405).

- **Client-side SSL certificates** can be used to verify that HTTP requests to your backend system are from API Gateway. For more information, see the section called "Generate and Configure an SSL Certificate for Backend Authentication" (p. 411).

- **AWS WAF** can be used to protect your API Gateway API from common web exploits. For more information, see the section called "Use AWS WAF to Protect Your API from Common Web Exploits" (p. 430).

The following mechanisms can be used for tracking and limiting the access that you have granted to authorized clients:

- **Usage plans** let you provide API keys to your customers — and then track and limit usage of your API stages and methods for each API key. For more information, see the section called "Use Usage Plans with API Keys" (p. 432).

**Control Access to an API with Amazon API Gateway Resource Policies**

Amazon API Gateway resource policies are JSON policy documents that you attach to an API to control whether a specified principal (typically an IAM user or role) can invoke the API. You can use API Gateway resource policies to allow your API to be securely invoked by:

- users from a specified AWS account
- specified source IP address ranges or CIDR blocks
- specified virtual private clouds (VPCs) or VPC endpoints (in any account)
You can use resource policies for all API endpoint types in API Gateway: private, edge-optimized, and regional.

For **private APIs**, you can use resource policies together with VPC endpoint policies to control which principals have access to which resources and actions. For more information, see the section called "Use VPC Endpoint Policies for Private APIs" (p. 378).

You can attach a resource policy to an API using the AWS console, AWS CLI, or AWS SDKs.

API Gateway resource policies are different from IAM policies. IAM policies are attached to IAM entities (users, groups, or roles) and define what actions those entities are capable of doing on which resources. API Gateway resource policies are attached to resources. For a more detailed discussion of the differences between identity-based (IAM) policies and resource policies, see **Identity-Based Policies and Resource-Based Policies**.

You can use API Gateway resource policies together with IAM policies.

**Topics**

- Access Policy Language Overview for Amazon API Gateway (p. 348)
- How Amazon API Gateway Resource Policies Affect Authorization Workflow (p. 349)
- API Gateway Resource Policy Examples (p. 358)
- Create and Attach an API Gateway Resource Policy to an API (p. 360)
- AWS Condition Keys that can be used in API Gateway Resource Policies (p. 361)

**Access Policy Language Overview for Amazon API Gateway**

This page describes the basic elements used in Amazon API Gateway resource policies.


For information about how an AWS service decides whether a given request should be allowed or denied, see Determining Whether a Request is Allowed or Denied.

**Common Elements in an Access Policy**

In its most basic sense, a resource policy contains the following elements:

- **Resources** – APIs are the Amazon API Gateway resources for which you can allow or deny permissions. In a policy, you use the Amazon Resource Name (ARN) to identify the resource.

  For the format of the Resource element, see [Resource Format of Permissions for Executing API in API Gateway](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-permissions.html).

- **Actions** – For each resource, Amazon API Gateway supports a set of operations. You identify resource operations you will allow (or deny) by using action keywords.

  For example, the `apigateway:invoke` permission will allow the user permission to invoke an API upon a client request.

  For the format of the Action element, see [Action Format of Permissions for Executing API in API Gateway](https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-permissions.html).

- **Effect** – What the effect will be when the user requests the specific action—this can be either Allow or Deny. You can also explicitly deny access to a resource, which you might do in order to make sure that a user cannot access it, even if a different policy grants access.
**Note**

"Implicit deny" is the same thing as "Deny by default."
"Implicit deny" is different from "Explicit deny." For more information, see The Difference Between Denying by Default and Explicit Deny.

- Principal – The account or user who is allowed access to the actions and resources in the statement. In a resource policy, the principal is the IAM user or account who is the recipient of this permission.

The following example resource policy shows the preceding common policy elements. The policy grants access to the API under the specified `account-id` in the specified `region` to any user whose source IP address is in the address block `123.4.5.6/24`. The policy denies all access to the API if the user's source IP is not within the range.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "execute-api:Invoke",
         "Resource": "arn:aws:execute-api:region:account-id:*"
      },
      {
         "Effect": "Deny",
         "Principal": "*",
         "Action": "execute-api:Invoke",
         "Resource": "arn:aws:execute-api:region:account-id:*",
         "Condition": {
            "NotIpAddress": {
               "aws:SourceIp": "123.4.5.6/24"
            }
         }
      }
   ]
}
```

**How Amazon API Gateway Resource Policies Affect Authorization Workflow**

When API Gateway evaluates the resource policy attached to your API, the result is affected by the authentication type that you have defined for the API, as illustrated in the flowcharts in the following sections.

**Topics**

- API Gateway Resource Policy Only (p. 349)
- Lambda Authorizer and Resource Policy (p. 351)
- IAM Authentication and Resource Policy (p. 353)
- Amazon Cognito Authentication and Resource Policy (p. 355)
- Policy Evaluation Outcome Tables (p. 357)

**API Gateway Resource Policy Only**

In this workflow, an API Gateway resource policy is attached to the API, but no authentication type is defined for the API. Evaluation of the policy will involve seeking an explicit allow based on the inbound criteria of the caller. An implicit denial or any explicit denial will result in denying the caller.

Following is an example of such a resource policy.
```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": ["192.0.2.0/24", "198.51.100.0/24"]
                }
            }
        }
    ]
}
```
Lambda Authorizer and Resource Policy

In this workflow, a Lambda authorizer is configured for the API in addition to a resource policy. The resource policy will be evaluated in two phases. Prior to calling the Lambda authorizer, API Gateway will first evaluate the policy and check for any explicit denials. If found, the caller is denied access immediately. Otherwise, the Lambda authorizer is called, and it returns a policy document (p. 391), which is evaluated in conjunction with the resource policy. The result is determined based on Table A (p. 357) below.

The following example resource policy allows calls only from the VPC endpoint whose VPC endpoint ID is `vpce-1a2b3c4d`. During the pre-auth evaluation, only the calls coming from the VPC endpoint indicated below will be allowed to move forward and evaluate the Lambda authorizer. All remaining calls will be blocked.
Auth type = Lambda

Perform Pre-Auth (Evaluate full resource policy)

Is there a Deny?  
Yes  
Final decision is Deny (explicit deny)  
No

Execute Lambda authorizer

Evaluate resource + identity-based policies

Final decision
IAM Authentication and Resource Policy

In this workflow, IAM authentication is configured for the API in addition to a resource policy. After authenticating the user with the IAM service, the policies attached to the IAM user in addition to the resource policy are evaluated together. The outcome will vary based on whether the caller is in the same account, or a separate AWS account, from the API owner. If the caller and API owner are from separate accounts, both the IAM user policies and the resource policy explicitly allow the caller to proceed. (See Table B (p. 357) below.) In contrast, if the caller and the API owner are in the same account, then either the user policies or the resource policy must explicitly allow the caller to proceed. (See Table A (p. 357) below.)
Following is an example of a cross-account resource policy. Assuming the IAM user policy contains an Allow, this resource policy will allow calls only from the VPC whose VPC ID is `vpc-2f09a348`. (See Table B (p. 357) below.)

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "",
            "Action": "execute-api:Invoke",
            "Resource": [
                "arn:aws:execute-api:region:account-id:api-id/"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceVpc": "vpc-2f09a348"
                }  
            }
        }
    ]
}
```

**Amazon Cognito Authentication and Resource Policy**

In this workflow, an Amazon Cognito user pool (p. 397) is configured for the API in addition to a resource policy. API Gateway first attempts to authenticate the caller via Amazon Cognito. This is typically performed via a JWT token provided by the caller. If authentication is successful, the resource policy is evaluated independently, and an explicit allow is required. A deny or neither allow or deny will result in a deny. Following is an example of a resource policy that might be used together with Amazon Cognito User Pools.
Auth type = Cognito

Perform authentication

Is there an explicit Allow?

Yes

Is there a resource policy?

Yes

Evaluate resource policies

Final decision is Deny (deny invoke)

No

Final decision is Allow (allow invoke)

No
Following is an example of a resource policy that allows calls only from specified source IPs, assuming that the Amazon Cognito authentication token contains an Allow. (See Table A (p. 357) below.)

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "execute-api:Invoke",
         "Condition": {
            "IpAddress": {
               "aws:SourceIp": ["192.0.2.0/24", "198.51.100.0/24"]
            }
         }
      }
   ]
}
```

**Policy Evaluation Outcome Tables**

Table A lists the resulting behavior when access to an API Gateway API is controlled by an IAM policy (or a Lambda or Amazon Cognito User Pools authorizer) and an API Gateway resource policy, both of which are in the same AWS account.

**Table A: Account A Calls API Owned by Account A**

<table>
<thead>
<tr>
<th>IAM User Policy (or Lambda or Amazon Cognito User Pools authorizer)</th>
<th>API Gateway Resource Policy</th>
<th>Resulting Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>Allow</td>
<td>Neither Allow nor Deny</td>
<td>Allow</td>
</tr>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Neither Allow nor Deny</td>
<td>Implicit Deny</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Allow</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Neither Allow nor Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
</tbody>
</table>

Table B lists the resulting behavior when access to an API Gateway API is controlled by an IAM policy (or a Lambda or Amazon Cognito User Pools authorizer) and an API Gateway resource policy, which are in different AWS accounts. If either is silent (neither allow nor deny), cross-account access is denied. This is because cross-account access requires that both the resource policy and the IAM policy (or a Lambda or Amazon Cognito User Pools authorizer) explicitly grant access.
Table B: Account B Calls API Owned by Account A

<table>
<thead>
<tr>
<th>IAM User Policy (or Lambda or Amazon Cognito User Pools authorizer)</th>
<th>API Gateway Resource Policy</th>
<th>Resulting Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>Allow</td>
<td>Neither Allow nor Deny</td>
<td>Implicit Deny</td>
</tr>
<tr>
<td>Allow</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Allow</td>
<td>Implicit Deny</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Neither Allow nor Deny</td>
<td>Implicit Deny</td>
</tr>
<tr>
<td>Neither Allow nor Deny</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Allow</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Neither Allow nor Deny</td>
<td>Explicit Deny</td>
</tr>
<tr>
<td>Deny</td>
<td>Deny</td>
<td>Explicit Deny</td>
</tr>
</tbody>
</table>

API Gateway Resource Policy Examples

This page presents a few examples of typical use cases for API Gateway resource policies. The policies use `account-id` and `api-id` strings in the resource value. To test these policies, you need to replace these strings with your own account ID and API ID. For information about access policy language, see Access Policy Language Overview for Amazon API Gateway (p. 348).

Topics

- Example: Allow users in another AWS account to use an API (p. 358)
- Example: Deny API traffic based on source IP address or range (p. 359)
- Example: Allow private API traffic based on source VPC or VPC endpoint (p. 359)

Example: Allow users in another AWS account to use an API

The following example resource policy grants API access in one AWS account to two users in a different AWS account via Signature Version 4 (SigV4) protocols. Specifically, Alice and the root user for the AWS account identified by `account-id-2` are granted the `execute-api:Invoke` action to execute the `GET` action on the `pets` resource (API) in the AWS account identified by `account-id-1`.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::account-id:user/Alice",
                    "arn:aws:iam::account-id-2"
                ]
            },
            "Action": "execute-api:Invoke",
            "Resource": [
                "arn:aws:execute-api:region:account-id-1:api-id/stage/GET/pets"
            ]
        }
    ]
}
```
Example: Deny API traffic based on source IP address or range

The following example resource policy is a "blacklist" policy that denies (blocks) incoming traffic to an API from two specified source IP address blocks.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "execute-api:Invoke",
      },
      {
         "Effect": "Deny",
         "Principal": "*",
         "Action": "execute-api:Invoke",
         "Resource": [ "arn:aws:execute-api:region:account-id:api-id/*" ],
         "Condition": {
            "IpAddress": { "aws:SourceIp": [ "192.0.2.0/24", "198.51.100.0/24" ]
         }
      }
   ]
}
```

Example: Allow private API traffic based on source VPC or VPC endpoint

The following example resource policies allow incoming traffic to a private API only from a specified virtual private cloud (VPC) or VPC endpoint.

This example resource policy specifies a source VPC:

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "execute-api:Invoke",
      },
      {
         "Effect": "Deny",
         "Principal": "*",
         "Action": "execute-api:Invoke",
         "Resource": [ "arn:aws:execute-api:region:account-id:api-id/*" ],
         "Condition": {
```

359
This example resource policy specifies a source VPC endpoint:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Resource": [
                "arn:aws:execute-api:region:account-id:api-id/**
            ]
        },
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "execute-api:Invoke",
            "Resource": [
                "arn:aws:execute-api:region:account-id:api-id/**
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:SourceVpc": "vpc-1a2b3c4d"
                }
            }
        }
    ]
}
```

Create and Attach an API Gateway Resource Policy to an API

To allow a user to access your API by calling the API execution service, you must create an API Gateway resource policy, which controls access to the API Gateway resources, and attach the policy to the API.

**Important**

To update an API Gateway resource policy, you'll need to have `apigateway:UpdateRestApiPolicy` permission in addition to `apigateway:PATCH` permission.

The resource policy can be attached to the API when the API is being created, or it can be attached afterwards. For private APIs, note that until you attach the resource policy to the private API, all calls to the API will fail.

**Important**

If you update the resource policy after the API is created, you'll need to deploy the API to propagate the changes after you've attached the updated policy. Updating or saving the policy alone won't change the runtime behavior of the API. For more information about deploying your API, see Deploying a REST API in Amazon API Gateway (p. 494).

Access can be controlled by IAM condition elements, including conditions on AWS account, source VPC, source VPC endpoint, or IP range. If the `Principal` in the policy is set to "*", other authorization types can be used alongside the resource policy. If the `Principal` is set to "AWS", authorization will fail for all resources not secured with AWS_IAM authorization, including unsecured resources.
The following sections describe how to create your own API Gateway resource policy and attach it to your API. Attaching a policy applies the permissions in the policy to the methods in the API.

**Important**
If you use the API Gateway console to attach a resource policy to a deployed API, or if you update an existing resource policy, you'll need to redeploy the API in the console for the changes to take effect.

**Topics**
- Attaching API Gateway Resource Policies (Console) (p. 361)
- Attaching API Gateway Resource Policies (AWS CLI) (p. 361)

**Attaching API Gateway Resource Policies (Console)**

You can use the AWS Management console to attach a resource policy to an API Gateway API.

**To attach a resource policy to an API Gateway API**

2. Choose the API name.
3. In the left navigation pane, choose Resource Policy.
4. If desired, choose one of the Examples. In the example policies, placeholders are enclosed in double curly braces ("{placeholder}"). Replace each of the placeholders (including the curly braces) with the necessary information.
   
   If you don't use one of the Examples, enter your resource policy.
5. Choose Save.

If the API has been deployed previously in the API Gateway console, you'll need to redeploy it for the resource policy to take effect.

**Attaching API Gateway Resource Policies (AWS CLI)**

To use the AWS CLI to create a new API and attach a resource policy to it, call the `create-rest-api` command as follows:

```bash
aws apigateway create-rest-api \\  --name "api-name" \\  --policy "\"jsonEscapedPolicyDocument\""
```

To use the AWS CLI to attach a resource policy to an existing API, call the `update-rest-api` command as follows:

```bash
aws apigateway update-rest-api \\  --rest-api-id api-id \\  --patch-operations op=replace, path=/policy, value='\"jsonEscapedPolicyDocument\"'
```

**AWS Condition Keys that can be used in API Gateway Resource Policies**

The following table contains the complete list of AWS condition keys that can be used in resource policies for APIs in API Gateway for each authorization type.
For more information about AWS condition keys, see AWS Global Condition Context Keys.

**Table of Condition Keys**

<table>
<thead>
<tr>
<th>Condition Keys</th>
<th>Criteria</th>
<th>Needs Auth?</th>
<th>Authorization Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>aws:CurrentTime</td>
<td>None</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:EpochTime</td>
<td>None</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:TokenIssueTime</td>
<td>Key is present only in requests that are signed using temporary security credentials.</td>
<td>Yes</td>
<td>IAM</td>
</tr>
<tr>
<td>aws:MultiFactorAuthPresent</td>
<td>Key is present only in requests that are signed using temporary security credentials.</td>
<td>Yes</td>
<td>IAM</td>
</tr>
<tr>
<td>aws:MultiFactorAuthenticationAge</td>
<td>Key is present only if MFA is present in the requests.</td>
<td>Yes</td>
<td>IAM</td>
</tr>
<tr>
<td>aws:PrincipalType</td>
<td>None</td>
<td>Yes</td>
<td>IAM</td>
</tr>
<tr>
<td>aws:Referer</td>
<td>Key is present only if the value is provided by the caller in the HTTP header.</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:SecureTransport</td>
<td>None</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:SourceArn</td>
<td>None</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:SourceIp</td>
<td>None</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:SourceVpc</td>
<td>This key can be used only for private APIs.</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:SourceVpce</td>
<td>This key can be used only for private APIs.</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:UserAgent</td>
<td>Key is present only if the value is provided by the caller in the HTTP header.</td>
<td>No</td>
<td>All</td>
</tr>
<tr>
<td>aws:userid</td>
<td>None</td>
<td>Yes</td>
<td>IAM</td>
</tr>
<tr>
<td>aws:username</td>
<td>None</td>
<td>Yes</td>
<td>IAM</td>
</tr>
</tbody>
</table>

**Control Access to an API with IAM Permissions**

You control access to your Amazon API Gateway API with IAM permissions by controlling access to the following two API Gateway component processes:

- To create, deploy, and manage an API in API Gateway, you must grant the API developer permissions to perform the required actions supported by the API management component of API Gateway.
To call a deployed API or to refresh the API caching, you must grant the API caller permissions to perform required IAM actions supported by the API execution component of API Gateway.

The access control for the two processes involves different permissions models, explained next.

API Gateway Permissions Model for Creating and Managing an API

To allow an API developer to create and manage an API in API Gateway, you must create IAM permissions policies that allow a specified API developer to create, update, deploy, view, or delete required API entities. You attach the permissions policy to an IAM user representing the developer, to an IAM group containing the user, or to an IAM role assumed by the user.

In this IAM policy document, the IAM Resource element contains a list of API Gateway API entities, including API Gateway resources and API Gateway link-relations. The IAM Action element contains the required API Gateway API-managing actions. These actions are declared in the apigateway:HTTP_VERB format, where apigateway designates the underlying API management component of API Gateway, and HTTP_VERB represents HTTP verbs supported by API Gateway.

For more information on how to use this permissions model, see Control Access for Managing an API (p. 364).

API Gateway Permissions Model for Invoking an API

To allow an API caller to invoke the API or refresh its caching, you must create IAM policies that permit a specified API caller to invoke the API method for which the IAM user authentication is enabled. The API developer sets the method's authorizationType property to AWS_IAM to require that the caller submit the IAM user's access keys to be authenticated. Then, you attach the policy to an IAM user representing the API caller, to an IAM group containing the user, or to an IAM role assumed by the user.

In this IAM permissions policy statement, the IAM Resource element contains a list of deployed API methods identified by given HTTP verbs and API Gateway resource paths. The IAM Action element contains the required API Gateway API executing actions. These actions include execute-api:Invoke or execute-api:InvalidateCache, where execute-api designates the underlying API execution component of API Gateway.

For more information on how to use this permissions model, see Control Access for Invoking an API (p. 369).

When an API is integrated with an AWS service (for example, AWS Lambda) in the back end, API Gateway must also have permissions to access integrated AWS resources (for example, invoking a Lambda function) on behalf of the API caller. To grant these permissions, create an IAM role of the AWS service for API Gateway type. When you create this role in the IAM Management console, this resulting role contains the following IAM trust policy that declares API Gateway as a trusted entity permitted to assume the role:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```
If you create the IAM role by calling the `create-role` command of CLI or a corresponding SDK method, you must supply the above trust policy as the input parameter of `assume-role-policy-document`. Do not attempt to create such a policy directly in the IAM Management console or calling AWS CLI `create-policy` command or a corresponding SDK method.

For API Gateway to call the integrated AWS service, you must also attach to this role appropriate IAM permissions policies for calling integrated AWS services. For example, to call a Lambda function, you must include the following IAM permissions policy in the IAM role:

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

Note that Lambda supports resource-based access policy, which combines both trust and permissions policies. When integrating an API with a Lambda function using the API Gateway console, you are not asked to set this IAM role explicitly, because the console sets the resource-based permissions on the Lambda function for you, with your consent.

**Note**
To enact access control to an AWS service, you can use either the caller-based permissions model, where a permissions policy is directly attached to the caller's IAM user or group, or the role-based permission model, where a permissions policy is attached to an IAM role that API Gateway can assume. The permissions policies may differ in the two models. For example, the caller-based policy blocks the access while the role-based policy allows it. You can take advantage of this to require that an IAM user access an AWS service through an API Gateway API only.

### Control Access for Managing an API

In this section, you will learn how to create IAM policy statements to control who can or cannot create, deploy and update an API in API Gateway. You'll also find the policy statements reference, including the formats of the `Action` and `Resource` fields related to the API managing service.

#### Control Who Can Create and Manage an API Gateway API with IAM Policies

To control who can or cannot create, deploy and update your API using the API managing service of API Gateway, create an IAM policy document with required permissions as shown in the following policy template:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Permission",
      "Action": ["apigateway:HTTP_VERB"
    }
  ]
}
```
Use IAM Permissions

Here, **Permission** can be **Allow** or **Deny** to grant or revoke, respectively, the access rights as stipulated by the policy statement. For more information, see AWS IAM permissions.

**HTTP_VERB** can be any of the API Gateway-supported HTTP verbs (p. 366). * can be used to denote any of the HTTP verbs.

**Resource** contains a list of ARNs of the affected API entities, including RestApi, Resource, Method, Integration, DocumentationPart, Model, Authorizer, UsagePlan, etc. For more information, see Resource Format of Permissions for Managing API in API Gateway (p. 366).

By combining different policy statements, you can customize the access permissions for individual users, groups or roles to access selected API entities and to perform specified actions against those entities. For example, you can include the following statement in the IAM policy to grant your documentation team permission to create, publish, update and delete the documentation parts of a specified API as well as to view the API entities.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET"
      ],
      "Resource": [
        "arn:aws:apigateway:region::/restapis/api-id/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:POST",
        "apigateway:PATCH",
        "apigateway:DELETE"
      ],
      "Resource": [
        "arn:aws:apigateway:region::/restapis/api-id/documentation/*"
      ]
    }
  ]
}
```

For your API core development team who is responsible for all operations, you can include the following statement in the IAM policy to grant the team much broader access permissions.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:*"
      ],
      "Resource": [
        "arn:aws:apigateway:region::/restapis/*"
      ]
    }
  ]
}
```
Statement Reference of IAM Policies for Managing API in API Gateway

The following information describes the Action and Resource element format used in an IAM policy statement to grant or revoke permissions for managing API Gateway API entities.

**Action Format of Permissions for Managing API in API Gateway**

The API-managing Action expression has the following general format:

```
apigateway:action
```

where `action` is one of the following API Gateway actions:

- `*`, which represents all of the following actions.
- `GET`, which is used to get information about resources.
- `POST`, which is primarily used to create child resources.
- `PUT`, which is primarily used to update resources (and, although not recommended, can be used to create child resources).
- `DELETE`, which is used to delete resources.
- `PATCH`, which can be used to update resources.

Some examples of the `Action` expression include:

- `apigateway:*` for all API Gateway actions.
- `apigateway:GET` for just the GET action in API Gateway.

**Resource Format of Permissions for Managing API in API Gateway**

The API-managing Resource expression has the following general format:

```
arn:aws:apigateway::resource-path-specifier
```

where `region` is a target AWS region (such as `us-east-1` or `*` for all supported AWS regions), and `resource-path-specifier` is the path to the target resources.

Some example resource expressions include:

- `arn:aws:apigateway:region::/restapis/*` for all resources, methods, models, and stages in the AWS region of `region`.
- `arn:aws:apigateway:region::/restapis/api-id/*` for all resources, methods, models, and stages in the API with the identifier of `api-id` in the AWS region of `region`.
- `arn:aws:apigateway:region::/restapis/api-id/resources/resource-id/*` for all resources and methods in the resource with the identifier `resource-id`, which is in the API with the identifier of `api-id` in the AWS region of `region`.
• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/resources/\[resource-id\]/methods/* for all of the methods in the resource with the identifier `resource-id`, which is in the API with the identifier of `api-id` in the AWS region of `region`.

• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/resources/\[resource-id\]/methods/GET for just the GET method in the resource with the identifier `resource-id`, which is in the API with the identifier of `api-id` in the AWS region of `region`.

• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/models/* for all of the models in the API with the identifier of `api-id` in the AWS region of `region`.

• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/models/\[model-name\] for the model with the name of `model-name`, which is in the API with the identifier of `api-id` in the AWS region of `region`.

• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/stages/* for all of the stages in the API with the identifier of `api-id` in the AWS region of `region`.

• `arn:aws:apigateway:`\[region\]::/restapis/\[api-id\]/stages/\[stage-name\] for just the stage with the name of `stage-name` in the API with the identifier of `api-id` in the AWS region of `region`.

Control Cross-Account Access to Your API

You can manage access to your APIs by creating IAM permission policies to control who can or cannot create, update, deploy, view, or delete API entities. A policy is attached to an IAM user representing your user, to an IAM group containing the user, or to an IAM role assumed by the user.

In the IAM policies you create for your APIs, you can use Condition elements to allow access only to certain Lambda integrations or authorizers.

The Condition block uses boolean condition operators to match the condition in the policy against values in the request. The String\[Xxx\] condition operator will work both for AWS integration (in which the value should be a Lambda function ARN) and Http integration (in which the value should be an Http URI). The following String\[Xxx\] condition operators are supported: StringEquals, StringNotEquals, StringEqualsIgnoreCase, StringNotEqualsIgnoreCase, StringLike, StringNotLike. For more information, see String Condition Operators in the IAM User Guide.

IAM Policy for Cross-Account Lambda Authorizer

Here is an example of an IAM policy to control a cross-account Lambda authorizer function:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["apigateway:POST"],
            "Resource": ["arn:aws:apigateway:[region]::/restapis/\[restapi_id\]/authorizers"],
            //Create Authorizer operation is allowed only with the following Lambda function
            "Condition": {
                "StringEquals": {
                }
            }
        }
    ]
}
```
IAM Policy for Cross-Account Lambda Integration

With cross-account integration, in order to restrict operations on some specific resources (such as `put-integration` for a specific Lambda function), a `Condition` element can be added to the policy to specify which resource (Lambda function) is affected.

Here is an example of an IAM policy to control a cross-account Lambda integration function:

To grant another AWS account permission to call `integration:put` or `put-integration` to set up a Lambda integration in your API, you can include the following statement in the IAM policy.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "apigateway:PUT" ],
      //PutIntegration is only valid with the following Lambda function
      "Condition": {
        "StringEquals": { "apigateway:IntegrationUri": "arn:aws:lambda:region:account-id:function:lambda-function-name" }
      }
    }
  ]
}
```

Allow Another Account to Manage the Lambda Function Used When Importing an OpenAPI File

To grant another AWS account permission to call `restapi:import` or `import-rest-api` to import an OpenAPI file, you can include the following statement in the IAM policy.

In the `Condition` statement below, the string "lambda:path/2015-03-31/functions/arn:aws:lambda:us-east-1:account-id:function:lambda-function-name" is the full ARN for the Lambda function.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "apigateway:POST" ],
      "Resource": "arn:aws:apigateway:*::/restapis",
      "Condition": {
      }
    }
  ]
}
```
Control Access for Invoking an API

In this section you will learn how to write up IAM policy statements to control who can call a deployed API in API Gateway. Here, you will also find the policy statement reference, including the formats of Action and Resource fields related to the API execution service. You should also study the IAM section in the section called “How Resource Policies Affect Authorization Workflow” (p. 349).

For private APIs, you should use a combination of an API Gateway resource policy and a VPC endpoint policy. For more information, see the following topics:

- the section called “Use API Gateway Resource Policies” (p. 347)
- the section called “Use VPC Endpoint Policies for Private APIs” (p. 378)

Control Who Can Call an API Gateway API Method with IAM Policies

To control who can or cannot call a deployed API with IAM permissions, create an IAM policy document with required permissions. A template for such a policy document is shown as follows.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Permission",
      "Action": [
        "execute-api:Execution-operation"
      ],
      "Resource": [
      ]
    }
  ]
}
```

Here, Permission is to be replaced by Allow or Deny depending on whether you want to grant or revoke the included permissions. Execution-operation is to be replaced by the operations supported by the API execution service. METHOD_HTTP_VERB stands for a HTTP verb supported by the specified resources. Resource-path is the placeholder for the URL path of a deployed API Resource instance.
supporting the said `METHOD_HTTP-VERB`. For more information, see Statement Reference of IAM Policies for Executing API in API Gateway (p. 371).

**Note**

For IAM policies to be effective, you must have enabled IAM authentication on API methods by setting `AWS_IAM` for the methods' `authorizationType` property. Failing to do so will make these API methods publicly accessible.

For example, to grant a user permission to view a list of pets exposed by a specified API, but to deny the user permission to add a pet to the list, you could include the following statement in the IAM policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "execute-api:Invoke"
         ],
         "Resource": [
            "arn:aws:execute-api:us-east-1:account-id:api-id/*/GET/pets"
         ]
      },
      {
         "Effect": "Deny",
         "Action": [
            "execute-api:Invoke"
         ],
         "Resource": [
            "arn:aws:execute-api:us-east-1:account-id:api-id/*/POST/pets"
         ]
      }
   ]
}
```

To grant a user permission to view a specific pet exposed by an API that is configured as `GET /pets/{petId}`, you could include the following statement in the IAM policy:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "execute-api:Invoke"
         ],
         "Resource": [
            "arn:aws:execute-api:us-east-1:account-id:api-id/*/GET/pets/a1b2"
         ]
      }
   ]
}
```

For a developer team testing APIs, you can include the following statement in the IAM policy to allow the team to call any method on any resource of any API by any developer in the `test` stage:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [          ]
      }
   ]
}
```
Statement Reference of IAM Policies for Executing API in API Gateway

The following information describes the Action and Resource format of IAM policy statements of access permissions for executing an API.

Action Format of Permissions for Executing API in API Gateway

The API-executing Action expression has the following general format:

```
execute-api:action
```

where `action` is an available API-executing action:

- `*`, which represents all of the following actions.
- `Invoke`, used to invoke an API upon a client request.
- `InvalidateCache`, used to invalidate API cache upon a client request.

Resource Format of Permissions for Executing API in API Gateway

The API-executing Resource expression has the following general format:

```
```

where:

- `region` is the AWS region (such as `us-east-1` or * for all AWS regions) that corresponds to the deployed API for the method.
- `account-id` is the 12-digit AWS account Id of the REST API owner.
- `api-id` is the identifier API Gateway has assigned to the API for the method. (* can be used for all APIs, regardless of the API's identifier.)
- `stage-name` is the name of the stage associated with the method (* can be used for all stages, regardless of the stage's name.)
- `HTTP-VERB` is the HTTP verb for the method. It can be one of the following: GET, POST, PUT, DELETE, PATCH.
- `resource-path-specifier` is the path to the desired method. (* can be used for all paths).

Some example resource expressions include:

- `arn:aws:execute-api:*:*:*:*` for any resource path in any stage, for any API in any AWS region. (This is equivalent to `*`.
- `arn:aws:execute-api:us-east-1:*:*` for any resource path in any stage, for any API in the AWS region of `us-east-1`.
- `arn:aws:execute-api:us-east-1:*:api-id/*` for any resource path in any stage, for the API with the identifier of `api-id` in the AWS region of `us-east-1`.
• `arn:aws:execute-api:us-east-1:*:api-id/*` for resource path in the stage of `test`, for the API with the identifier of `api-id` in the AWS region of `us-east-1`.

• `arn:aws:execute-api:us-east-1:*:api-id/test/*` for any resource path along the path of `mydemoresource`, for any HTTP method in the stage of `test`, for the API with the identifier of `api-id` in the AWS region of `us-east-1`.

• `arn:aws:execute-api:us-east-1:*:api-id/test/*/mydemoresource/*` for any resource path along the path of `mydemoresource`, in the stage of `test`, for the API with the identifier of `api-id` in the AWS region of `us-east-1`.

IAM Policy Examples for Managing API Gateway APIs

The following example policy documents shows various use cases to set access permissions for managing API resources in API Gateway. For permissions model and other background information, see Control Who Can Create and Manage an API Gateway API with IAM Policies (p. 364).

Topics
• Simple Read Permissions (p. 372)
• Read-Only Permissions on any APIs (p. 373)
• Full Access Permissions for any API Gateway Resources (p. 374)
• Full-Access Permissions for Managing API Stages (p. 374)
• Block Specified Users from Deleting any API Resources (p. 375)

Simple Read Permissions

The following policy statement gives the user permission to get information about all of the resources, methods, models, and stages in the API with the identifier of `a123456789` in the AWS region of `us-east-1`:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["apigateway:GET"],
        "Resource": ["arn:aws:apigateway:us-east-1::/restapis/a123456789/**"]
      }
    ]
}
```

The following example policy statement gives the IAM user permission to list information for all resources, methods, models, and stages in any region. The user also has permission to perform all available API Gateway actions for the API with the identifier of `a123456789` in the AWS region of `us-east-1`:

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": ["apigateway:GET"],
        "Resource": ["arn:aws:apigateway:*::/restapis/a123456789/**"]
      }
    ]
}
```
Read-Only Permissions on any APIs

The following policy document will permit attached entities (users, groups or roles) to retrieve any of the APIs of the caller’s AWS account. This includes any of the child resources of an API, such as method, integration, etc.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Stmt1467321237000",
         "Effect": "Deny",
         "Action": [ "apigateway:POST", "apigateway:PUT", "apigateway:PATCH", "apigateway:DELETE" ],
         "Resource": [ "arn:aws:apigateway:us-east-1::/*" ]
      },
      {
         "Sid": "Stmt1467321341000",
         "Effect": "Deny",
         "Action": [ "apigateway:GET" ],
      },
      {
         "Sid": "Stmt1467321344000",
         "Effect": "Allow",
         "Action": [ "apigateway:GET" ],
         "Resource": [ "arn:aws:apigateway:us-east-1:/restapis/*" ]
      }
   ]
}```
The first `Deny` statement explicitly prohibits any calls of POST, PUT, PATCH, DELETE on any resources in API Gateway. This ensures that such permissions will not be overridden by other policy documents also attached to the caller. The second `Deny` statement blocks the caller to query the root (/) resource, account information (/account), client certificates (/clientcertificates), custom domain names (/domainnames) and API keys (/apikyes). Together, the three statements ensure that the caller can only query API-related resources. This can be useful in API testing when you do not want the tester to modify any of the code.

To restrict the above read-only access to specified APIs, replace the `Resource` property of `Allow` statement by the following:

```
```

### Full Access Permissions for any API Gateway Resources

The following example policy document grants the full access to any of the API Gateway resource of the AWS account.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1467321765000",
            "Effect": "Allow",
            "Action": ["apigateway:*"],
            "Resource": ["*"],
        }
    ]
}
```

In general, you should refrain from using such a broad and open access policy. It may be necessary to do so for your API development core team so that they can create, deploy, update, and delete any API Gateway resources.

### Full-Access Permissions for Managing API Stages

The following example policy documents grants full-access permissions on Stage related resources of any API in the caller's AWS account.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["apigateway:*"],
        }
    ]
}
```
The above policy document grants full access permissions only to the stages collection and any of the contained stage resources, provided that no other policies granting more accesses have been attached to the caller. Otherwise, you must explicitly deny all the other accesses.

Using the above policy, caller must find out the REST API's identifier beforehand because the user cannot call GET /restapis to query the available APIs. Also, if arn:aws:apigateway:us-east-1::/restapis/*/stages is not specified in the Resource list, the Stages resource becomes inaccessible. In this case, the caller will not be able to create a stage nor get the existing stages, although he or she can still view, update or delete a stage, provided that he stage's name is known.

To grant permissions for a specific API's stages, simply replace the restapis/*/ portion of the Resource specifications by restapis/restapi_id, where restapi_id is the identifier of the API of interest.

Block Specified Users from Deleting any API Resources

The following example IAM policy document blocks a specified user from deleting any API resources in API Gateway.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1467331998000",
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "apigateway:PATCH",
        "apigateway:POST",
        "apigateway:PUT"
      ],
      "Resource": [
        "arn:aws:apigateway:us-east-1::/restapis/*"
      ]
    },
    {
      "Sid": "Stmt1467332141000",
      "Effect": "Allow",
      "Action": [
        "apigateway:DELETE"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:username": "johndoe"
        }
      },
      "Resource": [
        "arn:aws:apigateway:us-east-1::/restapis/*"
      ]
    }
  ]
}
```

This IAM policy grants full access permission to create, deploy, update and delete API for attached users, groups or roles, except for the specified user (johndoe), who cannot delete any API resources. It assumes that no other policy document granting Allow permissions on the root, API keys, client certificates or custom domain names has been attached to the caller.

To block the specified user from deleting specific API Gateway resources, e.g., a specific API or an API's resources, replace the Resource specification above by this:
IAM Policy Examples for API Execution Permissions

For permissions model and other background information, see Control Access for Invoking an API (p. 369).

The following policy statement gives the user permission to call any POST method along the path of mydemoresource, in the stage of test, for the API with the identifier of a123456789, assuming the corresponding API has been deployed to the AWS region of us-east-1:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["execute-api:Invoke"],
            "Resource": [
                "arn:aws:execute-api:us-east-1:*:a123456789/test/POST/mydemoresource/*"
            ]
        }
    ]
}
```

The following example policy statement gives the user permission to call any method on the resource path of petstorewalkthrough/pets, in any stage, for the API with the identifier of a123456789, in any AWS region where the corresponding API has been deployed:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["execute-api:Invoke"],
            "Resource": [
                "arn:aws:execute-api:*:*:a123456789/*/petstorewalkthrough/pets"
            ]
        }
    ]
}
```

Create and Attach a Policy to an IAM User

To enable a user to call the API managing service or the API execution service, you must create an IAM policy for an IAM user, which controls access to the API Gateway entities, and then attach the policy to the IAM user. The following steps describe how to create your IAM policy.

**To create your own IAM policy**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. Choose Policies, and then choose Create Policy. If a Get Started button appears, choose it, and then choose Create Policy.
3. Next to Create Your Own Policy, choose Select.
4. For Policy Name, type any value that is easy for you to refer to later. Optionally, type descriptive text in Description.
5. For Policy Document, type a policy statement with the following format, and then choose Create Policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "action-statement"
      ],
      "Resource": [
        "resource-statement"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "action-statement"
      ],
      "Resource": [
        "resource-statement"
      ]
    }
  ]
}
```

In this statement, substitute `action-statement` and `resource-statement` as needed, and add other statements to specify the API Gateway entities you want to allow the IAM user to manage, the API methods the IAM user can call, or both. By default, the IAM user does not have permissions unless there is an explicit corresponding Allow statement.

6. To enable the policy for a user, choose Users.
7. Choose the IAM user to whom you want to attach the policy.

You have just created an IAM policy. It won't have any effect until you attach it to an IAM user, to an IAM group containing the user, or to an IAM role assumed by the user.

**To attach an IAM policy to an IAM user**

1. For the chosen user, choose the Permissions tab, and then choose Attach Policy.
2. Under Grant permissions, choose Attach existing policies directly.
3. Choose the policy document just created from the displayed list and then choose Next: Review.
4. Under Permissions summary, choose Add permissions.

Alternatively, you can add the user to an IAM group, if the user is not already a member, and attach the policy document to the group so that the attached policies are applicable to all group members. It is helpful to manage and update policy configurations on a group of IAM users. In the following, we highlight how to attach the policy to an IAM group, assuming that you have already created the group and added the user to the group.

**To attach an IAM policy document to an IAM group**

1. Choose Groups from the main navigation pane.
2. Choose the Permissions tab under the chosen group.
3. Choose Attach policy.
4. Choose the policy document that you previously created, and then choose Attach policy.

For API Gateway to call other AWS services on your behalf, create an IAM role of the Amazon API Gateway type.

To create an Amazon API Gateway type of role
1. Choose Roles from the main navigation pane.
2. Choose Create New Role.
3. Type a name for Role name and then choose Next Step.
4. Under Select Role Type, in AWS Service Roles, choose Select next to Amazon API Gateway.
5. Choose an available managed IAM permissions policy, for example, AmazonAPIGatewayPushToCloudWatchLog if you want API Gateway to log metrics in CloudWatch, under Attach Policy and then choose Next Step.
6. Under Trusted Entities, verify that apigateway.amazonaws.com is listed as an entry, and then choose Create Role.
7. In the newly created role, choose the Permissions tab and then choose Attach Policy.
8. Choose the previously created custom IAM policy document and then choose Attach Policy.

Use VPC Endpoint Policies for Private APIs in API Gateway

You can improve the security of your private APIs by configuring API Gateway to use an interface VPC endpoint. Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access AWS services by using private IP addresses. For more information about creating VPC endpoints, see Creating an Interface Endpoint.

A VPC endpoint policy is an IAM resource policy that you can attach to an interface VPC endpoint to control access to the endpoint. For more information, see Controlling Access to Services with VPC Endpoints. You can use an endpoint policy to restrict the traffic going from your internal network to access your private APIs. You can choose to allow or disallow access to specific private APIs that can be accessed through the VPC endpoint.

VPC endpoint policies can be used together with API Gateway resource policies. The resource policy is used to specify which principals can access the API. The endpoint policy specifies which private APIs can be called via the VPC endpoint. For more information about resource policies, see the section called “Use API Gateway Resource Policies” (p. 347).

VPC Endpoint Policy Examples

You can create policies for Amazon Virtual Private Cloud endpoints for Amazon API Gateway in which you can specify:

- The principal that can perform actions.
- The actions that can be performed.
- The resources that can have actions performed on them.

To attach the policy to the VPC endpoint, you'll need to use the VPC console. For more information, see Controlling Access to Services with VPC Endpoints.
Example 1: VPC Endpoint Policy Granting Access to Two APIs

The following example policy grants access to only two specific APIs via the VPC endpoint that the policy is attached to.

```
{  
  "Statement": [ 
    { 
      "Principal": "*", 
      "Action": [ 
        "execute-api:Invoke" 
      ], 
      "Effect": "Allow", 
      "Resource": [ 
        "arn:aws:execute-api:us-east-1:123412341234:a1b2c3d4e5/*", 
        "arn:aws:execute-api:us-east-1:123412341234:a1b2c3d4e5:a00001111/*" 
      ] 
    } 
  ]
}
```

Example 2: VPC Endpoint Policy Granting Access to GET Methods

The following example policy grants users access to GET methods for a specific API via the VPC endpoint that the policy is attached to.

```
{  
  "Statement": [ 
    { 
      "Principal": "*", 
      "Action": [ 
        "execute-api:Invoke" 
      ], 
      "Effect": "Allow", 
      "Resource": [ 
        "arn:aws:execute-api:us-east-1:123412341234:a1b2c3d4e5/stageName/GET/*" 
      ] 
    } 
  ]
}
```

Example 3: VPC Endpoint Policy Granting a Specific User Access to a Specific API

The following example policy grants a specific user access to a specific API via the VPC endpoint that the policy is attached to.

```
{  
  "Statement": [ 
    { 
      "Principal": { 
        "AWS": [ 
          "arn:aws:iam::123412341234:user/MyUser" 
        ] 
      }, 
      "Action": [ 
        "execute-api:Invoke" 
      ] 
    } 
  ]
}
```
Using Tags to Control Access to a REST API in API Gateway

Permission to access REST APIs can be fine-tuned using tag-based access control in IAM policies.

For more information, see the section called “Tag-Based Access Control” (p. 682).

Use API Gateway Lambda Authorizers

A Lambda authorizer (formerly known as a custom authorizer) is an API Gateway feature that uses a Lambda function to control access to your API.

A Lambda authorizer is useful if you want to implement a custom authorization scheme that uses a bearer token authentication strategy such as OAuth or SAML, or that uses request parameters to determine the caller's identity.

When a client makes a request to one of your API's methods, API Gateway calls your Lambda authorizer, which takes the caller's identity as input and returns an IAM policy as output.

There are two types of Lambda authorizers:

- A token-based Lambda authorizer (also called a TOKEN authorizer) receives the caller's identity in a bearer token, such as a JSON Web Token (JWT) or an OAuth token.
- A request parameter-based Lambda authorizer (also called a REQUEST authorizer) receives the caller's identity in a combination of headers, query string parameters, stageVariables (p. 302), and $context (p. 293) variables.

For WebSocket APIs, only request parameter-based authorizers are supported.

It is possible to use an AWS Lambda function from an AWS account that is different from the one in which you created your Lambda authorizer function. For more information, see the section called “Configure a Cross-Account Lambda Authorizer” (p. 395).

To see an example of a .NET Lambda authorizer, view the Creating an API Gateway Custom Authorizer in .NET Core 2.0 video.

Topics

- Lambda Authorizer Auth Workflow (p. 381)
- Steps to Create an API Gateway Lambda Authorizer (p. 381)
- Create an API Gateway Lambda Authorizer Function in the Lambda Console (p. 382)
- Configure a Lambda Authorizer Using the API Gateway Console (p. 387)
- Configure a Lambda Authorizer Using the AWS CLI or an AWS SDK (p. 389)
- Input to an Amazon API Gateway Lambda Authorizer (p. 389)
- Output from an Amazon API Gateway Lambda Authorizer (p. 391)
- Call an API with API Gateway Lambda Authorizers (p. 392)
Lambda Authorizer Auth Workflow

The following diagram illustrates the authorization workflow for Lambda authorizers.

API Gateway Lambda authorization workflow

1. The client calls a method on an API Gateway API method, passing a bearer token or request parameters.
2. API Gateway checks whether a Lambda authorizer is configured for the method. If it is, API Gateway calls the Lambda function.
3. The Lambda function authenticates the caller by means such as the following:
   - Calling out to an OAuth provider to get an OAuth access token.
   - Calling out to a SAML provider to get a SAML assertion.
   - Generating an IAM policy based on the request parameter values.
   - Retrieving credentials from a database.
4. If the call succeeds, the Lambda function grants access by returning an output object containing at least an IAM policy and a principal identifier.
5. API Gateway evaluates the policy.
   - If access is denied, API Gateway returns a suitable HTTP status code, such as 403 ACCESS_DENIED.
   - If access is allowed, API Gateway executes the method. If caching is enabled in the authorizer settings, API Gateway also caches the policy so that the Lambda authorizer function doesn't need to be invoked again.

Steps to Create an API Gateway Lambda Authorizer

To create a Lambda authorizer, you need to perform the following tasks:
1. Create the Lambda authorizer function in the Lambda console as described in the section called “Create a Lambda Authorizer Function in the Lambda Console” (p. 382). You can use one of the blueprint examples as a starting point and customize the input (p. 389) and output (p. 391) as desired.

2. Configure the Lambda function as an API Gateway authorizer and configure an API method to require it, as described in the section called “Configure a Lambda Authorizer Using the Console” (p. 387). Alternatively, if you need a cross-account Lambda authorizer, see the section called “Configure a Cross-Account Lambda Authorizer” (p. 395).

   **Note**
   It is also possible to configure an authorizer by using the AWS CLI or an AWS SDK. See the section called “Configure a Lambda Authorizer Using the AWS CLI or an AWS SDK” (p. 389).

3. Test your authorizer by using Postman as described in the section called “Call an API with Lambda Authorizers” (p. 392).

### Create an API Gateway Lambda Authorizer Function in the Lambda Console

Before configuring a Lambda authorizer, you must first create the Lambda function that implements the logic to authorize and, if necessary, to authenticate the caller. The Lambda console provides a Python blueprint, which you can use by choosing Use a blueprint and choosing the `api-gateway-authorizer-python` blueprint. Otherwise, you'll want to use one of the blueprints in the awslabs GitHub repository as a starting point.

For the example Lambda authorizer functions in this section, which don't call other services, you can use the built-in `AWSLambdaBasicExecutionRole`. When creating the Lambda function for your own API Gateway Lambda authorizer, you'll need to assign an IAM execution role to the Lambda function if it calls other AWS services. To create the role, follow the instructions in AWS Lambda Execution Role.

**EXAMPLE: Create a Token-Based Lambda Authorizer Function**

To create a token-based Lambda authorizer function, enter the following Node.js 8.10 code in the Lambda console and test it in the API Gateway console as follows.

1. In the Lambda console, choose Create function.
2. Choose Author from scratch.
3. Enter a name for the function.
4. For Runtime, choose Node.js 8.10.
5. Choose Create function.
6. Copy/paste the following code into the code editor.

```javascript
// A simple token-based authorizer example to demonstrate how to use an authorization token
// to allow or deny a request. In this example, the caller named 'user' is allowed to
// invoke
// a request if the client-supplied token value is 'allow'. The caller is not allowed
to invoke
// the request if the token value is 'deny'. If the token value is 'unauthorized' or an
empty
// string, the authorizer function returns an HTTP 401 status code. For any other token
value,
// the authorizer returns an HTTP 500 status code.
// Note that token values are case-sensitive.
```

382
exports.handler = function(event, context, callback) {
  var token = event.authorizationToken;
  switch (token) {
    case 'allow':
      callback(null, generatePolicy('user', 'Allow', event.methodArn));
      break;
    case 'deny':
      callback(null, generatePolicy('user', 'Deny', event.methodArn));
      break;
    case 'unauthorized':
      callback("Unauthorized"); // Return a 401 Unauthorized response
      break;
    default:
      callback("Error: Invalid token"); // Return a 500 Invalid token response
  }
}

// Help function to generate an IAM policy
var generatePolicy = function(principalId, effect, resource) {
  var authResponse = {};
  authResponse.principalId = principalId;
  if (effect && resource) {
    var policyDocument = {};
    policyDocument.Version = '2012-10-17';
    policyDocument.Statement = [];
    var statementOne = {};
    statementOne.Action = 'execute-api:Invoke';
    statementOne.Effect = effect;
    statementOne.Resource = resource;
    policyDocument.Statement[0] = statementOne;
    authResponse.policyDocument = policyDocument;
  }

  // Optional output with custom properties of the String, Number or Boolean type.
  authResponse.context = {
    "stringKey": "stringval",
    "numberKey": 123,
    "booleanKey": true
  }
  return authResponse;
}

7. Choose Save.
8. In the API Gateway console, create a simple API (p. 42) if you don't already have one.
9. Choose your API from the API list.
10. Choose Authorizers.
12. Enter a name for the authorizer.
13. For Type, choose Lambda.
14. For Lambda Function, choose the region where you created your Lambda authorizer function and choose the function name from the dropdown list.
15. Leave Lambda Invoke Role blank.
16. For Lambda Event Payload, choose Token.
17. For Token Source, enter tokenHeader.
18. Choose Create Authorizer.
19. Choose Test.
20. For the tokenHeader value, enter allow.

In this example, when the API receives a method request, API Gateway passes the source token to this Lambda authorizer function in the event.authorizationToken attribute. The Lambda authorizer function reads the token and acts as follows:

- If the token value is 'allow', the authorizer function returns a 200 OK HTTP response and an IAM policy that looks like the following, and the method request succeeds:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "execute-api:Invoke",
      "Effect": "Allow",
      "Resource": "arn:aws:execute-api:us-east-1:123456789012:ivdtdhp7b5/ESTestInvoke-stage/GET/
    }
  ]
}
```

- If the token value is 'deny', the authorizer function returns a 403 Forbidden HTTP response and a Deny IAM policy that looks like the following, and the method request fails:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "execute-api:Invoke",
      "Effect": "Deny",
      "Resource": "arn:aws:execute-api:us-east-1:123456789012:ivdtdhp7b5/ESTestInvoke-stage/GET/
    }
  ]
}
```

- If the token value is 'unauthorized' or an empty string, the authorizer function returns a 401 Unauthorized HTTP response, and the method call fails.

- If the token is anything else, the client receives a 500 Invalid token response, and the method call fails.

Note

In production code, you may need to authenticate the user before granting authorization. If so, you can add authentication logic in the Lambda function as well by calling an authentication provider as directed in the documentation for that provider.

In addition to returning an IAM policy, the Lambda authorizer function must also return the caller's principal identifier. It can also optionally return a context object containing additional information that can be passed into the integration backend. For more information, see Output from an Amazon API Gateway Lambda Authorizer (p. 391).

EXAMPLE: Create a Request-Based Lambda Authorizer Function

To create a request-based Lambda authorizer function, enter the following Node.js 8.10 code in the Lambda console and test it in the API Gateway console as follows.

1. In the Lambda console, choose Create function.
2. Choose Author from scratch.
3. Enter a name for the function.
4. For **Runtime**, choose **Node.js 8.10**.
5. Choose **Create function**.
6. Copy/paste the following code into the code editor.

```javascript
exports.handler = function(event, context, callback) {

    console.log('Received event:', JSON.stringify(event, null, 2));

    // A simple request-based authorizer example to demonstrate how to use request
    // parameters to allow or deny a request. In this example, a request is
    // authorized if the client-supplied HeaderAuth1 header, QueryString1
    // query parameter, and stage variable of StageVar1 all match
    // specified values of 'headerValue1', 'queryValue1', and 'stageValue1',
    // respectively.

    // Retrieve request parameters from the Lambda function input:
    var headers = event.headers;
    var queryStringParameters = event.queryStringParameters;
    var pathParameters = event.pathParameters;
    var stageVariables = event.stageVariables;

    // Parse the input for the parameter values
    var tmp = event.methodArn.split(':');
    var apiGatewayArnTmp = tmp[5].split('/');
    var awsAccountId = tmp[4];
    var region = tmp[3];
    var restApiId = apiGatewayArnTmp[0];
    var stage = apiGatewayArnTmp[1];
    var method = apiGatewayArnTmp[2];
    var resource = '/'; // root resource
    if (apiGatewayArnTmp[3]) {
        resource += apiGatewayArnTmp[3];
    }

    // Perform authorization to return the Allow policy for correct parameters and
    // the 'Unauthorized' error, otherwise.
    var authResponse = {};
    var condition = {};
    condition.IpAddress = {};

    if (headers.HeaderAuth1 === "headerValue1"
        && queryStringParameters.QueryString1 === "queryValue1"
        && stageVariables.StageVar1 === "stageValue1") {
        callback(null, generateAllow('me', event.methodArn));
    } else {
        callback("Unauthorized");
    }

    // Help function to generate an IAM policy
    var generatePolicy = function(principalId, effect, resource) {
        // Required output:
        var authResponse = {};
        authResponse.principalId = principalId;
        if (effect && resource) {
            var policyDocument = {};
            policyDocument.Version = '2012-10-17'; // default version
            policyDocument.Statement = [];
            var statementOne = {};
            statementOne.Action = 'execute-api:Invoke'; // default action
            statementOne.Effect = effect;
            statementOne.Resource = resource;
            policyDocument.Statement[0] = statementOne;
            authResponse.policyDocument = policyDocument;
        }
    }

    // Help function to generate an IAM policy
    var generateAllow = function(principalId, resource) {
        return generatePolicy(principalId, 'Allow', resource);
    }

    generateAllow('me', event.methodArn);
}
```
Use Lambda Authorizers

```javascript
// Optional output with custom properties of the String, Number or Boolean type.
authResponse.context = {
  "stringKey": "stringval",
  "numberKey": 123,
  "booleanKey": true
};
return authResponse;
```

```javascript
var generateAllow = function(principalId, resource) {
  return generatePolicy(principalId, 'Allow', resource);
}

var generateDeny = function(principalId, resource) {
  return generatePolicy(principalId, 'Deny', resource);
}
```

7. Choose Save.
8. In the API Gateway console, create a simple API (p. 42) if you don't already have one.
9. Choose your API from the API list.
10. Choose Authorizers.
12. Enter a name for the authorizer.
13. For Type, choose Lambda.
14. For Lambda Function, choose the region where you created your Lambda authorizer function and choose the function name from the dropdown list.
15. Leave Lambda Invoke Role blank.
16. For Lambda Event Payload, choose Request.
17. Under Identity Sources, add a Header named HeaderAuth1, a Query String named QueryString1, and a Stage Variable named StageVar1.
18. Choose Test.
19. For HeaderAuth1, enter headerValue1. For QueryString1, enter queryValue1. For StageVar1, enter stageValue1.
20. Choose Test.

In this example, the Lambda authorizer function checks the input parameters and acts as follows:

- If all the required parameter values match the expected values, the authorizer function returns a 200 OK HTTP response and an IAM policy that looks like the following, and the method request succeeds:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "execute-api:Invoke",
      "Effect": "Allow",
      "Resource": "arn:aws:execute-api:us-east-1:123456789012:ivtdhp7b5/ESTestInvoke-stage/GET/"
    }
  ]
}
```

- Otherwise, the the authorizer function returns a 401 Unauthorized HTTP response, and the method call fails.
Note
In production code, you may need to authenticate the user before granting authorization. If so, you can add authentication logic in the Lambda function as well by calling an authentication provider as directed in the documentation for that provider.

In addition to returning an IAM policy, the Lambda authorizer function must also return the caller's principal identifier. It can also optionally return a context object containing additional information that can be passed into the integration backend. For more information, see Output from an Amazon API Gateway Lambda Authorizer (p. 391).

Configure a Lambda Authorizer Using the API Gateway Console

After you create the Lambda function and verify that it works, use the following steps to configure the API Gateway Lambda authorizer (formerly known as the custom authorizer) in the API Gateway console.

To configure a Lambda authorizer using the API Gateway console

1. Sign in to the API Gateway console.
2. Create a new or select an existing API and choose Authorizers under that API.
4. For Create Authorizer, type an authorizer name in the Name input field.
5. For Type, choose the Lambda option.
6. For Lambda Function, choose a region and then choose an available Lambda authorizer function that's in your account.
7. Leave Lambda Invoke Role blank to let the API Gateway console set a resource-based policy. The policy grants API Gateway permissions to invoke the authorizer Lambda function. You can also choose to type the name of an IAM role to allow API Gateway to invoke the authorizer Lambda function. For an example of such a role, see Create an Assumable IAM Role (p. 93).

If you choose to let the API Gateway console set the resource-based policy, the Add Permission to Lambda Function dialog is displayed. Choose OK. After the Lambda authorization is created, you can test it with appropriate authorization token values to verify that it works as expected.

8. For Lambda Event Payload, choose either Token for a TOKEN authorizer or Request for a REQUEST authorizer. (This is the same as setting the type property to TOKEN or REQUEST.)
9. Depending on the choice of the previous step, do one of the following:
   a. For the Token options, do the following:
      • Type the name of a header in Token Source. The API client must include a header of this name to send the authorization token to the Lambda authorizer.
      • Optionally, provide a RegEx statement in Token Validation input field. API Gateway performs initial validation of the input token against this expression and invokes the authorizer upon successful validation. This helps reduce chances of being charged for invalid tokens.
      • For Authorization Caching, select or clear the Enabled option, depending on whether you want to cache the authorization policy generated by the authorizer or not. When policy caching is enabled, you can choose to modify the TTL value. Setting TTL to zero disables policy caching. When policy caching is enabled, the header name specified in Token Source becomes the cache key.

         Note
         The default TTL value is 300 seconds. The maximum value is 3600 seconds; this limit cannot be increased.
   b. For the Request option, do the following:
• **For Identity Sources**, type a request parameter name of a chosen parameter type. Supported parameter types are Header, Query String, Stage Variable, and Context. To add more identity sources, choose **Add Identity Source**.

API Gateway uses the specified identity sources as the request authorizer caching key. When caching is enabled, API Gateway calls the authorizer's Lambda function only after successfully verifying that all the specified identity sources are present at runtime. If a specified identity source is missing, null, or empty, API Gateway returns a 401 Unauthorized response without calling the authorizer Lambda function.

When multiple identity sources are defined, they all used to derive the authorizer's cache key. Changing any of the cache key parts causes the authorizer to discard the cached policy document and generate a new one.

• **For Authorization Caching**, select or deselect the **Enabled** option, depending on whether you want to cache the authorization policy generated by the authorizer or not. When policy caching is enabled, you can choose to modify the **TTL** value from the default (300). Setting TTL=0 disables policy caching.

When caching is disabled, it is not necessary to specify an identity source. API Gateway does not perform any validation before invoking the authorizer's Lambda function.

**Note**
To enable caching, your authorizer must return a policy that is applicable to all methods across an API. To enforce method-specific policy, you can set the TTL value to zero to disable policy caching for the API.

10. Choose **Create** to create the new Lambda authorizer for the chosen API.

11. After the authorizer is created for the API, you can optionally test invoking the authorizer before it is configured on a method.

For the **TOKEN** authorizer, type a valid token in the **Identity token** input text field and the choose **Test**. The token will be passed to the Lambda function as the header you specified in the **Identity token source** setting of the authorizer.

For the **REQUEST** authorizer, type the valid request parameters corresponding to the specified identity sources and then choose **Test**.

In addition to using the API Gateway console, you can use AWS CLI or an AWS SDK for API Gateway to test invoking an authorizer. To do so using the AWS CLI, see **test-invoke-authorizer**.

**Note**
Test-invoking for method executions test-invokes for authorizers are independent processes. To test invoking a method using the API Gateway console, see **Use the Console to Test a REST API Method (p. 537)**. To test invoking a method using the AWS CLI, see **test-invoke-method**.

To test invoking a method and a configured authorizer, deploy the API, and then use cURL or Postman to call the method, providing the required token or request parameters.

The next procedure shows how to configure an API method to use the Lambda authorizer.

**To configure an API method to use a Lambda authorizer**

1. Go back to the API. Create a new method or choose an existing method. If necessary, create a new resource.

2. In **Method Execution**, choose the **Method Request** link.
3. Under **Settings**, expand the **Authorization** drop-down list to select the Lambda authorizer you just created (for example, **myTestApiAuthorizer**), and then choose the check mark icon to save the choice.

4. Optionally, while still on the **Method Request** page, choose **Add header** if you also want to pass the authorization token to the backend. In **Name**, type a header name that matches the **Token Source** name you specified when you created the Lambda authorizer for the API. Then, choose the check mark icon to save the settings. This step does not apply to **REQUEST** authorizers.

5. Choose **Deploy API** to deploy the API to a stage. Note the **Invoke URL** value. You need it when calling the API. For a **REQUEST** authorizer using stage variables, you must also define the required stage variables and specify their values while in **Stage Editor**.

### Configure a Lambda Authorizer Using the AWS CLI or an AWS SDK

You can also configure an API Gateway Lambda authorizer by using the AWS CLI or an AWS SDK.

First, you first need to grant IAM principals in the account that owns your API permission to call **authorizer:create** or **create-authorizer** to create the Lambda function used in your Lambda authorizer. To grant this permission, you need to create the following IAM policy:

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:POST"
      ],
      "Resource": [
        "arn:aws:apigateway:region::/restapis/restapi_id/authorizers"
      ],
      "Condition": {
        "StringEquals": {
          "apigateway:AuthorizerUri": "arn:aws:lambda:region:account-id:function:lambda-function-name"
        }
      }
    }
  ]
}
```

### Input to an Amazon API Gateway Lambda Authorizer

For a Lambda authorizer (formerly known as a custom authorizer) of the **TOKEN** type, you must specify a custom header as the **Token Source** when you configure the authorizer for your API. The API client must pass the required authorization token in that header in the incoming request. Upon receiving the incoming method request, API Gateway extracts the token from the custom header. It then passes the token as the **authorizationToken** property of the **event** object of the Lambda function, in addition to the method ARN as the **methodArn** property:

```json
{
  "type": "TOKEN",
  "authorizationToken": "{caller-supplied-token}"
}
```
In this example, the `type` property specifies the authorizer type, which is a `TOKEN` authorizer. The `{caller-supplied-token}` originates from the authorization header in a client request. The `methodArn` is the ARN of the incoming method request and is populated by API Gateway in accordance with the Lambda authorizer configuration.

For the example `TOKEN` authorizer Lambda function shown in the preceding section, the `{caller-supplied-token}` string is `allow`, `deny`, `unauthorized`, or any other string value. An empty string value is the same as `unauthorized`. The following shows an example of such an input to obtain an `Allow` policy on the `GET` method of an API (`ymy8tbxw7b`) of the AWS account (`123456789012`) in any stage (*):

```json
{
  "type": "TOKEN",
  "authorizationToken": "allow",
  "methodArn": "arn:aws:execute-api:us-west-2:123456789012:ymy8tbxw7b/*/GET/"
}
```

For a Lambda authorizer of the `REQUEST` type, API Gateway passes the required request parameters to the authorizer Lambda function as part of the `event` object. The affected request parameters include headers, path parameters, query string parameters, stage variables, and some of request context variables. The API caller can set the path parameters, headers, and query string parameters. The API developer must set the stage variables during the API deployment and API Gateway provides the request context at run time.

**Note**
Path parameters can be passed as request parameters to the Lambda authorizer function, but they cannot be used as identity sources.

The following example shows an input to a `REQUEST` authorizer for an API method (`GET /request`) with a proxy integration:

```json
{
  "type": "REQUEST",
  "methodArn": "arn:aws:execute-api:us-east-1:123456789012:s4x3opwd6i/test/GET/request",
  "resource": "/request",
  "path": "/request",
  "httpMethod": "GET",
  "headers": {
    "X-AMZ-Date": "20170718T062915Z",
    "Accept": "*/*",
    "HeaderValue1": "headerValue1",
    "CloudFront-View-Country": "US",
    "CloudFront-Forwarded-Proto": "https",
    "CloudFront-Is-Table-Viewer": "false",
    "CloudFront-Is-Mobile-Viewer": "false",
    "User-Agent": "...",
    "CloudFront-Is-Desktop-Viewer": "true",
    "Content-Type": "application/x-www-form-urlencoded"
  }
}
```
"queryStringParameters": { 
    "QueryString1": "queryValue1"
},
"pathParameters": {},
"stageVariables": { 
    "StageVar1": "stageValue1"
},
"requestContext": { 
    "path": "/request",
    "accountId": "123456789012",
    "resourceId": "05c7jb",
    "stage": "test",
    "requestId": "...",
    "identity": { 
        "apiKey": "...",
        "sourceIp": "..."
    },
    "resourcePath": "/request",
    "httpMethod": "GET",
    "apiId": "s4x3opwd6i"
}
}

The requestContext is a map of key-value pairs and corresponds to the $context (p. 293) variable. Its outcome is API-dependent. API Gateway may add new keys to the map. For more information about Lambda function input in Lambda proxy integration, see Input Format of a Lambda Function for Proxy Integration (p. 227).

**Output from an Amazon API Gateway Lambda Authorizer**

A Lambda authorizer function's output is a dictionary-like object, which must include the principal identifier (principalId) and a policy document (policyDocument) containing a list of policy statements. The output can also include a context map containing key-value pairs. If the API uses a usage plan (the apiKeySource is set to AUTHORIZER), the Lambda authorizer function must return one of the usage plan's API keys as the usageIdentifierKey property value.

The following shows an example of this output.

```
{
    "principalId": "yyyyyyyy", // The principal user identification associated with the token sent by the client.
    "policyDocument": { 
        "Version": "2012-10-17",
        "Statement": [ 
            { 
                "Action": "execute-api:Invoke",
                "Effect": "Allow|Deny",
                "Resource": "arn:aws:execute-api:{regionId}:{accountId}:{apiId}/{stage}/{{httpVerb}}/{resource}[/{child-resources}]"
            }
        ],
        "context": { 
            "stringKey": "value",
            "numberKey": "1",
            "booleanKey": "true"
        },
        "usageIdentifierKey": "{api-key}"
    }
}
```

Here, a policy statement specifies whether to allow or deny (Effect) the API Gateway execution service to invoke (Action) the specified API method (Resource). You can use a wild card (*) to specify a
resource type (method). For information about setting valid policies for calling an API, see Statement Reference of IAM Policies for Executing API in API Gateway (p. 371).

For an authorization-enabled method ARN, e.g., `arn:aws:execute-api:{regionId}:{accountId}:{apiId}/{stage}/{httpVerb}/*{resource}/{child-resources}`], the maximum length is 1600 bytes. The path parameter values, the size of which are determined at run time, can cause the ARN length to exceed the limit. When this happens, the API client will receive a 414 Request URI too long response.

In addition, the Resource ARN, as shown in the policy statement output by the authorizer, is currently limited to 512 characters long. For this reason, you must not use URI with a JWT token of a significant length in a request URI. You can safely pass the JWT token in a request header, instead.

You can access the `principalId` value in a mapping template using the `$context.authorizer.principalId` variable. This is useful if you want to pass the value to the backend. For more information, see `$context Variables for Data Models, Authorizers, Mapping Templates, and CloudWatch Access Logging (p. 293).

You can access the `stringKey`, `numberKey`, or `booleanKey` value (for example, "value", "1", or "true") of the context map in a mapping template by calling `$context.authorizer.stringKey`, `$context.authorizer.numberKey`, or `$context.authorizer.booleanKey`, respectively. The returned values are all stringified. Notice that you cannot set a JSON object or array as a valid value of any key in the context map.

You can use the context map to return cached credentials from the authorizer to the backend, using an integration request mapping template. This enables the backend to provide an improved user experience by using the cached credentials to reduce the need to access the secret keys and open the authorization tokens for every request.

For the Lambda proxy integration, API Gateway passes the context object from a Lambda authorizer directly to the backend Lambda function as part of the input event. You can retrieve the context key-value pairs in the Lambda function by calling `$event.requestContext.authorizer.key`.

{api-key} stands for an API key in the API stage's usage plan. For more information, see the section called “Use Usage Plans with API Keys” (p. 432).

The following shows example output from the example Lambda authorizer. The example output contains a policy statement to block (Deny) calls to the GET method in an API (ymy8tbxw7b) of an AWS account (123456789012) in any stage (*).

```json
{
  "principalId": "user",
  "policyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": "execute-api:Invoke",
        "Effect": "Deny",
      }
    ]
  }
}
```

### Call an API with API Gateway Lambda Authorizers

Having configured the Lambda authorizer (formerly known as the custom authorizer) and deployed the API, you should test the API with the Lambda authorizer enabled. For this, you need a REST client, such as cURL or Postman. For the following examples, we use Postman.
**Note**

When calling an authorizer-enabled method, API Gateway does not log the call to CloudWatch if the required token for the `TOKEN` authorizer is not set, is null, or is invalidated by the specified `Token validation expression`. Similarly, API Gateway does not log the call to CloudWatch if any of the required identity sources for the `REQUEST` authorizer are not set, are null, or are empty.

In the following, we show how to use Postman to call or test the API with the previously described Lambda `TOKEN` authorizer enabled. The method can be applied to calling an API with a Lambda `REQUEST` authorizer, if you specify the required path, header, or query string parameters explicitly.

**To call an API with the custom `TOKEN` authorizer**

1. Open **Postman**, choose the `GET` method, and paste the API's **Invoke URL** into the adjacent URL field.

   Add the Lambda authorization token header and set the value to `allow`. Choose **Send**.

   ![Postman screenshot](image)

   The response shows that the API Gateway Lambda authorizer returns a **200 OK** response and successfully authorizes the call to access the HTTP endpoint (http://httpbin.org/get) integrated with the method.

2. Still in Postman, change the Lambda authorization token header value to `deny`. Choose **Send**.
The response shows that the API Gateway Lambda authorizer returns a **403 Forbidden** response without authorizing the call to access the HTTP endpoint.

3. In Postman, change the Lambda authorization token header value to *unauthorized* and choose **Send**.

The response shows that API Gateway returns a **401 Unauthorized** response without authorizing the call to access the HTTP endpoint.

4. Now, change the Lambda authorization token header value to *fail*. Choose **Send**.
The response shows that API Gateway returns a **500 Internal Server Error** response without authorizing the call to access the HTTP endpoint.

**Configure a Cross-Account Lambda Authorizer**

You can now also use an AWS Lambda function from a different AWS account as your API authorizer function. Each account can be in any region where Amazon API Gateway is available. The Lambda authorizer function can use bearer token authentication strategies such as OAuth or SAML. This makes it easy to centrally manage and share a central Lambda authorizer function across multiple API Gateway APIs.

In this section, we show how to configure a cross-account Lambda authorizer function using the Amazon API Gateway console.

These instructions assume that you already have an API Gateway API in one AWS account and a Lambda authorizer function in another account.

**Configure a Cross-Account Lambda Authorizer Using the API Gateway Console**

Log in to the Amazon API Gateway console in your first account (the one that has your API in it) and do the following:

1. Locate your API and choose **Authorizers**.
2. Choose **Create New Authorizer**.
3. For **Create Authorizer**, type an authorizer name in the **Name** input field.
4. For **Type**, choose the **Lambda** option.
5. For **Lambda Function**, copy-paste the full ARN for the Lambda authorizer function that you have in your second account.
   
   **Note**
   In the Lambda console, you can find the ARN for your function in the upper right corner of the console window.
5. Leave **Lambda Invoke Role** blank to let the API Gateway console set a resource-based policy. The policy grants API Gateway permissions to invoke the authorizer Lambda function. You can also
choose to type the name of an IAM role to allow API Gateway to invoke the authorizer Lambda function. For an example of such a role, see Create an Assumable IAM Role (p. 93).

If you choose to let the API Gateway console set the resource-based policy, the Add Permission to Lambda Function dialog is displayed. Choose OK. After the Lambda authorization is created, you can test it with appropriate authorization token values to verify that it works as expected.

7. For Lambda Event Payload, choose either Token for a TOKEN authorizer or Request for a REQUEST authorizer.

8. Depending on the choice you made in the previous step, do one of the following:
   a. For the Token options, do the following:
      i. Type the name of a header in Token Source. The API client must include a header of this name to send the authorization token to the Lambda authorizer.
      
      ii. Optionally, provide a RegEx statement in Token Validation input field. API Gateway performs initial validation of the input token against this expression and invokes the authorizer upon successful validation. This helps reduce chances of being charged for invalid tokens.
      
      iii. For Authorization Caching, select or clear the Enabled option, depending on whether you want to cache the authorization policy generated by the authorizer or not. When policy caching is enabled, you can choose to modify the TTL value from the default (300). Setting TTL=0 disables policy caching. When policy caching is enabled, the header name specified in Token Source becomes the cache key.
   
   b. For the Request option, do the following:
      i. For Identity Sources, type a request parameter name of a chosen parameter type. Supported parameter types are Header, Query String, Stage Variable, and Context. To add more identity sources, choose Add Identity Source.

      API Gateway uses the specified identity sources as the request authorizer caching key. When caching is enabled, API Gateway calls the authorizer's Lambda function only after successfully verifying that all the specified identity sources are present at runtime. If a specified identify source is missing, null, or empty, API Gateway returns a 401 Unauthorized response without calling the authorizer Lambda function.

      When multiple identity sources are defined, they are all used to derive the authorizer’s cache key. Changing any of the cache key parts causes the authorizer to discard the cached policy document and generate a new one.

      ii. For Authorization Caching, leave the Enabled option selected. Leave the TTL value set to the default (300).

9. Choose Create to create the new Lambda authorizer for the chosen API.

10. You'll see a popup that says Add Permission to Lambda Function: You have selected a Lambda function from another account. Please ensure that you have the appropriate Function Policy on this function. You can do this by running the following AWS CLI command from account 123456789012, followed by an aws lambda add-permission command string.

11. Copy-paste the aws lambda add-permission command string into an AWS CLI window that is configured for your second account. This will grant your first account access to your second account’s Lambda authorizor function.

12. In the popup from the previous step, choose OK.
Control Access to a REST API Using Amazon Cognito User Pools as Authorizer

As an alternative to using IAM roles and policies (p. 362) or Lambda authorizers (p. 380) (formerly known as custom authorizers), you can use an Amazon Cognito user pool to control who can access your API in Amazon API Gateway.

To use an Amazon Cognito user pool with your API, you must first create an authorizer of the COGNITO_USER_POOLS type and then configure an API method to use that authorizer. After the API is deployed, the client must first sign the user in to the user pool, obtain an identity or access token for the user, and then call the API method with one of the tokens, which are typically set to the request's Authorization header. The API call succeeds only if the required token is supplied and the supplied token is valid, otherwise, the client isn't authorized to make the call because the client did not have credentials that could be authorized.

The identity token is used to authorize API calls based on identity claims of the signed-in user. The access token is used to authorize API calls based on the custom scopes of specified access-protected resources. For more information, see Using Tokens with User Pools and Resource Server and Custom Scopes.

To create and configure an Amazon Cognito user pool for your API, you perform the following tasks:

- Use the Amazon Cognito console, CLI/SDK, or API to create a user pool—or use one that's owned by another AWS account.
- Use the API Gateway console, CLI/SDK, or API to create an API Gateway authorizer with the chosen user pool.
- Use the API Gateway console, CLI/SDK, or API to enable the authorizer on selected API methods.

To call any API methods with a user pool enabled, your API clients perform the following tasks:

- Use the Amazon Cognito CLI/SDK or API to sign a user in to the chosen user pool, and obtain an identity token or access token.
- Use a client-specific framework to call the deployed API Gateway API and supply the appropriate token in the Authorization header.

As the API developer, you must provide your client developers with the user pool ID, a client ID, and possibly the associated client secrets that are defined as part of the user pool.

**Note**
To let a user sign in using Amazon Cognito credentials and also obtain temporary credentials to use with the permissions of an IAM role, use Amazon Cognito Federated Identities. For each API resource endpoint HTTP method, set the authorization type, category Method Execution, to AWS_IAM.

In this section, we describe how to create a user pool, how to integrate an API Gateway API with the user pool, and how to invoke an API that's integrated with the user pool.

**Topics**
- Obtain Permissions to Create Amazon Cognito User Pool Authorizers for a REST API (p. 398)
- Create an Amazon Cognito User Pool for a REST API (p. 399)
- Integrate a REST API with an Amazon Cognito User Pool (p. 400)
- Call a REST API Integrated with an Amazon Cognito User Pool (p. 404)
- Configure Cross-Account Amazon Cognito Authorizer for a REST API Using the API Gateway Console (p. 404)
Obtain Permissions to Create Amazon Cognito User Pool Authorizers for a REST API

To create an authorizer with an Amazon Cognito user pool, you must have Allow permissions to create or update an authorizer with the chosen Amazon Cognito user pool. The following IAM policy document shows an example of such permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["apigateway:POST"],
      "Resource": "arn:aws:apigateway:*::/restapis/*/authorizers",
      "Condition": {
        "ArnLike": {
          "apigateway:CognitoUserPoolProviderArn": [
            "arn:aws:cognito-idp:us-east-1:123456789012:userpool/us-east-1_aD06NQmjO",
            "arn:aws:cognito-idp:us-east-1:234567890123:userpool/us-east-1_xJ1MQtPEN"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": ["apigateway:PATCH"],
      "Resource": "arn:aws:apigateway:*::/restapis/*/authorizers/*",
      "Condition": {
        "ArnLike": {
          "apigateway:CognitoUserPoolProviderArn": [
            "arn:aws:cognito-idp:us-east-1:123456789012:userpool/us-east-1_aD06NQmjO",
            "arn:aws:cognito-idp:us-east-1:234567890123:userpool/us-east-1_xJ1MQtPEN"
          ]
        }
      }
    }
  ]
}
```

Make sure that the policy is attached to your IAM user, an IAM group that you belong to, or an IAM role that you're assigned to.

In the preceding policy document, the `apigateway:POST` action is for creating a new authorizer, and the `apigateway:PATCH` action is for updating an existing authorizer. You can restrict the policy to a specific region or a particular API by overriding the first two wildcard (*) characters of the `Resource` values, respectively.

The `Condition` clauses that are used here are to restrict the Allowed permissions to the specified user pools. When a `Condition` clause is present, access to any user pools that don't match the conditions is denied. When a permission doesn't have a `Condition` clause, access to any user pool is allowed.

You have the following options to set the `Condition` clause:
You can set an ArnLike or ArnEquals conditional expression to permit creating or updating COGNITO_USER_POOLS authorizers with the specified user pools only.
• You can set an ArnNotLike or ArnNotEquals conditional expression to permit creating or updating COGNITO_USER_POOLS authorizers with any user pool that isn't specified in the expression.
• You can omit the Condition clause to permit creating or updating COGNITO_USER_POOLS authorizers with any user pool, of any AWS account, and in any region.

For more information on the Amazon Resource Name (ARN) conditional expressions, see Amazon Resource Name Condition Operators. As shown in the example, apigateway:CognitoUserPoolProviderArn is a list of ARNs of the COGNITO_USER_POOLS user pools that can or can't be used with an API Gateway authorizer of the COGNITO_USER_POOLS type.

Create an Amazon Cognito User Pool for a REST API

Before integrating your API with a user pool, you must create the user pool in Amazon Cognito. For instructions on how to create a user pool, see Setting up User Pools in the Amazon Cognito Developer Guide.

Note
Note the user pool ID, client ID, and any client secret. The client must provide them to Amazon Cognito for the user to register with the user pool, to sign in to the user pool, and to obtain an identity or access token to be included in requests to call API methods that are configured with the user pool. Also, you must specify the user pool name when you configure the user pool as an authorizer in API Gateway, as described next.

If you're using access tokens to authorize API method calls, be sure to configure the app integration with the user pool to set up the custom scopes that you want on a given resource server. For more information about using tokens with Amazon Cognito user pools, see Using Tokens with User Pools. For more information about resource servers, see Defining Resource Servers for Your User Pool.

Note the configured resource server identifiers and custom scope names. You need them to construct the access scope full names for OAuth Scopes, which is used by the COGNITO_USER_POOLS authorizer.
Integrate a REST API with an Amazon Cognito User Pool

After creating an Amazon Cognito user pool, in API Gateway, you must then create a 
COGNITO_USER_POOLS authorizer that uses the user pool. The following procedure walks you through 
the steps to do this using the API Gateway console.

Important
After performing any of the procedures below, you'll need to deploy or redeploy your API to 
propagate the changes. For more information about deploying your API, see Deploying a REST 
API in Amazon API Gateway (p. 494).

To create a COGNITO_USER_POOLS authorizer by using the API Gateway console

1. Create a new API, or select an existing API in API Gateway.
2. From the main navigation pane, choose Authorizers under the specified API.
4. To configure the new authorizer to use a user pool, do the following:
   a. Type an authorizer name in Name.
   b. Select the Cognito option.
   c. Choose a region under Cognito User Pool.
   d. Select an available user pool. You must have created a user pool for the selected region in 
      Amazon Cognito for it to show up in the drop-down list.
   e. For Token source, type Authorization as the header name to pass the identity or access 
      token that's returned by Amazon Cognito when a user signs in successfully.
   f. Optionally, type a regular expression in the Token validation field to validate the aud 
      (audience) field of the identity token before the request is authorized with Amazon Cognito.
   g. To finish integrating the user pool with the API, choose Create.
5. After creating the COGNITO_USER_POOLS authorizer, you can optionally test invoke it by supplying 
an identity token that's provisioned from the user pool. You can obtain this identity token by calling 
the Amazon Cognito Identity SDK to perform user sign-in. Make sure to use the returned identity 
token, not the access token.

The preceding procedure creates a COGNITO_USER_POOLS authorizer that uses the newly created 
Amazon Cognito user pool. Depending on how you enable the authorizer on an API method, you can use 
either an identity token or an access token that's provisioned from the integrated user pool. The next 
procedure walks you through the steps to configure the authorizer on an API method.

To configure a COGNITO_USER_POOLS authorizer on methods

1. Choose (or create) a method on your API.
2. Choose Method Request.
3. Under Settings, choose the pencil icon next to Authorization.
4. Choose one of the available Amazon Cognito user pool authorizers from the drop-down list.
5. To save the settings, choose the check mark icon.
6. To use an identity token, do the following:
   a. Leave the OAuth Scopes option unspecified (as NONE).
   b. If needed, choose Integration Request to add the 
      $context.authorizer.claims['property-name'] or 
      $context.authorizer.claims.property-name expressions in a body-mapping template 
      to pass the specified identity claims property from the user pool to the backend. For simple 
      property names, such as sub or custom-sub, the two notations are identical. For complex 
      property names, such as custom:role, you can't use the dot notation. For example, the
following mapping expressions pass the claim's standard fields of sub and email to the backend:

```json
{
  "context" : {
    "sub" : "$context.authorizer.claims.sub",
    "email" : "$context.authorizer.claims.email"
  }
}
```

If you declared a custom claim field when you configured a user pool, you can follow the same pattern to access the custom fields. The following example gets a custom role field of a claim:

```json
{
  "context" : {
    "role" : "$context.authorizer.claims.role"
  }
}
```

If the custom claim field is declared as **custom:role**, use the following example to get the claim's property:

```json
{
  "context" : {
    "role" : "$context.authorizer.claims['custom:role']"
  }
}
```

7. To use an access token, do the following:
   a. Choose the pencil icon next to OAuth Scopes.
   b. Type one or more full names of a scope that has been configured when the Amazon Cognito user pool was created. For example, following the example given in Create an Amazon Cognito User Pool for a REST API (p. 399), one of the scopes is `com.hamuta.movies/drama.view`. Use a single space to separate multiple scopes.
   
   At runtime, the method call succeeds if any scope that's specified on the method in this step matches a scope that's claimed in the incoming token. Otherwise, the call fails with a 401 Unauthorized response.
   c. To save the setting, choose the check mark icon.
8. Repeat these steps for other methods that you choose.

With the COGITO_USER_POOLS authorizer, if the OAuth Scopes option isn't specified, API Gateway treats the supplied token as an identity token and verifies the claimed identity against the one from the user pool. Otherwise, API Gateway treats the supplied token as an access token and verifies the access scopes that are claimed in the token against the authorization scopes declared on the method.

Instead of using the API Gateway console, you can also enable an Amazon Cognito user pool on a method by specifying an OpenAPI definition file and importing the API definition into API Gateway.

To import a COGITO_USER_POOLS authorizer with an OpenAPI definition file

1. Create (or export) an OpenAPI definition file for your API.
2. Specify the COGITO_USER_POOLS authorizer (MyUserPool) JSON definition as part of the securitySchemes section in OpenAPI 3.0 or the securityDefinitions section in Open API 2.0 as follows:
OpenAPI 3.0

```json
"securitySchemes": {
  "MyUserPool": {
    "type": "apiKey",
    "name": "Authorization",
    "in": "header",
    "x-amazon-apigateway-authtype": "cognito_user_pools",
    "x-amazon-apigateway-authorizer": {
      "type": "cognito_user_pools",
      "providerARNs": [
        "arn:aws:cognito-idp:{region}:{account_id}:userpool/{user_pool_id}
      ]
    }
  }
}
```

OpenAPI 2.0

```json
"securityDefinitions": {
  "MyUserPool": {
    "type": "apiKey",
    "name": "Authorization",
    "in": "header",
    "x-amazon-apigateway-authtype": "cognito_user_pools",
    "x-amazon-apigateway-authorizer": {
      "type": "cognito_user_pools",
      "providerARNs": [
        "arn:aws:cognito-idp:{region}:{account_id}:userpool/{user_pool_id}
      ]
    }
  }
}
```

3. To use the identity token for method authorization, add `{ "MyUserPool": [] }` to the security definition of the method, as shown in the following GET method on the root resource.

```json
"paths": {
  ":": {
    "get": {
      "consumes": [
        "application/json"
      ],
      "produces": [
        "text/html"
      ],
      "responses": {
        "200": {
          "description": "200 response",
          "headers": {
            "Content-Type": {
              "type": "string"
            }
          }
        }
      },
      "security": [
        {
          "MyUserPool": []
        }
      ],
      "x-amazon-apigateway-integration": {
        "type": "mock",
        "responses": {
```
4. To use the access token for method authorization, change the above security definition to:

```json
"paths": {
  "/": {
    "get": {
      "consumes": ["application/json"],
      "produces": ["text/html"],
      "responses": {
        "200": {
          "description": "200 response",
          "headers": {
            "Content-Type": {
              "type": "string"
            }
          }
        }
      },
      "security": [
      ],
      "x-amazon-apigateway-integration": {
        "type": "mock",
        "responses": {
          "default": {
            "statusCode": "200",
            "responseParameters": {
              "method.response.header.Content-Type": "text/html"
            }
          }
        },
        "requestTemplates": {
          "application/json": "{\"statusCode\": 200}"
        },
        "passthroughBehavior": "when_no_match"
      }
    }
  }
```


5. If needed, you can set other API configuration settings by using the appropriate OpenAPI definitions or extensions. For more information, see API Gateway Extensions to OpenAPI (p. 575).

Call a REST API Integrated with an Amazon Cognito User Pool

To call a method with a user pool authorizer configured, the client must do the following:

- Enable the user to sign up with the user pool.
- Enable the user to sign in to the user pool.
- Obtain an identity token of the signed-in user from the user pool.
- Include the identity token in the Authorization header (or another header you specified when you created the authorizer).

You can use one of the AWS SDKs to perform these tasks. For example:

- To use the Android SDK, see Setting up the AWS Mobile SDK for Android to Work with User Pools.
- To use the iOS SDK, see Setting Up the AWS Mobile SDK for iOS to Work with User Pools.
- To use JavaScript, see Setting up the AWS SDK for JavaScript in the Browser to Work with User Pools.

The following procedure outlines the steps to perform these tasks. For more information, see the blog posts on Using Android SDK with Amazon Cognito User Pools and Using Amazon Cognito User Pool for iOS.

To call an API that's integrated with a user pool

1. Sign up a first-time user to a specified user pool.
2. Sign in a user to the user pool.
3. Get the user's identity token.
4. Call API methods that are configured with a user pool authorizer, and supply the unexpired token in the Authorization header or another header of your choosing.
5. When the token expires, repeat steps 2–4. Identity tokens provisioned by Amazon Cognito expire within an hour.

For code examples, see an Android Java sample and an iOS Objective-C sample.

Configure Cross-Account Amazon Cognito Authorizer for a REST API Using the API Gateway Console

You can now also use a Amazon Cognito user pool from a different AWS account as your API authorizer. Each account can be in any region where Amazon API Gateway is available. The Amazon Cognito user pool can use bearer token authentication strategies such as OAuth or SAML. This makes it easy to centrally manage and share a central Amazon Cognito user pool authorizer across multiple API Gateway APIs.

In this section, we show how to configure a cross-account Amazon Cognito user pool using the Amazon API Gateway console.

These instructions assume that you already have an API Gateway API in one AWS account and a Amazon Cognito user pool in another account.
Configure Cross-Account Amazon Cognito Authorizer Using the API Gateway Console

Log in to the Amazon API Gateway console in your first account (the one that has your API in it) and do the following:

1. Locate your API and choose **Authorizers**.
2. Choose **Create New Authorizer**.
3. For **Create Authorizer**, type an authorizer name in the **Name** input field.
4. For **Type**, choose the **Cognito** option.
5. For **Cognito User Pool**, copy-paste the full ARN for the user pool that you have in your second account.

   **Note**
   In the Amazon Cognito console, you can find the ARN for your user pool in the **Pool ARN** field of the **General Settings** pane.
6. Type the name of a header in **Token Source**. The API client must include a header of this name to send the authorization token to the Amazon Cognito authorizer.
7. Optionally, provide a RegEx statement in **Token Validation** input field. API Gateway performs initial validation of the input token against this expression and invokes the authorizer upon successful validation. This helps reduce chances of being charged for invalid tokens.
8. Choose **Create** to create the new Amazon Cognito authorizer for your API.

Enable CORS for an API Gateway REST API Resource

Cross-origin resource sharing (CORS) is a browser security feature that restricts cross-origin HTTP requests that are initiated from scripts running in the browser. If your REST API's resources receive non-simple cross-origin HTTP requests, you need to enable CORS support.

**Topics**
- Determining Whether to Enable CORS Support (p. 405)
- What It Means to Enable CORS Support (p. 406)
- Testing CORS (p. 408)
- Enable CORS on a Resource Using the API Gateway Console (p. 408)
- Enable CORS on a Resource Using the API Gateway Import API (p. 410)

Determining Whether to Enable CORS Support

A cross-origin HTTP request is one that is made to:

- A different **domain** (for example, from example.com to amazondomains.com)
- A different **subdomain** (for example, from example.com to petstore.example.com)
- A different **port** (for example, from example.com to example.com:10777)
- A different **protocol** (for example, from https://example.com to http://example.com)

Cross-origin HTTP requests can be divided into two types: **simple** requests and **non-simple** requests.

An HTTP request is **simple** if all of the following conditions are true:

- It is issued against an API resource that allows only **GET**, **HEAD**, and **POST** requests.
• If it is a POST method request, it must include an Origin header.
• The request payload content type is text/plain, multipart/form-data, or application/x-www-form-urlencoded.
• The request does not contain custom headers.
• Any additional requirements that are listed in the Mozilla CORS documentation for simple requests.

For simple cross-origin POST method requests, the response from your resource needs to include the header Access-Control-Allow-Origin, where the value of the header key is set to ‘*’ (any origin) or is set to the origins allowed to access that resource.

All other cross-origin HTTP requests are non-simple requests. If your API’s resources receive non-simple requests, you’ll need to enable CORS support.

What It Means to Enable CORS Support

When a browser receives a non-simple HTTP request, the CORS protocol requires the browser to send a preflight request to the server and wait for approval (or a request for credentials) from the server before sending the actual request. The preflight request appears to your API as an HTTP request that:

• Includes an Origin header.
• Uses the OPTIONS method.
• Includes the following headers:
  • Access-Control-Request-Method
  • Access-Control-Request-Headers

To support CORS, therefore, a REST API resource needs to implement an OPTIONS method that can respond to the OPTIONS preflight request with at least the following response headers mandated by the Fetch standard:

• Access-Control-Allow-Methods
• Access-Control-Allow-Headers
• Access-Control-Allow-Origin

How you enable CORS support depends on your API’s integration type.

Enabling CORS Support for Mock Integrations

For a mock integration, you enable CORS by creating an OPTIONS method to return the required response headers (with appropriate static values) as the method response headers. In addition, each of the actual CORS-enabled methods must also return the Access-Control-Allow-Origin: 'request-originating server addresses' header in at least its 200 response, where the value of the header key is set to '*' (any origin) or is set to the origins allowed to access the resource.

Enabling CORS Support for Lambda or HTTP Non-Proxy Integrations and AWS Service Integrations

For a Lambda custom (non-proxy) integration, HTTP custom (non-proxy) integration, or AWS service integration, you can set up the required headers by using API Gateway method response and integration response settings. API Gateway will create an OPTIONS method and attempt to add the Access-Control-Allow-Origin header to your existing method integration responses. This doesn’t always work and sometimes you need to manually modify the integration response to properly enable CORS. Usually this just means manually modifying the integration response to return the Access-Control-Allow-Origin header.
Enabling CORS Support for Lambda or HTTP Proxy Integrations

For a Lambda proxy integration or HTTP proxy integration, you can still set up the required OPTIONS response headers in API Gateway. However, your backend is responsible for returning the Access-Control-Allow-Origin and Access-Control-Allow-Headers headers, because a proxy integration doesn’t return an integration response.

The following is an example of a Node.js Lambda function that is configured to return the required CORS headers:

```javascript
'use strict';
exports.handler = function(event, context) {
  var responseCode = 200;
  var response = {
    statusCode: responseCode,
    headers: {
      "x-custom-header" : "my custom header value",
      "Access-Control-Allow-Origin": "my-origin.com"
    },
    body: JSON.stringify(event)
  }; 
  context.succeed(response);
};
```

A more complete Node.js example can be found at https://github.com/awslabs/serverless-application-model/blob/master/examples/2016-10-31/api_swagger_cors/index.js.

The following is an example of a Python code snippet that returns the required CORS headers:

```python
response['headers'] = {
    'Content-Type': 'application/json',
    'Access-Control-Allow-Origin': '*',
}
```

The following is an example that returns the required headers for CORS using Serverless Application Model (SAM), including AllowHeaders:

```yaml
Globals:
Api:
  # Allows an application running locally on port 8080 to call this API
Cors:
  AllowMethods: '"OPTIONS,POST,GET"'
  AllowHeaders: '"Content-Type"'
  AllowOrigin: '"http://localhost:8080"'
```

The following is a Lambda proxy example that returns the same headers as the SAM example:

```javascript
return {
    'statusCode': 200,
    'headers': {
      "Access-Control-Allow-Headers": "Content-Type",
      "Access-Control-Allow-Methods": "OPTIONS,POST,GET"
    },
    'body': json.dumps(response)
}
```
Testing CORS

You can test CORS by customizing the following `cURL` command for the actual method and origin header you are using:

```c
```

Enable CORS on a Resource Using the API Gateway Console

You can use the API Gateway console to enable CORS support for one or all methods on a REST API resource that you have created.

**Important**

Resources can contain child resources. Enabling CORS support for a resource and its methods does not recursively enable it for child resources and their methods.

**Enable CORS support on a REST API resource**

2. Choose the API from the **APIs** list.
3. Choose a resource under **Resources**. This will enable CORS for all the methods on the resource.

   Alternatively, you could choose a method under the resource to enable CORS for just this method.

4. Choose **Enable CORS** from the **Actions** drop-down menu.

   ![Enable CORS in API Gateway Console](image)

5. In the **Enable CORS** form, do the following:

   a. In the **Access-Control-Allow-Headers** input field, type a static string of a comma-separated list of headers that the client must submit in the actual request of the resource. Use the console-provided header list of `Content-Type,X-Amz-Date,Authorization,X-Api-Key,X-Amz-Security-Token` or specify your own headers.
b. Use the console-provided value of ‘*’ as the **Access-Control-Allow-Origin** header value to allow access requests from all origins, or specify origins to be permitted to access the resource.

c. Choose **Enable CORS and replace existing CORS headers**.

![Enable CORS and replace existing CORS headers](image)

**Important**
When applying the above instructions to the ANY method in a proxy integration, any applicable CORS headers will not be set. Instead, your backend must return the applicable CORS headers, such as **Access-Control-Allow-Origin**.

6. In **Confirm method changes**, choose **Yes, overwrite existing values** to confirm the new CORS settings.

![Confirm method changes](image)

After CORS is enabled on the GET method, an OPTIONS method is added to the resource, if it is not already there. The 200 response of the OPTIONS method is automatically configured to return the three **Access-Control-Allow-** headers to fulfill preflight handshakes. In addition, the actual (GET) method is also configured by default to return the **Access-Control-Allow-Origin** header in its 200 response as well. For other types of responses, you will need to manually configure them to return **Access-Control-Allow-Origin** header with ‘*’ or specific origins, if you do not want to return the Cross-origin access error.
After you enable CORS support on your resource, you must deploy or redeploy the API for the new settings to take effect. For more information, see the section called "Deploy a REST API from the Console" (p. 495).

Enable CORS on a Resource Using the API Gateway Import API

If you are using the API Gateway Import API (p. 341), you can set up CORS support using an OpenAPI file. You must first define an OPTIONS method in your resource that returns the required headers.

**Note**
Web browsers expect Access-Control-Allow-Headers, and Access-Control-Allow-Origin headers to be set up in each API method that accepts CORS requests. In addition, some browsers first make an HTTP request to an OPTIONS method in the same resource, and then expect to receive the same headers.

The following example creates an OPTIONS method for a mock integration.

OpenAPI 2.0

```yaml
/users
  options:
    summary: CORS support
    description: Enable CORS by returning correct headers
    consumes:
      - application/json
    produces:
      - application/json
    tags:
      - CORS
    x-amazon-apigateway-integration:
      type: mock
      requestTemplates:
        application/json: |
        {
          "statusCode" : 200
        }
      responses:
        "default":
          statusCode: "200"
          responseParameters:
            method.response.header.Access-Control-Allow-Headers : "Content-Type,X-Amz-Date,Authorization,X-Api-Key"
            method.response.header.Access-Control-Allow-Methods : "*"
      responseTemplates:
        application/json: |
        {
        }
  responses:
    200:
      description: Default response for CORS method
      headers:
        Access-Control-Allow-Headers:
          type: "string"
        Access-Control-Allow-Methods:
          type: "string"
        Access-Control-Allow-Origin:
          type: "string"
```

Once you have configured the OPTIONS method for your resource, you can add the required headers to the other methods in the same resource that need to accept CORS requests.
1. Declare the **Access-Control-Allow-Origin** and **Headers** to the response types.

OpenAPI 2.0

```
responses:
  200:
    description: Default response for CORS method
    headers:
      Access-Control-Allow-Headers:
        type: "string"
      Access-Control-Allow-Methods:
        type: "string"
      Access-Control-Allow-Origin:
        type: "string"
```

2. In the `x-amazon-apigateway-integration` tag, set up the mapping for those headers to your static values:

OpenAPI 2.0

```
responses:
  "default":
    statusCode: "200"
    responseParameters:
      method.response.header.Access-Control-Allow-Headers :
        '"Content-Type,X-Amz-Date,Authorization,X-Api-Key"'
      method.response.header.Access-Control-Allow-Methods : '"*"'
```

**Generate and Configure an SSL Certificate for Backend Authentication**

You can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. This allows your HTTP backend to control and accept only requests originating from Amazon API Gateway, even if the backend is publicly accessible.

**Note**

Some backend servers may not support SSL client authentication as API Gateway does and could return an SSL certificate error. For a list of incompatible backend servers, see the section called “Important Notes” (p. 692).

The SSL certificates that are generated by API Gateway are self-signed and only the public key of a certificate is visible in the API Gateway console or through the APIs.

**Topics**

- Generate a Client Certificate Using the API Gateway Console (p. 412)
- Configure an API to Use SSL Certificates (p. 412)
- Test Invoke to Verify the Client Certificate Configuration (p. 412)
- Configure Backend HTTPS Server to Verify the Client Certificate (p. 412)
- Rotate an Expiring Client Certificate (p. 413)
- API Gateway-Supported Certificate Authorities for HTTP and HTTP Proxy Integrations (p. 414)
Generate and Configure an SSL Certificate for Backend Authentication

Generate a Client Certificate Using the API Gateway Console

1. In the main navigation pane, choose Client Certificates.
2. From the Client Certificates pane, choose Generate Client Certificate.
3. Optionally, for Edit, choose to add a descriptive title for the generated certificate and choose Save to save the description. API Gateway generates a new certificate and returns the new certificate GUID, along with the PEM-encoded public key.

You are now ready to configure an API to use the certificate.

Configure an API to Use SSL Certificates

These instructions assume you already completed Generate a Client Certificate Using the API Gateway Console (p. 412).

1. In the API Gateway console, create or open an API for which you want to use the client certificate. Make sure the API has been deployed to a stage.
2. Choose Stages under the selected API and then choose a stage.
3. In the Stage Editor panel, select a certificate under the Client Certificate section.
4. To save the settings, choose Save Changes.

If the API has been deployed previously in the API Gateway console, you'll need to redeploy it for the changes to take effect. For more information, see the section called “Redeploy a REST API to a Stage” (p. 496).

After a certificate is selected for the API and saved, API Gateway uses the certificate for all calls to HTTP integrations in your API.

Test Invoke to Verify the Client Certificate Configuration

2. From Client Certificate, choose Test to invoke the method request.

API Gateway presents the chosen SSL certificate for the HTTP backend to authenticate the API.

Configure Backend HTTPS Server to Verify the Client Certificate

These instructions assume you already completed Generate a Client Certificate Using the API Gateway Console (p. 412) and downloaded a copy of the client certificate. You can download a client certificate by calling clientcertificate:by-id of the API Gateway REST API or get-client-certificate of AWS CLI.

Before configuring a backend HTTPS server to verify the client SSL certificate of API Gateway, you must have obtained the PEM-encoded private key and a server-side certificate that is provided by a trusted certificate authority.

If the server domain name is myserver.mydomain.com, the server certificate's CNAME value must be myserver.mydomain.com or *.mydomain.com.

Supported certificate authorities include Let’s Encrypt or one of the section called “Supported Certificate Authorities for HTTP and HTTP Proxy Integration” (p. 414).

As an example, suppose that the client certificate file is apig-cert.pem and the server private key and certificate files are server-key.pem and server-cert.pem, respectively, For a Node.js server in the backend, you can configure the server similar to the following:
For a node-express app, you can use the client-certificate-auth modules to authenticate client requests with PEM-encoded certificates.

For other HTTPS server, see the documentation for the server.

Rotate an Expiring Client Certificate

The client certificate generated by API Gateway is valid for 365 days. You must rotate the certificate before a client certificate on an API stage expires to avoid any downtime for the API. You can check the expiration date of certificate by calling clientCertificate:by-id of the API Gateway REST API or the AWS CLI command of get-client-certificate and inspecting the returned expirationDate property.

To rotate a client certificate, follow the steps below:

1. Generate a new client certificate, by calling clientCertificate:generate of the API Gateway REST API or the AWS CLI command of generate-client-certificate. In this tutorial, we’ll assume the new client certificate ID is ndiqef.

2. Update the backend server to include the new client certificate. Do not remove the existing client certificate yet.

Some server may require a restart to finish the update. Consult the server documentation to see if you must restart the server during the update.

3. Update the API stage to use the new client certificate by calling stage:update of the API Gateway REST API, with the new client certificate ID (ndiqef):

```
PATCH /restapis/{restapi-id}/stages/stage1 HTTP/1.1
Content-Type: application/json
Host: apigateway.us-east-1.amazonaws.com
X-Amz-Date: 20170603T200400Z
Authorization: AWS4-HMAC-SHA256 Credential=...

{ "patchOperations" : [
    { "op" : "replace",
      "path" : "/clientCertificateId",
      "value" : "ndiqef"
    }
  ]
}
```

or by calling the CLI command of update-stage.

4. Update the backend server to remove the old certificate.

5. Delete the old certificate from API Gateway by calling the clientCertificate:delete of the API Gateway REST API, specifying the clientCertificateId (a1b2c3) of the old certificate:
DEPRECATED /clientcertificates/a1b2c3

or by calling the CLI command of `delete-client-certificate`:

```bash
aws apigateway delete-client-certificate --client-certificate-id a1b2c3
```

To rotate a client certificate in the console for a previously deployed API:

1. In the main navigation pane, choose **Client Certificates**.
2. From the **Client Certificates** pane, choose **Generate Client Certificate**.
3. Open the API for which you want to use the client certificate.
4. Choose **Stages** under the selected API and then choose a stage.
5. In the **Stage Editor** panel, select the new certificate under the **Client Certificate** section.
6. To save the settings, choose **Save Changes**.

You'll need to redeploy the API for the changes to take effect. For more information, see the section called “Redeploy a REST API to a Stage” (p. 496).

### API Gateway-Supported Certificate Authorities for HTTP and HTTP Proxy Integrations

The following list shows the certificate authorities supported by API Gateway for HTTP and HTTP Proxy integrations.

<table>
<thead>
<tr>
<th>Alias name</th>
<th>MD5</th>
<th>SHA256</th>
</tr>
</thead>
</table>
Alias name: mozillacert134.pem
Alias name: mozillacert26.pem
Alias name: chungwaepkirootca
Alias name: verisignclass2g2ca
Alias name: mozillacert15.pem
Alias name: digicertglobalrootca
Alias name: mozillacert66.pem
Alias name: mozillacert122.pem
Alias name: utnuserfirstclientauthemailca
Alias name: verisignc2g1.pem
Alias name: mozillacert55.pem
Alias name: mozillacert101.pem

415
Alias name: mozillacert119.pem
SHA256:
Alias name: verisignc3g1.pem
SHA256:
Alias name: mozillacert44.pem
SHA256:
Alias name: mozillacert108.pem
SHA256:
Alias name: mozillacert95.pem
SHA256:
Alias name: keynecisrootca
SHA256:
Alias name: mozillacert141.pem
SHA256:
Alias name: equifaxsecureglobalbusinessca1
SHA256:
Alias name: affirmtrustpremiumpca
SHA256:
Alias name: baltimorecodesigningca
SHA256:
Alias name: mozillacert33.pem
SHA256:
Alias name: mozillacert100.pem
SHA256:
Alias name: mozillacert84.pem
SHA256:
Alias name: mozillacert130.pem
SHA256:
Alias name: mozillacert148.pem
SHA256:
Alias name: mozillacert22.pem
SHA256:
Alias name: verisignc1g1.pem
SHA256:
Alias name: mozillacert7.pem
SHA256:
Alias name: mozillacert73.pem
SHA256:
Alias name: mozillacert137.pem
SHA256:
Alias name: mozillacert11.pem
SHA256:
Alias name: mozillacert29.pem
SHA256:
Alias name: mozillacert62.pem
SHA256:
Alias name: mozillacert126.pem
MD5: 77:0D:19:B1:21:FD:00:42:9C:3E:0C:AC:5D:0B:02:8E
SHA256:
Alias name: securetrustca
SHA256:
Alias name: soneraclass1ca
SHA256:
Alias name: mozillacert18.pem
SHA256:
Alias name: mozillacert51.pem
SHA256:
Alias name: mozillacert69.pem
SHA256:
Alias name: mozillacert115.pem
MD5: 2B:9B:9E:EA:7B:6C:BP:00:72:1A:CC:C1:77:79:DF:16A
SHA256:
Alias name: verisignclass3g5ca
SHA256:
Alias name: utnuserfirsthardwareca
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias name:</td>
<td>addtrustqualifiedca</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert40.pem</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert104.pem</td>
</tr>
<tr>
<td>Alias name:</td>
<td>certplusclass3pprimaryca</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert80.pem</td>
</tr>
<tr>
<td>Alias name:</td>
<td>swisssigngoldg2ca</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert98.pem</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert144.pem</td>
</tr>
<tr>
<td>Alias name:</td>
<td>starfieldclass2ca</td>
</tr>
<tr>
<td>Alias name:</td>
<td>mozillacert36.pem</td>
</tr>
</tbody>
</table>
## Generate and Configure an SSL Certificate for Backend Authentication

<table>
<thead>
<tr>
<th>Alias name: mozillacert3.pem</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: mozillacert87.pem</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: mozillacert133.pem</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: verisignclass1g2ca</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: certumtrustednetworkca</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: mozillacert129.pem</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA256:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alias name: mozillacert118.pem</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5: 8F:5D:77:06:27:24:9B:3C:5B:93:78:E7:D7:7D:9B:CC</td>
</tr>
</tbody>
</table>
Generate and Configure an SSL Certificate for Backend Authentication

Alias name: gd-class2-root.pem
Alias name: thawteprimaryrootca3
Alias name: quovadisrootca
MD5:  27:DE:36:FE:72:B7:00:03:00:9D:FD:F0:1E:6C:04:24
Alias name: entrustrootca2
Alias name: mozillacert43.pem
Alias name: mozillacert107.pem
Alias name: trustcenterclass4caii
Alias name: mozillacert94.pem
Alias name: mozillacert140.pem
Alias name: telesecglobalrootclass3ca
Alias name: amzninternalcorpcma
Alias name: starfieldservicesrootg2ca
Alias name: mozillacert32.pem
<table>
<thead>
<tr>
<th>Alias name</th>
<th>MD5:</th>
<th>SHA256:</th>
</tr>
</thead>
</table>
SHA256:
Alias name: mozillacert125.pem
MD5: D6:A5:C3:ED:5D:DD:3E:00:Cl:3D:87:92:1F:1D:3F:E4
SHA256:
Alias name: mozillacert17.pem
SHA256:
Alias name: mozillacert50.pem
SHA256:
Alias name: mozillacert68.pem
SHA256:
Alias name: starfieldrootg2ca
SHA256:
42:22
Generate and Configure an SSL Certificate for Backend Authentication

Alias name: mozillacert97.pem
Alias name: mozillacert143.pem
SHA256: 423
Generate and Configure an SSL Certificate for Backend Authentication

Alias name: mozillacert121.pem
Alias name: mozillacert139.pem
MD5: 27:DE:36:FE:72:B7:00:03:00:9D:F4:F0:1E:6C:04:24
Alias name: mozillacert13.pem
Alias name: mozillacert64.pem
Alias name: mozillacert110.pem
Alias name: mozillacert128.pem
Alias name: entrust2048ca
Alias name: mozillacert53.pem
Alias name: mozillacert117.pem
Alias name: mozillacert150.pem
Alias name: thawteserverca
Alias name: secomvalicertclass1ca
Alias name: mozillacert42.pem
Alias name: verisignc2g6.pem
Alias name: godaddyroott2ca
Alias name: gtecybertrustglobalca
| Alias name: mozillacert5.pem | MD5: A1:0B:44:B3:CA:10:D8:00:6E:9D:0F:D8:0F:92:0A:D1 |
### Generate and Configure an SSL Certificate for Backend Authentication

| Alias name: mozillacert135.pem |
| Alias name: camerfirmachamberscommerceca |

| Alias name: mozillacert27.pem |
| Alias name: gd_bundle-g2.pem |

| Alias name: verisignc1g6.pem |

| Alias name: secomevrootca1 |
| Alias name: mozillacert16.pem |

| Alias name: globalsignr3ca |

| Alias name: secomevrootcal |
Alias name: gdroot-g2.pem
SHA256:

Alias name: aolrootca2
SHA256:

Alias name: trustcenteruniversalca1
SHA256:

Alias name: aolrootca1
SHA256:

Alias name: verisignc2g2.pem
SHA256:

Alias name: mozillacert56.pem
SHA256:

Alias name: verisignclass3ca
SHA256:

Alias name: mozillacert102.pem
SHA256:

Alias name: addtrustexternalca
SHA256:

Alias name: verisignc3g2.pem
SHA256:

Alias name: verisignclass3ca
SHA256:

Alias name: mozillacert45.pem
MD5: 1B:2E:00:CA:26:06:90:3D:AD:FF:6F:15:6B:D3:6B:B3
SHA256:

Alias name: verisignc4g2.pem
SHA256:

Alias name: digicertassuredidrootca
SHA256:

Alias name: verisignclass1ca
SHA256:

Alias name: mozillacert109.pem
SHA256:

Alias name: thawtepremiumserverca
Generate and Configure an SSL Certificate for Backend Authentication

Alias name: verisignsca
Alias name: mozillacert96.pem
Alias name: mozillacert142.pem
Alias name: thawteprimaryrootca
SHA256: 428
Use AWS WAF to Protect Your Amazon API Gateway API from Common Web Exploits

AWS WAF is a web application firewall that helps protect web applications and APIs from attacks by allowing you to configure a set of rules (called a web access control list, or web ACL) that allow, block, or count web requests based on customizable web security rules and conditions that you define. For more information, see How AWS WAF Works.

You can use AWS WAF to protect your API Gateway API from common web exploits, such as SQL injection and cross-site scripting (XSS) attacks, that could affect API availability, performance, and compromise security or consume excessive resources. For example, you can create rules to allow or block requests from specified IP address ranges or CIDR blocks or originating from a specific country or region, containing malicious SQL code, or containing malicious script. You can also create rules that match a specified string or a regular expression pattern in HTTP headers, method, query string, URI, and the request body (limited to the first 8 KB). Additionally, you can create rules to block attacks from specific user-agents, bad bots, and content scrapers. For example, you can use rate-based rules to specify the number of web requests that are allowed by each client IP in a trailing, continuously updated, 5-minute period.

Important
AWS WAF is your first line of defense against web exploits. When AWS WAF is enabled on an API, AWS WAF rules are evaluated before other access control features, such as resource...
policies (p. 347), IAM policies (p. 362), Lambda authorizers (p. 380), and Amazon Cognito
authorizers (p. 397). For example, if AWS WAF blocks access from a CIDR block that a resource
policy allows, AWS WAF takes precedence and the resource policy is not evaluated.

To enable AWS WAF for your API, you'll need to:

1. Use the AWS WAF console, AWS SDK, or CLI to create a regional web ACL containing the desired
   combination of AWS WAF managed rules and your own custom rules. For more information, see
   Getting Started with AWS WAF and Creating and Configuring a Web Access Control List (Web ACL).

   **Important**
   API Gateway requires a regional web ACL.

2. Associate the AWS WAF regional web ACL with an API stage. You can do this by using the AWS WAF
   console, AWS SDK, or CLI or by using the API Gateway console, AWS SDK, or CLI.

**To Associate an AWS WAF Regional Web ACL with an API Gateway API Stage Using the API Gateway Console**

To use the API Gateway console to associate an AWS WAF regional web ACL with an existing API Gateway
API stage, use the following steps:

2. In the **APIs** navigation pane, choose the API, and then choose **Stages**.
3. In the **Stages** pane, choose the name of the stage.
4. In the **Stage Editor** pane, choose the **Settings** tab.
5. To associate a regional web ACL with the API stage:
   - In the AWS WAF Web ACL dropdown list, choose the regional web ACL that you want to
     associate with this stage.

   **Note**
   If the Web ACL you need doesn't exist yet, choose **Create WebACL** and then choose **Go
to AWS WAF** to open the WAF console in a new browser tab and create a regional web
ACL. Then return to the API Gateway console to associate the web ACL with the stage.

6. Choose **Save Changes**.

**Associate an AWS WAF Regional Web ACL with an API Gateway API Stage Using the AWS CLI**

To use the AWS CLI to associate an AWS WAF regional web ACL with an existing API Gateway API stage,
call the `associate-web-acl` command as in the following example:

```
aws waf-regional associate-web-acl \
  --web-acl-id 'aabc123a-fb4f-4fc6-becb-2b00831cadcf' \
  --resource-arn 'arn:aws:apigateway:
  {region}::/restapis/4wk1k4onj3/stages/prod'
```

**Associate an AWS WAF Regional Web ACL with an API Stage Using the AWS WAF REST API**

To use the AWS WAF REST API to associate an AWS WAF regional web ACL with an existing API Gateway
API stage, call the `AssociateWebACL` command as in the following example:

```
import boto3
```
Create and Use Usage Plans with API Keys

After you create, test, and deploy your APIs, you can use API Gateway usage plans to make them available as product offerings for your customers. You can configure usage plans and API keys to allow customers to access selected APIs at agreed-upon request rates and quotas that meet their business requirements and budget constraints. If desired, you can set default method-level throttling limits for an API or set throttling limits for individual API methods.

What Are Usage Plans and API Keys?

A usage plan specifies who can access one or more deployed API stages and methods — and also how much and how fast they can access them. The plan uses API keys to identify API clients and meters access to the associated API stages for each key. It also lets you configure throttling limits and quota limits that are enforced on individual client API keys.

API keys are alphanumeric string values that you distribute to app developer customers to grant access to your API. You can use API keys together with usage plans (p. 432) or Lambda authorizers (p. 380) to control access to your APIs. API Gateway can generate API keys on your behalf, or you can import them from a CSV file (p. 446). You can generate an API key in API Gateway, or import it into API Gateway from an external source. For more information, see the section called “Set Up API Keys Using the API Gateway Console” (p. 435).

An API key has a name and a value. (The terms "API key" and "API key value" are often used interchangeably.) The value is an alphanumeric string between 30 and 128 characters, for example, apikey1234abcdefgij0123456789.

Important

API key values must be unique. If you try to create two API keys with different names and the same value, API Gateway considers them to be the same API key.

An API key can be associated with more than one usage plan. A usage plan can be associated with more than one stage. However, a given API key can only be associated with one usage plan for each stage of your API.

A throttling limit is a request rate limit that is applied to each API key that you add to the usage plan. You can also set a default method-level throttling limit for an API or set throttling limits for individual API methods.

A quota limit is the maximum number of requests with a given API key that can be submitted within a specified time interval. You can configure individual API methods to require API key authorization based on usage plan configuration. And you can use the get-usage CLI command and the usage:get REST API method to determine the amount of quota that a customer of your API has used.

Note

Throttling and quota limits apply to requests for individual API keys that are aggregated across all API stages within a usage plan.

Best Practices for API Keys and Usage Plans

The following are suggested best practices to follow when using API keys and usage plans.
• Don't rely on API keys as your only means of authentication and authorization for your APIs. For one thing, if you have multiple APIs in a usage plan, a user with a valid API key for one API in that usage plan can access all APIs in that usage plan. Instead, use an IAM role, a Lambda authorizer (p. 380), or an Amazon Cognito user pool (p. 397).

• If you’re using a developer portal (p. 630) to publish your APIs, note that all APIs in a given usage plan are subscribable, even if you haven't made them visible to your customers.

Steps to Configure a Usage Plan

The following steps outline how you, as the API owner, create and configure a usage plan for your customers.

To configure a usage plan

1. Create one or more APIs, configure the methods to require an API key, and deploy the APIs to stages.
2. Generate or import API keys to distribute to app developers (your customers) who will be using your API.
3. Create the usage plan with the desired throttle and quota limits.
4. Associate API stages and API keys with the usage plan.

Callers of the API must supply an assigned API key in the x-api-key header in requests to the API.

Note

To include API methods in a usage plan, you must configure individual API methods to require an API key (p. 435). For user authentication and authorization, don't use API keys. Use an IAM role, a Lambda authorizer (p. 380), or an Amazon Cognito user pool (p. 397).

Choose an API Key Source

When you associate a usage plan with an API and enable API keys on API methods, every incoming request to the API must contain an API key (p. 6). API Gateway reads the key and compares it against the keys in the usage plan. If there is a match, API Gateway throttles the requests according to the plan's request limit and quota. Otherwise, it throws an InvalidKeyParameter exception. As a result, the caller receives a 403 Forbidden response.

Your API Gateway API can receive API keys from one of two sources:

HEADER

You distribute API keys to your customers and require them to pass the API key as the X-API-Key header of each incoming request.

AUTHORIZER

You have a Lambda authorizer return the API key as part of the authorization response. For more information on the authorization response, see the section called “Output from an Amazon API Gateway Lambda Authorizer” (p. 391).

To choose an API key source for an API by using the API Gateway console:

1. Sign in to the API Gateway console.
2. Choose an existing API or create a new one.
3. In the primary navigation pane, choose Settings under the chosen or newly created API.
4. Under the **API Key Source** section in the **Settings** pane, choose **HEADER** or **AUTHORIZER** from the drop-down list.

5. Choose **Save Changes**.

To choose an API key source for an API by using the AWS CLI, call the `update-rest-api` command as follows:

```bash
aws apigateway update-rest-api --rest-api-id 1234123412 --patch-operations
    op=replace,path=/apiKeySource,value=AUTHORIZER
```

To have the client submit an API key, set the value to **HEADER** in the above CLI command.

To choose an API key source for an API by using the API Gateway REST API, call `restapi:update` as follows:

```http
PATCH /restapis/fugvjdxtri/ HTTP/1.1
Content-Type: application/json
Host: apigateway.us-east-1.amazonaws.com
X-Amz-Date: 20160603T205348Z
Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20160603/us-east-1/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature={sig4_hash}

{
    "patchOperations" : [
        {
            "op" : "replace",
            "path" : "/apiKeySource",
            "value" : "HEADER"
        }
    ]
}
```

To have an authorizer return an API key, set the value to **AUTHORIZER** in the previous `patchOperations` input.

Depending on the API key source type you choose, use one of the following procedures to use header-sourced API keys or authorizer-returned API keys in method invocation:

**To use header-sourced API keys:**

1. Create an API with desired API methods. And deploy the API to a stage.
2. Create a new usage plan or choose an existing one. Add the deployed API stage to the usage plan. Attach an API key to the usage plan or choose an existing API key in the plan. Note the chosen API key value.
3. Set up API methods to require an API key.
4. Redeploy the API to the same stage. If you deploy the API to a new stage, make sure to update the usage plan to attach the new API stage.

The client can now call the API methods while supplying the `x-api-key` header with the chosen API key as the header value.

**To use authorizer-sourced API keys:**

1. Create an API with desired API methods. And deploy the API to a stage.
2. Create a new usage plan or choose an existing one. Add the deployed API stage to the usage plan. Attach an API key to the usage plan or choose an existing API key in the plan. Note the chosen API Key value.

3. Create a custom Lambda authorizer of the token type. Include, as a root-level property of the authorization response, \(\text{usageIdentifierKey: \{api-key\}}\), where \(\{api-key\}\) stands for the API key value mentioned in the previous step.

4. Set up API methods to require an API key and enable the Lambda authorizer on the methods as well.

5. Redeploy the API to the same stage. If you deploy the API to a new stage, make sure to update the usage plan to attach the new API stage.

The client can now call the API key-required methods without explicitly supplying any API key. The authorizer-returned API key is used automatically.

Set Up API Keys Using the API Gateway Console

To set up API keys, do the following:

- Configure API methods to require an API key.
- Create or import an API key for the API in a region.

Before setting up API keys, you must have created an API and deployed it to a stage.

For instructions on how to create and deploy an API by using the API Gateway console, see Creating a REST API in Amazon API Gateway (p. 177) and Deploying a REST API in Amazon API Gateway (p. 494), respectively.

Topics
- Require API Key on a Method (p. 435)
- Create an API Key (p. 436)
- Import API Keys (p. 437)

Require API Key on a Method

The following procedure describes how to configure an API method to require an API key.

To configure an API method to require an API key

1. Sign in to the AWS Management Console and open the API Gateway console at https://console.aws.amazon.com/apigateway/.
2. In the API Gateway main navigation pane, choose Resources.
3. Under Resources, create a new method or choose an existing one.
5. Under the Authorization Settings section, choose true for API Key Required.
6. Select the checkmark icon to save the settings.
7. Deploy or redeploy the API for the requirement to take effect.

If the **API Key Required** option is set to `false` and you don't execute the previous steps, any API key that's associated with an API stage isn't used for the method.

**Create an API Key**

If you've already created or imported API keys for use with usage plans, you can skip this and the next procedure.

**To create an API key**

1. Sign in to the AWS Management Console and open the API Gateway console at https://console.aws.amazon.com/apigateway/.
2. In the API Gateway main navigation pane, choose **API Keys**.
3. From the **Actions** drop-down menu, choose **Create API key**.
4. In **Create API Key**, do the following:
   a. Type an API key name (for example, **MyFirstKey**) in the **Name** input field.
   b. Choose **Auto Generate** to have API Gateway generate the key value, or choose **Custom** to enter the key manually.
c. Choose **Save**.

5. Repeat the preceding steps to create more API keys, if needed.

**Import API Keys**

The following procedure describes how to import API keys to use with usage plans.

**To import API keys**

1. In the main navigation pane, choose **API Keys**.
2. From the **Actions** drop-down menu, choose **Import API keys**.
3. To load a comma-separated key file, choose **Select CSV File**. You can also type the keys manually. For information about the file format, see the section called “API Gateway API Key File Format” (p. 446).
4. Choose **Fail on warnings** to stop the import when there's an error, or choose **Ignore warnings** to continue to import valid key entries when there's an error.

5. To start importing the selected API keys, choose **Import**.

Now that you've set up the API key, you can proceed to **create and use a usage plan** (p. 438).

### Create, Configure, and Test Usage Plans with the API Gateway Console

Before creating a usage plan, make sure that you've set up the desired API keys. For more information, see **Set Up API Keys Using the API Gateway Console** (p. 435).

This section describes how to create and use a usage plan by using the API Gateway console.

**Topics**

- **Migrate Your API to Default Usage Plans (If Needed)** (p. 438)
- **Create a Usage Plan** (p. 439)
- **Test a Usage Plan** (p. 441)
- ** Maintain a Usage Plan** (p. 441)

### Migrate Your API to Default Usage Plans (If Needed)

If you started to use API Gateway after the usage plans feature was rolled out on August 11, 2016, you will automatically have usage plans enabled for you in all supported regions.

If you started to use API Gateway before that date, you may need to migrate to default usage plans. You'll be prompted with the **Enable Usage Plans** option before using usage plans for the first time in...
the selected region. When you enable this option, you have default usage plans created for every unique API stage that's associated with existing API keys. In the default usage plan, no throttle or quota limits are set initially, and the associations between the API keys and API stages are copied to the usage plans. The API behaves the same as before. However, you must use the UsagePlan apiStages property to associate specified API stage values (apiId and stage) with included API keys (via UsagePlanKey), instead of using the ApiKey stageKeys property.

To check whether you've already migrated to default usage plans, use the get-account CLI command. In the command output, the features list will include an entry of "UsagePlans" when usage plans are enabled.

You can also migrate your APIs to default usage plans by using the AWS CLI as follows:

**To migrate to default usage plans using the AWS CLI**

1. Call this CLI command: `update-account`
2. For the cli-input-json parameter, use the following JSON:

```json
[
  {
    "op": "add",
    "path": "/features",
    "value": "UsagePlans"
  }
]
```

**Create a Usage Plan**

The following procedure describes how to create a usage plan.

**To create a usage plan**

1. In the Amazon API Gateway main navigation pane, choose Usage Plans, and then choose Create.
2. Under Create Usage Plan, do the following:
   a. For Name, type a name for your plan (for example, Plan_A).
   b. For Description, type a description for your plan.
   c. Select Enable throttling, and set Rate (for example, 100) and Burst (for example, 200).
   d. Choose Enable quota, and set its limit (for example, 5000) for a selected time interval (for example, Month).
   e. Choose Next.
3. To add a stage to the plan, do the following in the **Associated API Stages** pane:
   a. Choose **Add API Stage**.
   b. Choose an API (for example, PetStore) from the API drop-down list.
   c. Choose a stage (for example, Stage_1) from the Stage drop-down list.
   d. Choose the checkmark icon to save.

4. To configure method throttling (p. 507), do the following:
   a. Choose **Configure Method Throttling**.
   b. Choose **Add Resource/Method**.
   c. Choose the resource from the Resource drop-down menu.
   d. Choose the method from the Method drop-down menu.
Use Usage Plans with API Keys

5. To add a key to the plan, do the following in the **API Keys** tab:
   a. To use an existing key, choose **Add API Key to Usage Plan**.
   b. For **Name**, type a name for the key you want to add (for example, **MyFirstKey**).
   c. Choose the checkmark icon to save.
   d. As needed, repeat the preceding steps to add other existing API keys to this usage plan.

   **Note**
   Alternatively, to create a new API key and add it to the usage plan, choose **Create API Key and add to Usage Plan** and follow the instructions.

   **Note**
   An API key can be associated with more than one usage plan. A usage plan can be associated with more than one stage. However, a given API key can only be associated with one usage plan for each stage of your API.

6. To finish creating the usage plan, choose **Done**.

7. If you want to add more API stages to the usage plan, choose **Add API Stage** to repeat the preceding steps.

**Test a Usage Plan**

To test the usage plan, you can use an AWS SDK, AWS CLI, or a REST API client like Postman. For an example of using Postman to test the usage plan, see Test Usage Plans (p. 445).

**Maintain a Usage Plan**

Maintaining a usage plan involves monitoring the used and remaining quotas over a given time period and, if needed, extending the remaining quotas by a specified amount. The following procedures describe how to monitor and extend quotas.
To monitor used and remaining quotas

1. In the API Gateway main navigation pane, choose Usage Plans.
2. Choose a usage plan from the list of usage plans.
3. From within the specified plan, choose API Keys.
4. Choose an API key, and then choose Usage to view Subscriber's Traffic from the plan you're monitoring.
5. Optionally, choose Export, choose a From date and a To date, choose JSON or CSV for the exported data format, and then choose Export.

The following example shows an exported file.

```json
{  
  "thisPeriod": {  
    "px1KW6...qBazOJH": [  
      [0, 5000],
      [0, 5000],
      [0, 10]
    ],  
  },  
  "startDate": "2016-08-01",
  "endDate": "2016-08-03"
}
```

The usage data in the example shows the daily usage data for an API client, as identified by the API key (px1KW6...qBazOJH), between August 1, 2016 and August 3, 2016. Each daily usage data shows used and remaining quotas. In this example, the subscriber hasn't used any allotted quotas yet, and the API owner or administrator has reduced the remaining quota from 5000 to 10 on the third day.

To extend the remaining quotas

1. Repeat steps 1–3 of the previous procedure.
2. In the usage plan pane, choose Extension from the usage plan window.
3. Type a number for the Remaining request quotas.
4. Choose Save.

Set Up API Keys Using the API Gateway REST API

To set up API keys, do the following:

- Configure API methods to require an API key.
- Create or import an API key for the API in a region.

Before setting up API keys, you must have created an API and deployed it to a stage.
For the REST API calls to create and deploy an API, see `restapi:create` and `deployment:create`, respectively.

**Topics**
- Require an API Key on a Method (p. 443)
- Create or Import API Keys (p. 443)

**Require an API Key on a Method**

To require an API key on a method, do one of the following:

- Call `method:put` to create a method. Set `apiKeyRequired` to `true` in the request payload.
- Call `method:update` to set `apiKeyRequired` to `true`.

**Create or Import API Keys**

To create or import an API key, do one of the following:

- Call `apikey:create` to create an API key.
- Call `apikey:import` to import an API key from a file. For the file format, see API Gateway API Key File Format (p. 446).

With the API key created, you can now proceed to Create, Configure, and Test Usage Plans Using the API Gateway CLI and REST API (p. 443).

**Create, Configure, and Test Usage Plans Using the API Gateway CLI and REST API**

Before configuring a usage plan, you must have already done the following: set up methods of a selected API to require API keys, deployed or redeployed the API to a stage, and created or imported one or more API keys. For more information, see Set Up API Keys Using the API Gateway REST API (p. 442).

To configure a usage plan by using the API Gateway REST API, use the following instructions, assuming that you've already created the APIs to be added to the usage plan.

**Topics**
- Migrate to Default Usage Plans (p. 443)
- Create a Usage Plan (p. 444)
- Manage a Usage Plan by Using the AWS CLI (p. 444)
- Test Usage Plans (p. 445)

**Migrate to Default Usage Plans**

When creating a usage plan the first time, you can migrate existing API stages that are associated with selected API keys to a usage plan by calling `account:update` with the following body:

```json
{
    "patchOperations" : [ {
        "op" : "add",
        "path" : "/features",
        "value" : "UsagePlans"
    } ]
}
```
For more information about migrating API stages associated with API keys, see Migrate to Default Usage Plans in the API Gateway Console (p. 438).

Create a Usage Plan

The following procedure describes how to create a usage plan.

To create a usage plan with the REST API

1. Call usageplan:create to create a usage plan. In the payload, specify the name and description of the plan, associated API stages, rate limits, and quotas.
   
   Make note of the resultant usage plan identifier. You need it in the next step.

2. Do one of the following:
   
   a. Call usageplankey:create to add an API key to the usage plan. Specify keyId and keyType in the payload.
      
      To add more API keys to the usage plan, repeat the previous call, one API key at a time.
   
   b. Call apikey:import to add one or more API keys directly to the specified usage plan. The request payload should contain API key values, the associated usage plan identifier, the Boolean flags to indicate that the keys are enabled for the usage plan, and, possibly, the API key names and descriptions.
      
      The following example of the apikey:import request adds three API keys (as identified by key, name, and description) to one usage plan (as identified by usageplanIds):

      ```
      POST /apikeys?mode=import&format=csv&failonwarnings=fase HTTP/1.1
      Host: apigateway.us-east-1.amazonaws.com
      Content-Type: text/csv
      Authorization: ...

      key,name, description, enabled, usageplanIds
      abcdef1234ghijklmnop8901234567, importedKey_1, firstone, TRUE, n371pt
      abcdef1234ghijklmnop0123456789, importedKey_2, secondone, TRUE, n371pt
      abcdef1234ghijklmnop9012345678, importedKey_3,          , true, n371pt
      
      As a result, three UsagePlanKey resources are created and added to the UsagePlan.
      
      You can also add API keys to more than one usage plan this way. To do this, change each usageplanIds column value to a comma-separated string that contains the selected usage plan identifiers, and is enclosed within a pair of quotes ("n371pt,m282qs" or 'n371pt,m282qs').
      
      Note
      An API key can be associated with more than one usage plan. A usage plan can be associated with more than one stage. However, a given API key can only be associated with one usage plan for each stage of your API.

Manage a Usage Plan by Using the AWS CLI

The following code examples show how to add, remove, or modify the method-level throttling settings in a usage plan by calling the update-usage-plan command.

Note
Be sure to change us-east-1 to the appropriate region value for your API.

To add or replace a rate limit for throttling an individual resource and method:
To add or replace a burst limit for throttling an individual resource and method:

```
aws apigateway --region us-east-1 update-usage-plan --usage-plan-id <planId> --patch-operations op="replace",path="/apiStages/<apiId>:<stage>/throttle/<resourcePath>/<httpMethod>/burstLimit",value="1"
```

To remove the method-level throttling settings for an individual resource and method:

```
aws apigateway --region us-east-1 update-usage-plan --usage-plan-id <planId> --patch-operations op="remove",path="/apiStages/<apiId>:<stage>/throttle/<resourcePath>/<httpMethod>",value=""
```

To remove all method-level throttling settings for an API:

```
aws apigateway --region us-east-1 update-usage-plan --usage-plan-id <planId> --patch-operations op="remove",path="/apiStages/<apiId>:<stage>/throttle",value=""
```

Here is an example using the Pet Store sample API:

```
aws apigateway --region us-east-1 update-usage-plan --usage-plan-id <planId> --patch-operations op="replace",path="/apiStages/<apiId>:<stage>/throttle",value='"{"/pets/GET":{"rateLimit":1.0,"burstLimit":1},"/GET":{"rateLimit":1.0,"burstLimit ":1}}"'
```

**Test Usage Plans**

As an example, let's use the PetStore API, which was created in TUTORIAL: Create a REST API by Importing an Example (p. 42). Assume that the API is configured to use an API key of Hiorr45VR...c4GJc. The following steps describe how to test a usage plan.

**To test your usage plan**

- Make a GET request on the Pets resource (/pets), with the ?type=...&page=... query parameters, of the API (for example, xbvxlpijch) in a usage plan:

  ```
  GET /testStage/pets?type=dog&page=1 HTTP/1.1
  x-api-key: Hiorr45VR...c4GJc
  Content-Type: application/x-www-form-urlencoded
  Host: xbvxlpijch.execute-api.ap-southeast-1.amazonaws.com
  X-Amz-Date: 20160803T001845Z
  Authorization: AWS4-HMAC-SHA256 Credential={access_key_ID}/20160803/ap-southeast-1/execute-api/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-api-key, Signature={sigv4_hash}
  ```

**Note**

You must submit this request to the execute-api component of API Gateway and provide the required API key (for example, Hiorr45VR...c4GJc) in the required x-api-key header.

The successful response returns a 200 OK status code and a payload that contains the requested results from the backend. If you forget to set the x-api-key header or set it with an incorrect key,
you get a 403 Forbidden response. However, if you didn’t configure the method to require an API key, you will likely get a 200 OK response whether you set the x-api-key header correctly or not, and the throttle and quota limits of the usage plan are bypassed.

Occasionally, when an internal error occurs where API Gateway is unable to enforce usage plan throttling limits or quotas for the request, API Gateway serves the request without applying the throttling limits or quotas as specified in the usage plan. But, it logs an error message of Usage Plan check failed due to an internal error in CloudWatch. You can ignore such occasional errors.

**API Gateway API Key File Format**

API Gateway can import API keys from external files of a comma-separated value (CSV) format, and then associate the imported keys with one or more usage plans. The imported file must contain the Name and Key columns. The column header names aren't case sensitive, and columns can be in any order, as shown in the following example:

<table>
<thead>
<tr>
<th>Key, name</th>
</tr>
</thead>
<tbody>
<tr>
<td>apikey1234abcdefghij0123456789, MyFirstApiKey</td>
</tr>
</tbody>
</table>

A Key value must be between 30 and 128 characters.

An API key file can also have the Description, Enabled, or UsagePlanIds column, as shown in the following example:

<table>
<thead>
<tr>
<th>Name, key, description, Enabled, usageplanIds</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyFirstApiKey, apikey1234abcdefghij0123456789, An imported key, TRUE, c7y23b</td>
</tr>
</tbody>
</table>

When a key is associated with more than one usage plan, the UsagePlanIds value is a comma-separated string of the usage plan IDs, enclosed with a pair of double or single quotes, as shown in the following example:

<table>
<thead>
<tr>
<th>Enabled, Name, key, UsageplanIds</th>
</tr>
</thead>
<tbody>
<tr>
<td>true, MyFirstApiKey, apikey1234abcdefghij0123456789, &quot;c7y23b, glvrsr&quot;</td>
</tr>
</tbody>
</table>

Unrecognized columns are permitted, but are ignored. The default value is an empty string or a true Boolean value.

The same API key can be imported multiple times, with the most recent version overwriting the previous one. Two API keys are identical if they have the same key value.

**Documenting a REST API in API Gateway**

To help customers understand and use your API, you should document the API. To help you document your API, API Gateway lets you add and update the help content for individual API entities as an integral part of your API development process. API Gateway stores the source content and enables you to archive different versions of the documentation. You can associate a documentation version with an API stage, export a stage-specific documentation snapshot to an external OpenAPI file, and distribute the file as a publication of the documentation.

To document your API, you can call the API Gateway REST API, use one of the AWS SDKs or AWS CLIs for API Gateway, or use the API Gateway console. In addition, you can import or export the documentation parts defined in an external OpenAPI file. Before explaining how to document your API, we'll show how API documentation is represented in API Gateway.
Representation of API Documentation in API Gateway

API Gateway API documentation consists of individual documentation parts associated with specific API entities that include API, resource, method, request, response, message parameters (i.e., path, query, header), as well as authorizers and models.

In API Gateway, a documentation part is represented by a `DocumentationPart` resource. The API documentation as a whole is represented by the `DocumentationParts` collection.

Documenting an API involves creating `DocumentationPart` instances, adding them to the `DocumentationParts` collection, and maintaining versions of the documentation parts as your API evolves.

Topics
- Documentation Parts (p. 447)
- Documentation Versions (p. 454)

Documentation Parts

A `DocumentationPart` resource is a JSON object that stores the documentation content applicable to an individual API entity. Its `properties` field contains the documentation content as a map of key-value pairs. Its `location` property identifies the associated API entity.

The shape of a content map is determined by you, the API developer. The value of a key-value pair can be a string, number, boolean, object, or array. The shape of the `location` object depends on the targeted entity type.

The `DocumentationPart` resource supports content inheritance: the documentation content of an API entity is applicable to children of that API entity. For more information about the definition of child entities and content inheritance, see Inherit Content from an API Entity of More General Specification (p. 449).

Location of a Documentation Part

The `location` property of a `DocumentationPart` instance identifies an API entity to which the associated content applies. The API entity can be an API Gateway REST API resource, such as `RestApi, Resource, Method, MethodResponse, Authorizer`, or `Model`. The entity can also be a message parameter, such as a URL path parameter, a query string parameter, a request or response header parameter, a request or response body, or response status code.

To specify an API entity, set the `type` attribute of the `location` object to be one of `API, AUTHORIZER, MODEL, RESOURCE, METHOD, PATH_PARAMETER, QUERY_PARAMETER, REQUEST_HEADER, REQUEST_BODY, RESPONSE, RESPONSE_HEADER, or RESPONSE_BODY`.

Depending on the type of an API entity, you might specify other `location` attributes, including `method`, `name`, `path`, and `statusCode`. Not all of these attributes are valid for a given API entity. For
example, type, path, name, and statusCode are valid attributes of the RESPONSE entity; only type
and path are valid location attributes of the RESOURCE entity. It is an error to include an invalid field in
the location of a DocumentationPart for a given API entity.

Not all valid location fields are required. For example, type is both the valid and required location
field of all API entities. However, method, path, and statusCode are valid but not required attributes
for the RESPONSE entity. When not explicitly specified, a valid location field assumes its default
value. The default path value is /, i.e., the root resource of an API. The default value of method, or
statusCode is *, meaning any method, or status code values, respectively.

Content of a Documentation Part

The properties value is encoded as a JSON string. The properties value contains any information
you choose to meet your documentation requirements. For example, the following is a valid content
map:

```json
{
    "info": {
        "description": "My first API with Amazon API Gateway."
    },
    "x-custom-info" : "My custom info, recognized by OpenAPI.",
    "my-info" : "My custom info not recognized by OpenAPI."
}
```

Although API Gateway accepts any valid JSON string as the content map, the content attributes are
treated as two categories: those that can be recognized by OpenAPI and those that cannot. In the
preceding example, info, description, and x-custom-info are recognized by OpenAPI as a standard
OpenAPI object, property, or extension. In contrast, my-info is not compliant with the OpenAPI
specification. API Gateway propagates OpenAPI-compliant content attributes into the API entity
definitions from the associated DocumentationPart instances. API Gateway does not propagate the
non-compliant content attributes into the API entity definitions.

As another example, here is DocumentationPart targeted for a Resource entity:

```json
{
    "location" : {
        "type" : "RESOURCE",
        "path": "/pets"
    },
    "properties" : {
        "summary" : "The /pets resource represents a collection of pets in PetStore.",
        "description": "... a child resource under the root...",
    }
}
```

Here, both type and path are valid fields to identify the target of the RESOURCE type. For the root
resource (/), you can omit the path field.

```json
{
    "location" : {
        "type" : "RESOURCE"
    },
    "properties" : {
        "description" : "The root resource with the default path specification."
    }
}
```

This is the same as the following DocumentationPart instance:
Inherit Content from an API Entity of More General Specifications

The default value of an optional location field provides a patterned description of an API entity. Using the default value in the location object, you can add a general description in the properties map to a DocumentationPart instance with this type of location pattern. API Gateway extracts the applicable OpenAPI documentation attributes from the DocumentationPart of the generic API entity and injects them into a specific API entity with the location fields matching the general location pattern, or matching the exact value, unless the specific entity already has a DocumentationPart instance associated with it. This behavior is also known as content inheritance from an API entity of more general specifications.

Content inheritance does not apply to certain API entity types. See the table below for details.

When an API entity matches more than one DocumentationPart's location pattern, the entity will inherit the documentation part with the location fields of the highest precedence and specificities. The order of precedence is path > statusCode. For matching with the path field, API Gateway chooses the entity with the most specific path value. The following table shows this with a few examples.

<table>
<thead>
<tr>
<th>Case</th>
<th>path</th>
<th>statusCode</th>
<th>name</th>
<th>Remark</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>/pets</td>
<td>*</td>
<td>id</td>
<td>Documentation associated with this location pattern will be inherited by entities matching the location pattern.</td>
</tr>
<tr>
<td>2</td>
<td>/pets</td>
<td>200</td>
<td>id</td>
<td>Documentation associated with this location pattern will be inherited by entities matching the path.</td>
</tr>
<tr>
<td>Case</td>
<td>path</td>
<td>statusCodes</td>
<td>name</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>-------------</td>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>location pattern when both Case 1 and Case 2 are matched, because Case 2 is more specific than Case 1.</td>
</tr>
<tr>
<td>3</td>
<td>/pets/</td>
<td>*</td>
<td>id</td>
<td>Documentation associated with this location pattern will be inherited by entities matching the location pattern when Cases 1, 2, and 3 are matched, because Case 3 has a higher precedence than Case 2 and is more specific than Case 1.</td>
</tr>
</tbody>
</table>
Here is another example to contrast a more generic `DocumentationPart` instance to a more specific one. The following general error message of "Invalid request error" is injected into the OpenAPI definitions of the 400 error responses, unless overridden.

```json
{
   "location": {
      "type": "RESPONSE",
      "statusCode": "400"
   },
   "properties": {
      "description": "Invalid request error."
   }
}
```

With the following overwrite, the 400 responses to any methods on the /pets resource has a description of "Invalid petId specified" instead.

```json
{
   "location": {
      "type": "RESPONSE",
      "path": "/pets",
      "statusCode": "400"
   },
   "properties": {
      "description": "Invalid petId specified."
   }
}
```

## Valid Location Fields of `DocumentationPart`

The following table shows the valid and required fields as well as applicable default values of a `DocumentationPart` resource that is associated with a given type of API entities.

<table>
<thead>
<tr>
<th>API entity</th>
<th>Valid location fields</th>
<th>Required location fields</th>
<th>Default field values</th>
<th>Inheritable Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>API</td>
<td>{ &quot;location&quot;: {</td>
<td>type</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;API&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>}, ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>{ &quot;location&quot;: {</td>
<td>type</td>
<td>The default value of path is /.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;RESOURCE&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;path&quot;: &quot;resource_path&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>}, ...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Method</td>
<td>{ &quot;location&quot;: {</td>
<td>type</td>
<td>The default values of path and method are / and * respectively.</td>
<td>Yes, matching path by prefix and matching method of any values.</td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;METHOD&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;path&quot;:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;resource_path&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API entity</td>
<td>Valid location fields</td>
<td>Required location fields</td>
<td>Default field values</td>
<td>Inheritable Content</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>{</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;method&quot;:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;http_verb&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>},</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>}</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Query parameter</td>
<td>{</td>
<td>type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;location&quot;: {</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;QUERY_PARAMETER&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;path&quot;: &quot;resource_path&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;method&quot;: &quot;HTTP_verb&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;name&quot;: &quot;query_parameter_name&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>},</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request body</td>
<td>{</td>
<td>type</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;location&quot;: {</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;REQUEST_BODY&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;path&quot;: &quot;resource_path&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;method&quot;: &quot;http_verb&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>},</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Request header</td>
<td>{</td>
<td>type, name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>parameter</td>
<td>&quot;location&quot;: {</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;type&quot;: &quot;REQUEST_HEADER&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;path&quot;: &quot;resource_path&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;method&quot;: &quot;HTTP_verb&quot;,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&quot;name&quot;: &quot;header_name&quot;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>},</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### API entity | Valid location fields | Required location fields | Default field values | Inheritable Content
---|---|---|---|---
Request path parameter | 

```
{
  "location": {
    "type": "PATH_PARAMETER",
    "path": "resource/{path_parameter_name}",
    "method": "HTTP_verb",
    "name": "path_parameter_name"
  },
  ...
}
```

type, name

The default values of path and method are / and *, respectively.

Yes, matching path by prefix and matching method by exact values.

Response | 

```
{
  "location": {
    "type": "RESPONSE",
    "path": "resource_path",
    "method": "http_verb",
    "statusCode": "status_code"
  },
  ...
}
```

type

The default values of path, method, and statusCode are /, * and *, respectively.

Yes, matching path by prefix and matching method and statusCode by exact values.

Response header | 

```
{
  "location": {
    "type": "RESPONSE_HEADER",
    "path": "resource_path",
    "method": "http_verb",
    "statusCode": "status_code",
    "name": "header_name"
  },
  ...
}
```

type, name

The default values of path, method and statusCode are /, * and *, respectively.

Yes, matching path by prefix and matching method, and statusCode by exact values.

Response body | 

```
{
  "location": {
    "type": "RESPONSE_BODY",
    "path": "resource_path",
    "method": "http_verb",
    "statusCode": "status_code"
  },
  ...
}
```

type

The default values of path, method and statusCode are /, * and *, respectively.

Yes, matching path by prefix and matching method, and statusCode by exact values.
### Documentation Versions

A documentation version is a snapshot of the `DocumentationParts` collection of an API and is tagged with a version identifier. Publishing the documentation of an API involves creating a documentation version, associating it with an API stage, and exporting that stage-specific version of the API documentation to an external OpenAPI file. In API Gateway, a documentation snapshot is represented as a `DocumentationVersion` resource.

As you update an API, you create new versions of the API. In API Gateway, you maintain all the documentation versions using the `DocumentationVersions` collection.

### Document an API Using the API Gateway Console

In this section, we describe how to create and maintain documentation parts of an API using the API Gateway console.

A prerequisite for creating and editing the documentation of an API is that you must have already created the API. In this section, we use the PetStore API as an example. To create an API using the API Gateway console, follow the instructions in TUTORIAL: Create a REST API by Importing an Example (p. 42).

**Topics**
- Document the API Entity (p. 455)
- Document a RESOURCE Entity (p. 457)
- Document a METHOD Entity (p. 457)
- Document a QUERY_PARAMETER Entity (p. 458)
- Document a PATH_PARAMETER Entity (p. 459)
- Document a REQUEST_HEADER Entity (p. 459)
- Document a REQUEST_BODY Entity (p. 460)
- Document a RESPONSE Entity (p. 460)
- Document a RESPONSE_HEADER Entity (p. 460)
- Document a RESPONSE_BODY Entity (p. 461)
Document the API Entity

To add a documentation part for the API entity, choose Resources from the PetStore API. Choose the Actions → Edit API Documentation menu item.

If a documentation part was not created for the API, you get the documentation part's properties map editor. Type the following properties map in the text editor and then choose Save to create the documentation part.

```
{
  "info": {
    "description": "Your first API Gateway API.",
    "contact": {
      "name": "John Doe",
      "email": "john.doe@api.com"
    }
  }
}
```

**Note**
You do not need to encode the properties map into a JSON string. The API Gateway console stringifies the JSON object for you.
Provide your API documentation in JSON format in the form below.

```
Type   API
1 |
2   "info": {
3     "description": "Your first API Gateway API.",
4     "contact": {
5       "name": "John Doe",
6       "email": "john.doe@api.com"
7     }
8   }
9 ]
```

If a documentation part has already been created, you first get the properties map viewer, as shown in the following.
Document an API Using the API Gateway Console

Choosing **Edit** brings up the **properties** map editor as shown previously.

### Document a RESOURCE Entity

To add or edit the documentation part for the API's root resource, choose **/** under the **Resource** tree, and then choose the **Actions → Edit Resource Documentation** menu item.

If no documentation part was created for this entity, you get the **Documentation** window. Type a valid properties map in the editor. Then choose **Save** and **Close**.

```json
{
   "description": "The PetStore's root resource."
}
```

If a documentation part has already been defined for the RESOURCE entity, you get the documentation viewer. Choose **Edit** to open the **Documentation** editor. Modify the existing properties map. Choose **Save** and then choose **Close**.

If necessary, repeat these steps to add a documentation part to other RESOURCE entities.

### Document a METHOD Entity

To add or edit documentation for a METHOD entity, using the **GET** method on the root resource as an example, choose **GET** under the **/** resource and the choose the **Actions → Edit Method Documentation** menu item.
For the new documentation part, type the following properties map in the **Documentation** editor in the **Documentation** window. Then choose **Save** and **Close**.

```json
{
  "tags" : [ "pets" ],
  "description" : "PetStore HTML web page containing API usage information"
}
```

For the existing documentation, choose **Edit** from the **Documentation** viewer. Edit the documentation content in the **Documentation** editor and choose **Save**. Choose **Close**.

From the **Documentation** viewer, you can also delete the documentation part.

If necessary, repeat these steps to add a documentation part to other methods.

### Document a **QUERY_PARAMETER** Entity

To add or edit a documentation part for a request query parameter, using the `GET /pets? type=...&page=...` method as an example, choose **GET** under `/pets` from the **Resources** tree. Choose **Method Request** in the **Method Execution** window. Expand the **URL Query String Parameters** section. Choose the **page** query parameter, for example, and choose the book icon to open the **Documentation** viewer or editor.

Alternatively, you can choose **Documentation** under the **PetStore** API from the main navigation pane. Then choose **Query Parameter** for **Type**. For the PetStore example API, this shows the documentation parts for the **page** and **type** query parameters.
For an API with query parameters defined for other methods, you can filter your selection by specifying the path of the affected resource for **Path**, choosing the desired HTTP method from **Method**, or typing the query parameter name in **Name**.

For example, choose the *page* query parameter. Choose **Edit** to modify the existing documentation. Choose **Save** to save the change.

To add a new documentation part for a **QUERY_PARAMETER** entity, choose **Create Documentation Part**. Choose **Query Parameter** for **Type**. Type a resource path (e.g., `/pets`) in **Path**. Choose an HTTP verb (e.g., GET) for **Method**. Type a properties description in the text editor. Then choose **Save**.

If necessary, repeat these steps to add a documentation part to other request query parameters.

**Document a PATH_PARAMETER Entity**

To add or edit documentation for a path parameter, go to **Method Request** of the method on the resource specified by the path parameter. Expand the **Request Paths** section. Choose the book icon for the path parameter to open the **Documentation** viewer or editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the **PetStore** API from the main navigation pane. Choose **Path Parameter** for **Type**. Choose **Edit** on a path parameter from the list. Modify the content and then choose **Save**.

To add documentation for a path parameter not listed, choose **Create Documentation Part**. Choose **Path Parameter** for **Type**. Set a resource path in **Path**, choose a method from **Method**, and set a path parameter name in **Name**. Add the documentation's properties and choose **Save**.

If required, repeat these steps to add or edit a documentation part to other path parameters.

**Document a REQUEST_HEADER Entity**

To add or edit documentation for a request header, go to **Method Request** of the method with the header parameter. Expand the **HTTP Request Headers** section. Choose the book icon for the header to open the **Documentation** viewer or editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the API from the main navigation pane. Then choose **Request Header** for **Type**. Choose **Edit** on a listed request header to change the documentation. To
add documentation for an unlisted request header, choose **Create Documentation Part**. Choose **Request Header** for **Type**. Specify a resource path in **Path**. Choose a method for **Method**. Type a header name in **Name**. Then add and save a properties map.

If required, repeat these steps to add or edit a documentation part to other request headers.

**Document a REQUEST_BODY Entity**

To add or edit documentation for a request body, go to **Method Request** for a method. Choose the book icon for **Request Body** to open the **Documentation** viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the API from the main navigation pane. Then choose **Request Body** for **Type**. Choose **Edit** on a listed request body to change the documentation. To add documentation for an unlisted request body, choose **Create Documentation Part**. Choose **Request Body** for **Type**. Set a resource path in **Path**. Choose an HTTP verb for **Method**. Then add and save a properties map.

If required, repeat these steps to add or edit a documentation part to other request bodies.

**Document a RESPONSE Entity**

To add or edit documentation for a response, go to **Method Response** of a method. Choose the book icon for **Method Response** to open the **Documentation** viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the API from the main navigation pane. Then choose **Response (status code)** for **Type**. Choose **Edit** on a listed response of a specified HTTP status code to change the documentation. To add documentation for an unlisted response body, choose **Create Documentation Part**. Choose **Response (status code)** for **Type**. Set a resource path in **Path**. Choose an HTTP verb for **Method**. Type an HTTP status code in **Status Code**. Then add and save the documentation part properties.

If required, repeat these steps to add or edit a documentation part to other responses.

**Document a RESPONSE_HEADER Entity**

To add or edit documentation for a response header, go to **Method Response** of a method. Expand a response section of a given HTTP status. Choose the book icon for a response header under **Response Headers for StatusCode** to open the **Documentation** viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the API from the main navigation pane. Then choose **Response Header** for **Type**. Choose **Edit** on a listed response header to change the documentation. To add documentation for an unlisted response header, choose **Create Documentation Part**. Choose
**Response Header** for **Type**. Set a resource path in **Path**. Choose an HTTP verb for **Method**. Type an HTTP status code in **Status Code**. Type the response header name in **Name**. Then add and save the documentation part properties.

If required, repeat these steps to add or edit a documentation part to other response headers.

### Document a **RESPONSE_BODY** Entity

To add or edit documentation for a response body, go to **Method Response** of a method. Expand the response section of a given HTTP status. Choose the book icon for **Response Body for StatusCode** to open the **Documentation** viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose **Documentation** under the API from the main navigation pane. Then choose **Response Body** for **Type**. Choose **Edit** on a listed response body to change the documentation. To add documentation for an unlisted response body, choose **Create Documentation Part**. Choose **Response Body** for **Type**. Set a resource path in **Path**. Choose an HTTP verb for **Method**. Type an HTTP status code in **Status Code**. Then add and save the documentation part properties.

If required, repeat these steps to add or edit a documentation part to other response bodies.

### Document a **MODEL** Entity

Documenting a **MODEL** entity involves creating and managing **DocumentPart** instances for the model and each of the model's properties. For example, for the **Error** model that comes with every API by default has the following schema definition,

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Error Schema",
  "type": "object",
  "properties": {
    "message": { "type": "string" }
  }
}
```

and requires two **DocumentationPart** instances, one for the **Model** and the other for its **message** property:

```json
{
  "location": {
    "type": "MODEL",
    "name": "Error"
  },
  "properties": {
    "title": "Error Schema",
    "description": "A description of the Error model"
  }
}
```

and

```json
{
  "location": {
    "type": "MODEL",
    "name": "Error.message"
  },
  "properties": {
    "description": "An error message."
  }
}
```
When the API is exported, the DocumentationPart's properties will override the values in the original schema.

To add or edit documentation for a model, go to Models of the API in the main navigation pane. Choose the book icon for the name of a listed model to open the Documentation viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose Documentation under the API from the main navigation pane. Then choose Model for Type. Choose Edit on a listed model to change the documentation. To add documentation for an unlisted model, choose Create Documentation Part. Choose Model for Type. Give a name to the model in Name. Then add and save the documentation part properties.

If required, repeat these steps to add or edit a documentation part to other models.

**Document an AUTHORIZER Entity**

To add or edit documentation for an authorizer, go to Authorizers for the API in the main navigation pane. Choose the book icon for the listed authorizer to open the Documentation viewer and then editor. Add or modify the properties of the documentation part.

Alternatively, choose Documentation under the API from the main navigation pane. Then choose Authorizer for Type. Choose Edit on a listed authorizer to change the documentation. To add documentation for an unlisted authorizer, choose Create Documentation Part. Choose Authorizer for Type. Give a name to the authorizer in Name. Then add and save the documentation part properties.

If required, repeat these steps to add or edit a documentation part to other authorizers.

To add a documentation part for an authorizer, choose Create Documentation Part. Choose Authorizer for Type. Specify a value for the valid location field of Name for the authorizer.

Add and save the documentation content in the properties map editor.

If required, repeat these steps to add a documentation part to another authorizer.

**Publish API Documentation Using the API Gateway Console**

The following procedure describes how to publish a documentation version.

**To publish a documentation version using the API Gateway console**

1. Choose Documentation for the API from the main navigation pane in the API Gateway console.
2. Choose Publish Documentation in the Documentation pane.
3. Set up the publication:
   a. Choose an available name for Stage.
   b. Type a version identifier, e.g., 1.0.0, in Version.
   c. Optionally, provide a description about the publication in Description.
4. Choose Publish.

You can now proceed to download the published documentation by exporting the documentation to an external OpenAPI file.
Document an API Using the API Gateway REST API

In this section, we describe how to create and maintain documentation parts of an API using the API Gateway REST API.

Before creating and editing the documentation of an API, first create the API. In this section, we use the PetStore API as an example. To create an API using the API Gateway console, follow the instructions in TUTORIAL: Create a REST API by Importing an Example (p. 42).

Topics
- Document the API Entity (p. 463)
- Document a RESOURCE Entity (p. 464)
- Document a METHOD Entity (p. 467)
- Document a QUERY_PARAMETER Entity (p. 469)
- Document a PATH_PARAMETER Entity (p. 470)
- Document a REQUEST_BODY Entity (p. 471)
- Document a REQUEST_HEADER Entity (p. 472)
- Document a RESPONSE Entity (p. 473)
- Document a RESPONSE_HEADER Entity (p. 473)
- Document an AUTHORIZER Entity (p. 474)
- Document a MODEL Entity (p. 475)
- Update Documentation Parts (p. 477)
- List Documentation Parts (p. 477)

Document the API Entity

To add documentation for an API, add a DocumentationPart resource for the API entity:

```
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=sigv4_secret

{
    "location" : {
        "type" : "API"
    },
    "properties": "{"\n    "info": {
        "description" : "Your first API with Amazon API Gateway."
    }
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```
{
    ...`
```
```
    "id": "s2e5xf",
    "location": {`
        "path": null,
        "method": null,
        "name": null,
```
```
```
463
```
"statusCode": null,
"type": "API"
},
"properties": "{(\n\t"info": {\n\t\"description\": \"Your first API with Amazon API Gateway.\n\t\n\n}"
}"
}

If the documentation part has already been added, a 409 Conflict response returns, containing the error message of Documentation part already exists for the specified location: type 'API'. In this case, you must call the documentationpart:update operation.

PATCH /restapis/4wk1k4onj3/documentation/parts/part_id HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=signv4_secret
{
"patchOperations": [ {
  "op": "replace",
  "path": "/properties",
  "value": "{(\n\t"info": {\n\t\"description\": \"Your first API with Amazon API Gateway.\n\t\n\n}"
}"
} ]
}

The successful response returns a 200 OK status code with the payload containing the updated DocumentationPart instance in the payload.

**Document a RESOURCE Entity**

To add documentation for the root resource of an API, add a DocumentationPart resource targeted for the corresponding Resource resource:

POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=signv4_secret
{
  "location": {
    "type": "RESOURCE",
    "properties": "{(\n\t\"description\": \"The PetStore root resource.\n\t\n\n}"
  }
}

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

{ "_links": { "curies": { "href": "http://docs.aws.amazon.com/apigateway/latest/developerguide/restapi-documentationpart-{rel}.html",
  "name": "documentationpart",
When the resource path is not specified, the resource is assumed to be the root resource. You can add "path": "/" to properties to make the specification explicit.

To create documentation for a child resource of an API, add a DocumentationPart resource targeted for the corresponding Resource resource:

POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "location": {
    "type": "RESOURCE",
    "path": "/pets"
  },
  "properties": "\"A child resource under the root of PetStore.\"
}

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

{
  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/qcht86"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/qcht86"
    }
  }
}
"documentationpart:update": {  
  "href": "/restapis/4wk1k4onj3/documentation/parts/qcht86"
},
"id": "qcht86",
"location": {  
  "path": "/pets",
  "method": null,
  "name": null,
  "statusCode": null,
  "type": "RESOURCE"
},
"properties": "\"A child resource under the root of PetStore.\""
}

To add documentation for a child resource specified by a path parameter, add a DocumentationPart resource targeted for the Resource resource:

POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "location": {
    "type": "RESOURCE",
    "path": "/pets/{petId}"
  },
  "properties": "\"A child resource specified by the petId path parameter.\"
}

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

{
  
  "_links": {
    "curies": {
      "href": "http://docs.aws.amazon.com/apigateway/latest/developerguide/restapi-documentationpart-\{rel\}.html",
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/k6fpwb"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/k6fpwb"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/k6fpwb"
    }
  },
  "id": "k6fpwb",
  "location": {
    "path": "/pets/{petId}",
    "method": null,
    "name": null,
    "statusCode": null,
    "type": "RESOURCE"
  },
  "properties": "\"A child resource specified by the petId path parameter.\"
}
"type": "RESOURCE",
},
"properties": "{"\n\t\"description\": \"A child resource specified by the petId path parameter.\"\n\n"
}

**Note**

The DocumentationPart instance of a RESOURCE entity cannot be inherited by any of its child resources.

**Document a METHOD Entity**

To add documentation for a method of an API, add a DocumentationPart resource targeted for the corresponding Method resource:

```
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=sigv4_secret

{
  "location": {
    "type": "METHOD",
    "path": "/pets",
    "method": "GET"
  },
  "properties": "{"\n    \"summary\": \"List all pets.\"\n  }"
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```
{
  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    }
  },
  "id": "o64jbj",
  "location": {
    "path": "/pets",
    "method": "GET",
    "name": null,
    "statusCode": null,
    "type": "METHOD"
  },
  "properties": "{"\n    \"summary\": \"List all pets.\"\n  }"
}
```
If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```json
{
  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
    }
  },
  "id": "o64jbj",
  "location": {
    "path": "/pets",
    "method": "GET",
    "name": null,
    "statusCode": null,
    "type": "METHOD"
  },
  "properties": "{\n    "summary" : "List all pets."
  }"
}
```

If the location.method field is not specified in the preceding request, it is assumed to be ANY method that is represented by a wild card * character.

To update the documentation content of a METHOD entity, call the documentationpart:update operation, supplying a new properties map:

```
PATCH /restapis/4wk1k4onj3/documentation/part_id HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=sigv4_secret

{
  "patchOperations" : [ {
    "op" : "replace",
    "path" : "/properties",
    "value" : "{\n      "tags" : [ "pets" ], \n      "summary" : "List all pets."
    }"
  } ]
}
```

The successful response returns a 200 OK status code with the payload containing the updated DocumentationPart instance in the payload. For example:

```json
{
  "_links": {
    "curies": {
```
Document an API Using the API Gateway REST API

"name": "documentationpart",
"templated": true
},
"self": {
  "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
},
"documentationpart:delete": {
  "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
},
"documentationpart:update": {
  "href": "/restapis/4wk1k4onj3/documentation/parts/o64jbj"
}
},
"id": "o64jbj",
"location": {
  "path": "/pets",
  "method": "GET",
  "name": null,
  "statusCode": null,
  "type": "METHOD"
},
"properties": "{\n  \"tags\" : [ \"pets\" ], \n  \"summary\" : \"List all pets.\" \n}"
}

Document a QUERY_PARAMETER Entity

To add documentation for a request query parameter, add a DocumentationPart resource targeted for the QUERY_PARAMETER type, with the valid fields of path and name.

POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "location": {
    "type": "QUERY_PARAMETER",
    "path": "/pets",
    "method": "GET",
    "name": "page"
  },
  "properties": "{\n    \"description\" : \"Page number of results to return.\" \n}"
}

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

{
  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/h9ht5w"
    }
  }
}
The documentation part's properties map of a QUERY_PARAMETER entity can be inherited by one of its child QUERY_PARAMETER entities. For example, if you add a treats resource after /pets/{petId}, enable the GET method on /pets/{petId}/treats, and expose the page query parameter, this child query parameter inherits the DocumentationPart's properties map from the like-named query parameter of the GET /pets method, unless you explicitly add a DocumentationPart resource to the page query parameter of the GET /pets/{petId}/treats method.

## Document a PATH_PARAMETER Entity

To add documentation for a path parameter, add a DocumentationPart resource for the PATH_PARAMETER entity.

```
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=signv4_secret

{
    "location": {
        "type": "PATH_PARAMETER",
        "path": "/pets/{petId}",
        "method": "*",
        "name": "petId"
    },
    "properties": "\{"\n        \"description\": \"The id of the pet to retrieve.\"
    }"
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```
{
    "_links": {
        "curies": {
            "name": "documentationpart",
            "templated": true
        },
        "self": {
            "href": "/restapis/4wk1k4onj3/documentation/parts/ckpgog"
        }
    }
}
```
Document an API Using the API Gateway REST API

To add documentation for a request body, add a DocumentationPart resource for the request body.

```plaintext
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=signature

{
    "location": {
        "type": "REQUEST_BODY",
        "path": "/pets",
        "method": "POST"
    },
    "properties": "{\n        "description": "A Pet object to be added to PetStore."
    }"}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```plaintext
{
    "_links": {
        "curies": {
            "name": "documentationpart",
            "templated": true
        },
        "self": {
            "href": "/restapis/4wk1k4onj3/documentation/parts/kgmfr1"
        },
        "documentationpart:delete": {
            "href": "/restapis/4wk1k4onj3/documentation/parts/kgmfr1"
        },
        "documentationpart:update": {
            "href": "/restapis/4wk1k4onj3/documentation/parts/kgmfr1"
        }
    },
    "id": "kgmfr1",
    "_status": "CREATED"
}
```
**Document a REQUEST_HEADER Entity**

To add documentation for a request header, add a DocumentationPart resource for the request header.

```
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.REGION.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "location": {
    "type": "REQUEST_HEADER",
    "path": "/pets",
    "method": "GET",
    "name": "x-my-token"
  },
  "properties": "{\n    "description": "A custom token used to authorization the method invocation.\n  }"
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```
{
  ",_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/h0m3uf"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/h0m3uf"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/h0m3uf"
    },
  },
  "id": "h0m3uf",
  "location": {
    "path": "/pets",
    "method": "GET",
    "name": "x-my-token",
    "statusCode": null,
    "type": "REQUEST_HEADER"
  }
}
```
"properties": "{\n  "description": "A custom token used to authorization the method invocation.\n\n"\n}"

---

**Document a RESPONSE Entity**

To add documentation for a response of a status code, add a DocumentationPart resource targeted for the corresponding MethodResponse resource.

```json
{
  "location": {
    "path": "/",
    "method": "*",
    "name": null,
    "statusCode": "200",
    "type": "RESPONSE"
  },
  "properties": "{\n    "description": "Successful operation.\n\n\n"\n}"
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```json
{
  "_links": {
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    }
  },
  "id": "lattew",
  "location": {
    "path": "/",
    "method": "*",
    "name": null,
    "statusCode": "200",
    "type": "RESPONSE"
  },
  "properties": "{\n    "description": "Successful operation.\n\n\n"\n}"
}
```

---

**Document a RESPONSE_HEADER Entity**

To add documentation for a response header, add a DocumentationPart resource for the response header.

```json
{
  "_links": {
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lattew"
    }
  },
  "id": "lattew",
  "location": {
    "path": "/",
    "method": "*",
    "name": null,
    "statusCode": "200",
    "type": "RESPONSE"
  },
  "properties": "{\n    "description": "Successful operation.\n\n\n"\n}"
}
```
Document an API Using the API Gateway REST API

Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/ YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

"location": {
  "path": "/",
  "method": "GET",
  "name": "Content-Type",
  "statusCode": "200",
  "type": "RESPONSE_HEADER"
},
"properties": "{"\n  "description": "Media type of request"
}"}

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

{  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/fev7j7"
    },
    "documentationpart:delete": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/fev7j7"
    },
    "documentationpart:update": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/fev7j7"
    }
  },
  "id": "fev7j7",
  "location": {
    "path": "/",
    "method": "GET",
    "name": "Content-Type",
    "statusCode": "200",
    "type": "RESPONSE_HEADER"
  },
  "properties": "{"\n    "description": "Media type of request"
  }"
}

The documentation of this Content-Type response header is the default documentation for the Content-Type headers of any responses of the API.

Document an AUTHORIZER Entity

To add documentation for an API authorizer, add a DocumentationPart resource targeted for the specified authorizer.

POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/ YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret
If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```json
{
  "location": {
    "type": "AUTHORIZER",
    "name": "myAuthorizer"
  },
  "properties": "{\"description\" : \"Authorizes invocations of configured methods.\n\"\n}"
}
```

**Note**
The DocumentationPart instance of an AUTHORIZER entity cannot be inherited by any of its child resources.

### Document a MODEL Entity

Documenting a MODEL entity involves creating and managing DocumentPart instances for the model and each of the model's properties. For example, for the Error model that comes with every API by default has the following schema definition,

```json
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "title": "Error Schema",
  "type": "object",
  "properties": {
    "message": { "type": "string" }
  }
}
```
and requires two DocumentationPart instances, one for the Model and the other for its message property:

```json
{
  "location": {
    "type": "MODEL",
    "name": "Error"
  },
  "properties": {
    "title": "Error Schema",
    "description": "A description of the Error model"
  }
}
```

and

```json
{
  "location": {
    "type": "MODEL",
    "name": "Error.message"
  },
  "properties": {
    "description": "An error message."
  }
}
```

When the API is exported, the DocumentationPart's properties will override the values in the original schema.

To add documentation for an API model, add a DocumentationPart resource targeted for the specified model.

```bash
POST /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTTTTTTZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "location": {
    "type": "MODEL",
    "name": "Pet"
  },
  "properties": "{\n    "description": "Data structure of a Pet object.\"\n  }"
}
```

If successful, the operation returns a 201 Created response containing the newly created DocumentationPart instance in the payload. For example:

```json
{
  "_links": {
    "curies": {
      "name": "documentationpart",
      "templated": true
    },
    "self": {
      "href": "/restapis/4wk1k4onj3/documentation/parts/lkn4uq"
    }
  }
```
Repeat the same step to create a DocumentationPart instance for any of the model's properties.

**Note**

The DocumentationPart instance of a MODEL entity cannot be inherited by any of its child resources.

## Update Documentation Parts

To update the documentation parts of any type of API entities, submit a PATCH request on a DocumentationPart instance of a specified part identifier to replace the existing properties map with a new one.

```plaintext
PATCH /restapis/4wk1k4onj3/documentation/parts/part_id HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=signv4_secret

{
  "patchOperations": [
    {
      "op": "replace",
      "path": "RESOURCE_PATH",
      "value": "NEW_properties_VALUE_AS_JSON_STRING"
    }
  ]
}
```

The successful response returns a 200 OK status code with the payload containing the updated DocumentationPart instance in the payload.

You can update multiple documentation parts in a single PATCH request.

## List Documentation Parts

To list the documentation parts of any type of API entities, submit a GET request on a DocumentationParts collection.

```plaintext
GET /restapis/restapi_id/documentation/parts HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
```
Publish API Documentation Using the API Gateway REST API

To publish the documentation for an API, create, update, or get a documentation snapshot, and then associate the documentation snapshot with an API stage. When creating a documentation snapshot, you can also associate it with an API stage at the same time.

Topics
- Create a Documentation Snapshot and Associate it with an API Stage (p. 478)
- Create a Documentation Snapshot (p. 478)
- Update a Documentation Snapshot (p. 479)
- Get a Documentation Snapshot (p. 479)
- Associate a Documentation Snapshot with an API Stage (p. 479)
- Download a Documentation Snapshot Associated with a Stage (p. 480)

Create a Documentation Snapshot and Associate it with an API Stage

To create a snapshot of an API's documentation parts and associate it with an API stage at the same time, submit the following POST request:

```
POST /restapis/restapi_id/documentation/versions HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
  "documentationVersion": "1.0.0",
  "stageName": "prod",
  "description": "My API Documentation v1.0.0"
}
```

If successful, the operation returns a 200 OK response, containing the newly created DocumentationVersion instance as the payload.

Alternatively, you can create a documentation snapshot without associating it with an API stage first and then call restapi:update to associate the snapshot with a specified API stage. You can also update or query an existing documentation snapshot and then update its stage association. We show the steps in the next four sections.

Create a Documentation Snapshot

To create a snapshot of an API's documentation parts, create a new DocumentationVersion resource and add it to the DocumentationVersions collection of the API:
POST /restapis/restapi_id/documentation/versions HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
   "documentationVersion": "1.0.0",
   "description": "My API Documentation v1.0.0"
}

If successful, the operation returns a 200 OK response, containing the newly created DocumentationVersion instance as the payload.

Update a Documentation Snapshot

You can only update a documentation snapshot by modifying the description property of the corresponding DocumentationVersion resource. The following example shows how to update the description of the documentation snapshot as identified by its version identifier, version, e.g., 1.0.0.

PATCH /restapis/restapi_id/documentation/versions/version HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
   "patchOperations": [{
      "op": "replace",
      "path": "/description",
      "value": "My API for testing purposes."
   }]
}

If successful, the operation returns a 200 OK response, containing the updated DocumentationVersion instance as the payload.

Get a Documentation Snapshot

To get a documentation snapshot, submit a GET request against the specified DocumentationVersion resource. The following example shows how to get a documentation snapshot of a given version identifier, 1.0.0.

GET /restapis/<restapi_id>/documentation/versions/1.0.0 HTTP/1.1
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

Associate a Documentation Snapshot with an API Stage

To publish the API documentation, associate a documentation snapshot with an API stage. You must have already created an API stage before associating the documentation version with the stage.
To associate a documentation snapshot with an API stage using the API Gateway REST API, call the `stage:update` operation to set the desired documentation version on the `stage.documentationVersion` property:

```
PATCH /restapis/RESTAPI_ID/stages/STAGE_NAME
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDThhmmssZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{  
  "patchOperations": [{
    "op": "replace",
    "path": "/documentationVersion",
    "value": "VERSION_IDENTIFIER"
  }
}
```

**Download a Documentation Snapshot Associated with a Stage**

After a version of the documentation parts is associated with a stage, you can export the documentation parts together with the API entity definitions, to an external file, using the API Gateway console, the API Gateway REST API, one of its SDKs, or the AWS CLI for API Gateway. The process is the same as for exporting the API. The exported file format can be JSON or YAML.

Using the API Gateway REST API, you can also explicitly set the `extensions=documentation,integrations,authorizers` query parameter to include the API documentation parts, API integrations and authorizers in an API export. By default, documentation parts are included, but integrations and authorizers are excluded, when you export an API. The default output from an API export is suited for distribution of the documentation.

To export the API documentation in an external JSON OpenAPI file using the API Gateway REST API, submit the following `GET` request:

```
GET /restapis/restapi_id/stages/stage_name/exports/swagger?extensions=documentation HTTP/1.1
Accept: application/json
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDThhmmssZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret
```

Here, the `x-amazon-apigateway-documentation` object contains the documentation parts and the API entity definitions contains the documentation properties supported by OpenAPI. The output does not include details of integration or Lambda authorizers (formerly known as custom authorizers). To include both details, set `extensions=integrations,authorizers,documentation`. To include details of integrations but not of authorizers, set `extensions=integrations,documentation`. To include details of authorizers but not of integrations, set `extensions=authorizers,documentation`.

You must set the `Accept:application/json` header in the request to output the result in a JSON file. To produce the YAML output, change the request header to `Accept:application/yaml`.

As an example, we will look at an API that exposes a simple `GET` method on the root resource (`/`). This API has four API entities defined in an OpenAPI definition file, one for each of the API, MODEL, METHOD, and RESPONSE types. A documentation part has been added to each of the API, METHOD, and RESPONSE entities. Calling the preceding documentation-exporting command, we get the following output, with
the documentation parts listed within the x-amazon-apigateway-documentation object as an extension to a standard OpenAPI file.

OpenAPI 3.0

```json
{
  "openapi": "3.0.0",
  "info": {
    "description": "API info description",
    "title": "doc",
    "x-bar": "API info x-bar"
  },
  "paths": {
    "": {
      "get": {
        "description": "Method description.",
        "responses": {
          "200": {
            "description": "200 response",
            "content": {
              "application/json": {
                "schema": {
                  "$ref": "#/components/schemas/Empty"
                }
              }
            }
          }
        },
        "x-example": "x- Method example"
      },
      "x-bar": "resource x-bar"
    }
  },
  "x-amazon-apigateway-documentation": {
    "version": "1.0.0",
    "createdDate": "2016-11-22T22:41:40Z",
    "documentationParts": [
      {
        "location": {
          "type": "API"
        },
        "properties": {
          "description": "API description",
          "foo": "API foo",
          "x-bar": "API x-bar",
          "info": {
            "description": "API info description",
            "version": "API info version",
            "foo": "API info foo",
            "x-bar": "API info x-bar"
          }
        }
      },
      {
        "location": {
          "type": "METHOD",
          "method": "GET"
        },
        "properties": {
          "description": "Method description.",
          "x-example": "x- Method example",
          "foo": "Method foo",
          "info": {
            "version": "method info version",
            "method": "GET"
          }
        }
      }
    ]
  }
}
```
"description": "method info description",
"foo": "method info foo"
}
}
",
"location": {
"type": "RESOURCE"
},
"properties": {
"description": "resource description",
"foo": "resource foo",
"x-bar": "resource x-bar",
"info": {
"description": "resource info description",
"version": "resource info version",
"foo": "resource info foo",
"x-bar": "resource info x-bar"
}
}
]
},
"x-bar": "API x-bar",
"servers": [
{
"url": "https://rznaap68yi.execute-api.ap-southeast-1.amazonaws.com/{basePath}
{basePath}
"
"variables": {
"basePath": {
"default": "/test"
}
}
}
],
"components": {
"schemas": {
"Empty": {
"type": "object",
"title": "Empty Schema"
}
}
}
}

OpenAPI 2.0

{
"swagger": "2.0",
"info": {
"description": "API info description",
"title": "doc",
"x-bar": "API info x-bar"
},
"host": "rznaap68yi.execute-api.ap-southeast-1.amazonaws.com",
"basePath": "/test",
"schemes": [ "https" ],
"paths": {
"": {
"get": {
"description": "Method description.",
"produces": [ "application/json" ],
"responses": {
"200": {

"description" : "200 response",
"schema" : {
"$ref" : "#/definitions/Empty"
}
},
"x-example" : "x- Method example"
},
"x-bar" : "resource x-bar"
}
},
"definitions" : {
"Empty" : {
"type" : "object",
"title" : "Empty Schema"
}
},
"x-amazon-apigateway-documentation" : {
"version" : "1.0.0",
"createdDate" : "2016-11-22T22:41:40Z",
"documentationParts" : [ {
"location" : {
"type" : "API"
},
"properties" : {
"description" : "API description",
"foo" : "API foo",
"x-bar" : "API x-bar",
"info" : {
"description" : "API info description",
"version" : "API info version",
"foo" : "API info foo",
"x-bar" : "API info x-bar"
}
},
"location" : {
"type" : "METHOD",
"method" : "GET"
},
"properties" : {
"description" : "Method description.",
"x-example" : "x- Method example",
"foo" : "Method foo",
"info" : {
"version" : "method info version",
"description" : "method info description",
"foo" : "method info foo"
}
}
},
"location" : {
"type" : "RESOURCE"
},
"properties" : {
"description" : "resource description",
"foo" : "resource foo",
"x-bar" : "resource x-bar",
"info" : {
"description" : "resource info description",
"version" : "resource info version",
"foo" : "resource info foo",
"x-bar" : "resource info x-bar"
}
}
} ]
For an OpenAPI-compliant attribute defined in the `properties` map of a documentation part, API Gateway inserts the attribute into the associated API entity definition. An attribute of `x-something` is a standard OpenAPI extension. This extension gets propagated into the API entity definition. For example, see the `x-example` attribute for the `GET` method. An attribute like `foo` is not part of the OpenAPI specification and is not injected into its associated API entity definitions.

If a documentation-rendering tool (e.g., OpenAPI UI) parses the API entity definitions to extract documentation attributes, any non OpenAPI-compliant `properties` attributes of a `DocumentationPart` instance are not available for the tool. However, if a documentation-rendering tool parses the `x-amazon-apigateway-documentation` object to get content, or if the tool calls `restapi:documentation-parts` and `documentationpart:by-id` to retrieve documentation parts from API Gateway, all the documentation attributes are available for the tool to display.

To export the documentation with API entity definitions containing integration details to a JSON OpenAPI file, submit the following `GET` request:

```
GET /restapis/restapi_id/stages/stage_name/exports/swagger?
extensions=integrations,documentation HTTP/1.1
Accept: application/json
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=signature
```

To export the documentation with API entity definitions containing details of integrations and authorizers to a YAML OpenAPI file, submit the following `GET` request:

```
GET /restapis/restapi_id/stages/stage_name/exports/swagger?
extensions=integrations,authorizers,documentation HTTP/1.1
Accept: application/yaml
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date,
Signature=signature
```

To use the API Gateway console to export and download the published documentation of an API, follow the instructions in Export REST API Using the API Gateway Console (p. 665).

### Import API Documentation

As with importing API entity definitions, you can import documentation parts from an external OpenAPI file into an API in API Gateway. You specify the to-be-imported documentation parts within the `x-amazon-apigateway-documentation` Object (p. 582) extension in a valid OpenAPI definition file. Importing documentation does not alter the existing API entity definitions.

You have an option to merge the newly specified documentation parts into existing documentation parts in API Gateway or to overwrite the existing documentation parts. In the `MERGE` mode, a new documentation part defined in the OpenAPI file is added to the `DocumentationParts` collection of the API. If an imported `DocumentationPart` already exists, an imported attribute replaces the existing one.
if the two are different. Other existing documentation attributes remain unaffected. In the `OVERWRITE` mode, the entire `DocumentationParts` collection is replaced according to the imported OpenAPI definition file.

**Importing Documentation Parts Using the API Gateway REST API**

To import API documentation using the API Gateway REST API, call the `documentationpart:import` operation. The following example shows how to overwrite existing documentation parts of an API with a single `GET` / method, returning a `200 OK` response when successful.

**OpenAPI 3.0**

```json
PUT /restapis/<restapi_id>/documentation/parts&mode=overwrite&failonwarnings=true
Host: apigateway.region.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=signature

{
  "openapi": "3.0.0",
  "info": {
    "description": "description",
    "version": "1",
    "title": "doc"
  },
  "paths": {
    ": "/",
    "get": {
      "description": "Method description.",
      "responses": {
        "200": {
          "description": "200 response",
          "content": {
            "application/json": {
              "schema": {
                "$ref": "#/components/schemas/Empty"
              }
            }
          }
        }
      }
    }
  }
}
```

```
"x-amazon-apigateway-documentation": {
  "version": "1.0.3",
  "documentationParts": [
    {
      "location": {
        "type": "API"
      },
      "properties": {
        "description": "API description",
        "info": {
          "description": "API info description 4",
          "version": "API info version 3"
        }
      }
    }
  ]
}
```

485
OpenAPI 2.0

```
PUT /restapis/<restapi_id>/documentation/parts&mode=overwrite&failonwarnings=true
Host: apigateway.<region>.amazonaws.com
Content-Type: application/json
X-Amz-Date: YYYYMMDDTttttttZ
Authorization: AWS4-HMAC-SHA256 Credential=access_key_id/YYYYMMDD/region/apigateway/aws4_request, SignedHeaders=content-length;content-type;host;x-amz-date, Signature=sigv4_secret

{
    "swagger": "2.0",
    "info": {
        "description": "description",
        "version": "1",
        "title": "doc"
    },
    "host": "",
    "basePath": "/",
    "schemes": [
        "https"
    ],
    "servers": [
        {
            "url": "/",
        },
        {
            "url": "http://localhost:8080",
        }
    ],
    "components": {
        "schemas": {
            "Empty": {
                "type": "object",
                "title": "Empty Schema"
            }
        }
    },
    "paths": {
        "": {
            "get": {
                "operationId": "list",
                "description": "List API operations",
                "tags": [
                    "API Operations"
                ],
                "parameters": [
                    {
                        "in": "path",
                        "name": "restapi_id",
                        "description": "The ID of the API to list operations for",
                        "required": true,
                        "schema": {
                            "type": "string"
                        }
                    }
                ],
                "responses": {
                    "200": {
                        "description": "List of API operations",
                        "schema": {
                            "$ref": "#/components/schemas/Empty"
                        }
                    }
                }
            }
        }
    }
}
```
"paths": {
  "/": {
    "get": {
      "description": "Method description.",
      "produces": [
        "application/json"
      ],
      "responses": {
        "200": {
          "description": "200 response",
          "schema": {
            "$ref": "#/definitions/Empty"
          }
        }
      }
    }
  }
},
"definitions": {
  "Empty": {
    "type": "object",
    "title": "Empty Schema"
  }
},
"x-amazon-apigateway-documentation": {
  "version": "1.0.3",
  "documentationParts": [
    {
      "location": {
        "type": "API"
      },
      "properties": {
        "description": "API description",
        "info": {
          "description": "API info description 4",
          "version": "API info version 3"
        }
      }
    },
    {
      "location": {
        "type": "METHOD",
        "method": "GET"
      },
      "properties": {
        "description": "Method description."
      }
    },
    {
      "location": {
        "type": "MODEL",
        "name": "Empty"
      },
      "properties": {
        "title": "Empty Schema"
      }
    },
    {
      "location": {
        "type": "RESPONSE",
        "method": "GET",
        "statusCode": "200"
      },
      "properties": {
        "description": "200 response"
      }
    }
  ]
}
When successful, this request returns a 200 OK response containing the imported DocumentationPartId in the payload.

```
{
  "ids": [
    "kg3mth",
    "796rtf",
    "zhek4p",
    "5ukm9s"
  ]
}
```

In addition, you can also call restapi:import or restapi:put, supplying the documentation parts in the x-amazon-apigateway-documentation object as part of the input OpenAPI file of the API definition. To exclude the documentation parts from the API import, set ignore=documentation in the request query parameters.

**Importing Documentation Parts Using the API Gateway Console**

The following instructions describe how to import documentation parts.

**To use the console to import documentation parts of an API from an external file**

1. Choose **Documentation** for the API from the main navigation pane on the console.
2. Choose **Import Documentation** in the **Documentation** pane.
3. Choose **Select OpenAPI File** to load a file from a drive, or copy and paste a file contents into the file view. For an example, see the payload of the example request in Importing Documentation Parts Using the API Gateway REST API (p. 485).
4. Optionally, choose **Fail on warnings** or **Ignore warnings**, and choose **Merge** or **Overwrite** from **Import mode**.
5. Choose **Import**.

**Control Access to API Documentation**

If you have a dedicated documentation team to write and edit your API documentation, you can configure separate access permissions for your developers (for API development) and for your writers or editors (for content development). This is especially appropriate when a third-party vendor is involved in creating the documentation for you.

To grant your documentation team the access to create, update, and publish your API documentation, you can assign the documentation team an IAM role with the following IAM policy, where `account_id` is the AWS account ID of your documentation team.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StmtDocPartsAddEditViewDelete",
      "Effect": "Allow",
      "Action": [
        "apigateway:ImportDocumentation",
        "apigateway:PutDocumentation",
        "apigateway:UpdateDocumentation",
        "apigateway:GetDocumentation",
        "apigateway:DeleteDocumentation"
      ],
    }
  ]
}
```
"Effect": "Allow",
"Action": [
  "apigateway:GET",
  "apigateway:PUT",
  "apigateway:POST",
  "apigateway:PATCH",
  "apigateway:DELETE"
],
"Resource": [
  "arn:aws:apigateway::account_id:/restapis/*/documentation/*"
]
}
}

For information on setting permissions to access API Gateway resources, see Control Who Can Create and Manage an API Gateway API with IAM Policies (p. 364).

Update and Maintain a REST API in Amazon API Gateway

Maintaining an API amounts to viewing, updating and deleting the existing API setups. You can maintain an API using the API Gateway console, AWS CLI, an SDK or the API Gateway REST API. Updating an API involves modifying certain resource properties or configuration settings of the API. Resource updates require redeploying the API, whereas configuration updates do not.

API resources that can be updated are detailed in the following table.

**API resource updates requiring redeployment of the API**

<table>
<thead>
<tr>
<th>Resource</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiKey</td>
<td>For applicable properties and supported operations, see apikey:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>Authorizer</td>
<td>For applicable properties and supported operations, see authorizer:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>DocumentationPart</td>
<td>For applicable properties and supported operations, see documentationpart:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>DocumentationVersion</td>
<td>For applicable properties and supported operations, see documentationversion:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>GatewayResponse</td>
<td>For applicable properties and supported operations, see gatewayresponse:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>Integration</td>
<td>For applicable properties and supported operations, see integration:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>IntegrationResponse</td>
<td>For applicable properties and supported operations, see integrationresponse:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>Method</td>
<td>For applicable properties and supported operations, see method:update. The update requires redeploying the API.</td>
</tr>
<tr>
<td>MethodResponse</td>
<td>For applicable properties and supported operations, see methodresponse:update. The update requires redeploying the API.</td>
</tr>
</tbody>
</table>
API configurations that can be updated are detailed in the following table.

### API configuration updates without requiring redeployment of the API

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account</td>
<td>For applicable properties and supported operations, see account:update. The update does not require redeploying the API.</td>
</tr>
<tr>
<td>Deployment</td>
<td>For applicable properties and supported operations, see deployment:update.</td>
</tr>
<tr>
<td>DomainName</td>
<td>For applicable properties and supported operations, see domainname:update. The update does not require redeploying the API.</td>
</tr>
<tr>
<td>BasePathMapping</td>
<td>For applicable properties and supported operations, see basepathmapping:update. The update does not require redeploying the API.</td>
</tr>
<tr>
<td>Stage</td>
<td>For applicable properties and supported operations, see stage:update. The update does not require redeploying the API.</td>
</tr>
<tr>
<td>Usage</td>
<td>For applicable properties and supported operations, see usage:update. The update does not require redeploying the API.</td>
</tr>
<tr>
<td>UsagePlan</td>
<td>For applicable properties and supported operations, see usageplan:update. The update does not require redeploying the API.</td>
</tr>
</tbody>
</table>

### Change a Public or Private API Endpoint Type in API Gateway

Changing an API endpoint type requires you to update the API's configuration. You can change an existing API type using the API Gateway console, the AWS CLI, or an AWS SDK for API Gateway. The update operation may take up to 60 seconds to complete. During this time, your API will be available, but its endpoint type cannot be changed again until the current change is completed.
The following endpoint type changes are supported:

- From edge-optimized to regional or private
- From regional to edge-optimized or private
- From private to regional

You cannot change a private API into an edge-optimized API.

If you are changing a public API from edge-optimized to regional or vice versa, note that an edge-optimized API may have different behaviors than a regional API. For example, an edge-optimized API removes the `Content-MD5` header. Any MD5 hash value passed to the backend can be expressed in a request string parameter or a body property. However, the regional API passes this header through, although it may remap the header name to some other name. Understanding the differences helps you decide how to update an edge-optimized API to a regional one or from a regional API to an edge-optimized one.

**Topics**

- Use the API Gateway Console to Change an API Endpoint Type (p. 491)
- Use the AWS CLI to Change an API Endpoint Type (p. 491)

**Use the API Gateway Console to Change an API Endpoint Type**

To change the API endpoint type of your API, perform one of the following sets of steps:

**To convert a public endpoint from regional or edge-optimized and vice versa**

1. Sign in to the API Gateway console and choose **APIs** in the primary navigation pane.
2. Choose the settings (gear icon) of an API under **+ Create API**.
3. Change the **Endpoint Type** option under **Endpoint Configuration** from Edge Optimized to Regional or from Regional to Edge Optimized.
4. Choose **Save** to start the update.

**To convert a private endpoint to a regional endpoint**

1. Sign in to the API Gateway console and choose **APIs** in the primary navigation pane.
2. Choose the settings (gear icon) of an API under **+ Create API**.
3. Edit the resource policy for your API to remove any mention of VPCs or VPC endpoints so that API calls from outside your VPC as well as inside your VPC will succeed.
4. Change the **Endpoint Type** to Regional.
5. Choose **Save** to start the update.
6. Remove the resource policy from your API.
7. Redeploy your API so that the changes will take effect.

**Use the AWS CLI to Change an API Endpoint Type**

To use the AWS CLI to update an edge-optimized API whose API ID is `{api-id}`, call `update-rest-api` as follows:

```bash
aws apigateway update-rest-api \
  --rest-api-id {api-id} \
  --patch-operations op=replace,path=/endpointConfiguration/types/EDGE,value=REGIONAL
```
The successful response has a status code of 200 OK and a payload similar to the following:

```json
{
   "createdDate": "2017-10-16T04:09:31Z",
   "description": "Your first API with Amazon API Gateway. This is a sample API that integrates via HTTP with our demo Pet Store endpoints",
   "endpointConfiguration": {
      "types": "REGIONAL"
   },
   "id": "0gsnjtjck8",
   "name": "PetStore imported as edge-optimized"
}
```

Conversely, update a regional API to an edge-optimized API as follows:

```bash
aws apigateway update-rest-api \
   --rest-api-id {api-id} \
   --patch-operations op=replace,path=/endpointConfiguration/types(REGIONAL),value=EDGE
```

Because `put-rest-api` is for updating API definitions, it is not applicable to updating an API endpoint type.

**Maintain an API Using the API Gateway Console**

**Topics**

- View a List of APIs in API Gateway (p. 492)
- Delete an API in API Gateway (p. 492)
- Delete a Resource in API Gateway (p. 493)
- View a Methods List in API Gateway (p. 493)
- Delete a Method in API Gateway (p. 493)

**View a List of APIs in API Gateway**

Use the API Gateway console to view a list of APIs.

**View a List of APIs with the API Gateway Console**

You must have an API available in API Gateway. Follow the instructions in Creating a REST API in Amazon API Gateway (p. 177).

2. The list of APIs is displayed.

**Delete an API in API Gateway**

Use the API Gateway console to delete an API.

**Warning**

Deleting an API means that you can no longer call it. This action cannot be undone.

**Delete an API with the API Gateway Console**

You must have deployed the API at least once. Follow the instructions in Deploying a REST API in Amazon API Gateway (p. 494).
2. In the box that contains the name of the API you want to delete, choose Resources.
3. Choose Delete API.
4. When prompted to delete the API, choose Ok.

Delete a Resource in API Gateway

Use the API Gateway console to delete a resource.

Warning
When you delete a resource, you also delete its child resources and methods. Deleting a resource may cause part of the corresponding API to be unusable. Deleting a resource cannot be undone.

Delete a Resource with the API Gateway Console

2. In the box that contains the name of the API for the resource you want to delete, choose Resources.
3. In the Resources pane, choose the resource, and then choose Delete Resource.
4. When prompted, choose Delete.

View a Methods List in API Gateway

Use the API Gateway console to view a list of methods for a resource.

View a Methods List with the API Gateway Console

You must have methods available in API Gateway. Follow the instructions in TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).

2. In the box that contains the name of the API, choose Resources.
3. The list of methods is displayed in the Resources pane.

Tip
You may need to choose the arrow next to one or more resources to display all of the available methods.

Delete a Method in API Gateway

Use the API Gateway console to delete a method.

Warning
Deleting a method may cause part of the corresponding API to become unusable. Deleting a method cannot be undone.

Delete a Method with the API Gateway Console

2. In the box that contains the name of the API for the method, choose Resources.
3. In the Resources pane, choose the arrow next to the resource for the method.
4. Choose the method, and then choose Delete Method.
5. When prompted, choose Delete.
Deploying a REST API in Amazon API Gateway

After creating your API, you must deploy it to make it callable by your users.

To deploy an API, you create an API deployment and associate it with a stage. Each stage is a snapshot of the API and is made available for client apps to call.

**Important**
Every time you update an API, which includes modification of routes, methods, integrations, authorizers, and anything else other than stage settings, you must redeploy the API to an existing stage or to a new stage.

As your API evolves, you can continue to deploy it to different stages as different versions of the API. You can also deploy your API updates as a canary release deployment (p. 666), enabling your API clients to access, on the same stage, the production version through the production release, and the updated version through the canary release.

To call a deployed API, the client submits a request against an API's URL. The URL is determined by an API's protocol (HTTP(S) or (WSS)), hostname, stage name, and (for REST APIs) resource path. The host name and the stage name determine the API's base URL.

Using the API's default domain name, the base URL of (for example) a REST API in a given stage (\{stageName\}) is in the following format:

```
https://\{restapi-id\}.execute-api.\{region\}.amazonaws.com/\{stageName\}
```

To make the API's default base URL more user-friendly, you can create a custom domain name (e.g., api.example.com) to replace the default host name of the API. To support multiple APIs under the custom domain name, you must map an API stage to a base path.

With a custom domain name of {api.example.com} and the API stage mapped to a base path of \{basePath\} under the custom domain name, the base URL of a REST API becomes the following:

```
https://{api.example.com}/\{basePath\}
```

For each stage, you can optimize API performance by adjusting the default account-level request throttling limits and enabling API caching. You can also enable logging API calls to CloudTrail or CloudWatch and select a client certificate for the backend to authenticate the API requests. In addition, you can override stage-level settings for individual methods and define stage variables to pass stage-specific environment contexts to the API integration at run time.

Stages enable robust version control of your API. For example, you can deploy an API to a test stage and a prod stage, and use the test stage as a test build and use the prod stage as a stable build. After the updates pass the test, you can promote the test stage to the prod stage. The promotion can be done by redeploying the API to the prod stage or updating a stage variable (p. 496) value from the stage name of test to that of prod.

In this section, we discuss how to deploy an API, using the API Gateway console or calling the API Gateway REST API. To use other tools to do the same, see the documentation of, for example, AWS CLI or an AWS SDK.

Topics
- Deploy a REST API in API Gateway (p. 495)
- Set up a Stage in API Gateway (p. 497)
- Generate an SDK for a REST API in API Gateway (p. 521)
Deploy a REST API in API Gateway

In API Gateway, a REST API deployment is represented by a Deployment resource. It is like an executable of an API represented by a RestApi resource. For the client to call your API, you must create a deployment and associate a stage with it. A stage is represented by a Stage resource and represents a snapshot of the API, including methods, integrations, models, mapping templates, Lambda authorizers (formerly known as custom authorizers), etc. When you update the API, you can redeploy the API by associating a new stage with the existing deployment. We discuss creating a stage in the section called “Set up a Stage” (p. 497).

Topics
• Create a Deployment Using AWS CLI (p. 495)
• Deploy a REST API from the API Gateway Console (p. 495)

Create a Deployment Using AWS CLI

Creating a deployment amounts to instantiating the Deployment resource. You can use the API Gateway console, AWS CLI, an AWS SDK or the API Gateway REST API to create an deployment.

To use CLI to create a deployment, use the create-deployment command:

```
aws apigateway create-deployment --rest-api-id <rest-api-id> --region <region>
```

The API is not callable until you associate this deployment with a stage. With an existing stage, you can do so by updating the stage’s deploymentId property with the newly created deployment ID (<deployment-id>).

```
aws apigateway update-stage --region <region> \
--rest-api-id <rest-api-id> \
--stage-name <stage-name> \
--patch-operations op='replace',path='/deploymentId',value='<deployment-id>'
```

When deploying an API the first time, you can combine the stage creation and deployment creation at the same time:

```
aws apigateway create-deployment --region <region> \
--rest-api-id <rest-api-id> \
--stage-name <stage-name>
```

This is what is done behind the scenes in the API Gateway console, when you deploy an API the first time or when you redeploy the API to a new stage.

Deploy a REST API from the API Gateway Console

You must have created a REST API before deploying it for the first time. For more information see Creating a REST API in Amazon API Gateway (p. 177).

Topics
• Deploy a REST API to a Stage (p. 496)
• Redeploy a REST API to a Stage (p. 496)
• Update the Stage Configuration of a REST API Deployment (p. 496)
• Set Stage Variables for a REST API Deployment (p. 496)
• Associate a Stage with a Different REST API Deployment (p. 496)
Deploy a REST API to a Stage

The API Gateway console lets you deploy an API by creating a deployment and associating it with a new or existing stage.

**Note**

To associate a stage in API Gateway with a different deployment, see Associate a Stage with a Different REST API Deployment (p. 496) instead.

2. In the **APIs** navigation pane, choose the API you want to deploy.
3. In the **Resources** navigation pane, choose **Actions**.
4. From the **Actions** drop-down menu, choose **Deploy API**.
5. In the **Deploy API** dialog, choose an entry from the **Deployment stage** dropdown list.
6. If you choose **[New Stage]**, type a name in **Stage name** and optionally provide a description for the stage and deployment in **Stage description** and **Deployment description**. If you choose an existing stage, you may want to provide a description of the new deployment in **Deployment description**.
7. Choose **Deploy** to deploy the API to the specified stage with default stage settings.

Redeploy a REST API to a Stage

To redeploy an API, perform the same steps as in the section called “Deploy a REST API to a Stage” (p. 496). You can reuse the same stage as many times as desired.

Update the Stage Configuration of a REST API Deployment

After an API is deployed, you can modify the stage settings to enable or disable API cache, logging, or request throttling. You can also choose a client certificate for the backend to authenticate API Gateway and set stage variables to pass deployment context to the API integration at run time. For more information, see Update Stage Settings (p. 498).

**Important**

After modifying stage settings, you must redeploy the API for the changes to take effect.

**Note**

If the updated settings, such as enabling logging, requires a new IAM role, you can add the required IAM role without redeploying the API. However, it can take a few minutes before the new IAM role takes effect. Before that happens, traces of your API calls will not be logged even if you have enabled the logging option.

Set Stage Variables for a REST API Deployment

For a deployment, you can set or modify stage variables to pass deployment-specific data to the API integration at run time. You can do this on the **Stage Variables** tab in the **Stage Editor**. For more information, see instructions in Set up Stage Variables for a REST API Deployment (p. 514).

Associate a Stage with a Different REST API Deployment

Because a deployment represents an API snapshot and a stage defines a path into a snapshot, you can choose different deployment-stage combinations to control how users call into different versions of the API. This is useful, for example, when you want to roll back API state to a previous deployment or to merge a ‘private branch’ of the API into the public one.

The following procedure shows how to do this using the **Stage Editor** in the API Gateway console. It is assumed that you must have deployed an API more than once.

1. If not already in **Stage Editor**, choose the stage you want to update the deployment from an API's **Stages** option in the **APIs** main navigation pane.
2. On the **Deployment History** tab, choose the option button next to the deployment you want the stage to use.
3. Choose **Change Deployment**.

## Set up a Stage in API Gateway

A stage is a named reference to a deployment, which is a snapshot of the API. You use a **Stage** to manage and optimize a particular deployment. For example, you can set up stage settings to enable caching, customize request throttling, configure logging, define stage variables or attach a canary release for testing.

**Topics**
- Set up a Stage Using the API Gateway Console (p. 497)
- Enable API Caching to Enhance Responsiveness (p. 500)
- Throttle API Requests for Better Throughput (p. 505)
- Set Up Client-Side SSL Authentication in API Gateway (p. 508)
- Set Up AWS WAF in API Gateway (p. 508)
- Set Up Tags for an API Stage in API Gateway (p. 508)
- Set Up CloudWatch API Logging in API Gateway (p. 510)
- Set Up X-Ray Tracing in API Gateway (p. 513)
- Set Up CloudTrail Logging in API Gateway (p. 513)
- Set up Stage Variables for a REST API Deployment (p. 514)

## Set up a Stage Using the API Gateway Console

**Topics**
- Create a New Stage (p. 497)
- Update Stage Settings (p. 498)
- Delete a Stage for an API (p. 500)

### Create a New Stage

After the initial deployment, you can add more stages and associate them with existing deployments. You can use the API Gateway console to create and use a new stage or choose an existing stage while deploying an API. In general, you can add a new stage to an API deployment before redeploying the API. To do so using the API Gateway console, follow the instructions below.

2. From the **APIs** navigation pane, choose **Stages** under an API.
3. From the **Stages** navigation pane, choose **Create**.
4. Under **Create Stage**, type a stage name, for example, *prod*, for **Stage name**.
   
   **Note**
   Stage names can only contain alphanumeric characters, hyphens, and underscores. Maximum length is 128 characters.
5. Optionally, type a stage description for **Stage description**.
6. From the **Deployment** drop-down list, choose the date and time of the existing API deployment you want to associate with this stage.
7. Choose **Create**.
Update Stage Settings

After a successful deployment of an API, the stage is populated with default settings. You can use the console or API Gateway REST API to change the stage settings, including API caching and logging. In the following, we show how to do so using the Stage Editor of the API Gateway console.

Update Stage Settings Using the API Gateway Console

These steps assume that you have already deployed the API to a stage.

2. In the APIs pane, choose the API, and then choose Stages.
3. In the Stages pane, choose the name of the stage.
4. In the Stage Editor pane, choose the Settings tab.
5. To enable API caching for the stage, select the Enable API cache option under the Cache Settings section. Then choose desired options and associated values for Cache capacity, Encrypt cache data, Cache time-to-live (TTL), as well as any requirements for per-key cache invalidation.

For more information about stage-level cache settings, see Enable API Caching (p. 500).

Important
If you enable API caching for an API stage, your AWS account may be charged for API caching. Caching is not eligible for the AWS free tier.

Tip
You can also override enabled stage-level cache settings for individual methods. To do so, expand the stage under the Stages secondary navigation pane and choose a method. Then, in the stage editor, choose the Override for this method option for Settings. In the Cache Settings area, you can set or clear Enable Method Cache or customize any other desired options. For more information about the method-level cache settings, see Enable API Caching (p. 500).

6. To enable Amazon CloudWatch Logs for all of the methods associated with this stage of this API Gateway API, do the following:
   a. Under the CloudWatch Settings section, select the Enable CloudWatch Logs option.
      
      Tip
      To enable method-level CloudWatch settings, expand the stage under the Stages secondary navigation pane, choose each method of interest, and, back in the stage editor, choose Override for this method for Settings. In the CloudWatch Settings area, make sure to select Log to CloudWatch Logs and any other desired options, before choosing Save Changes.
      
      Important
      Your account will be charged for accessing method-level CloudWatch metrics, but not the API- or stage-level metrics.
   
   b. For Log level, choose ERROR to write only error-level entries to CloudWatch Logs, or choose INFO to include all ERROR events as well as extra informational events.
   
   c. To log full API call request and response information, select Log full requests/responses data.
      No sensitive data will be logged unless the Log full requests/responses data option is selected.
      
      Important
      Setting logs to ERROR and then choosing Log full requests/responses data results in every request being logged in detail. This is the intended behavior.
   
   d. To have API Gateway report to CloudWatch the API metrics of API calls, Latency, Integration latency, 400 errors and 500 errors, choose Enable Detailed CloudWatch Metrics option. For more information about CloudWatch, see the Amazon CloudWatch User Guide.

498
e. Choose **Save Changes**. The new settings will take effect after a new deployment.

**Important**
To enable CloudWatch Logs for all or only some of the methods, you must also specify the ARN of an IAM role that enables API Gateway to write information to CloudWatch Logs on behalf of your IAM user. To do so, choose **Settings** from the **APIs** main navigation pane. Then type the ARN of an IAM role in the **CloudWatch log role ARN** text field. For common application scenarios, the IAM role could attach the managed policy of **AmazonAPIGatewayPushToCloudWatchLogs**, which contains the following access policy statement:

```json
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "logs:CreateLogGroup",
               "logs:CreateLogStream",
               "logs:DescribeLogGroups",
               "logs:DescribeLogStreams",
               "logs:PutLogEvents",
               "logs:GetLogEvents",
               "logs:FilterLogEvents"
           ],
           "Resource": "*"
       }
   ]
}
```

The IAM role must also contain the following trust relationship statement:

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

For more information about CloudWatch, see the [Amazon CloudWatch User Guide](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/).

7. To set stage-level throttling limits for all of the methods associated with this API, do the following in the **Default Method Throttling** section:

a. Choose **Enable throttling**.

b. For **Rate**, type the maximum number of stage-level steady-state requests per second that API Gateway can serve without returning a **429 Too Many Requests** response. This stage-level rate limit must not be more than the **account-level** rate limit as specified in [API Gateway Limits for Configuring and Running a REST API](https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-configure-limits.html).

c. For **Burst**, type the maximum number of stage-level concurrent requests that API Gateway can serve without returning a **429 Too Many Requests** response. This stage-level burst must not be more than the **account-level** burst limit as specified in [API Gateway Limits for Configuring and Running a REST API](https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-configure-limits.html).
8. To override the stage-level throttling for an individual method, expand the stage in the Stages secondary navigation pane, choose a method, and choose Override for this method for Settings. In the Method Throttling section, select appropriate options.

9. To associate an AWS WAF web ACL with the stage, choose a web ACL from the Web ACL dropdown list.

   Note
   If needed, choose Create Web ACL to open the AWS WAF console in a new browser tab, create the web ACL, and return to the API Gateway console to associate the web ACL with the stage.

10. If desired, choose Block API Request if WebACL cannot be evaluated (Fail- Close).

11. To enable AWS X-Ray tracing for the API stage:
   a. In the Stage Editor pane, choose the Logs/Tracing tab.
   b. To enable X-Ray tracing, choose Enable X-Ray Tracing under X-Ray Tracing.
   c. To set sampling rules in the X-Ray console, choose Set X-Ray Sampling Rules.
   d. If desired, choose Set X-Ray Sampling Rules and go to the X-Ray console to configure sampling rules.

   For more information, see Trace API Gateway API Execution with AWS X-Ray (p. 558).

12. Choose Save Changes. The new settings will take effect after you redeploy the API to the stage.

Delete a Stage for an API

When you no longer need a stage, you can delete it to avoid paying for unused resources. In the following, we explain how to use the API Gateway console to delete a stage.

   Warning
   Deleting a stage may cause part or all of the corresponding API to be unusable by API callers. Deleting a stage cannot be undone, but you can recreate the stage and associate it with the same deployment.

Delete a Stage with the API Gateway Console

2. In the box that contains the name of the API for the stage, choose Stages.
3. In the Stages pane, choose the stage you want to delete, and then choose Delete Stage.
4. When prompted, choose Delete.

Enable API Caching to Enhance Responsiveness

You can enable API caching in Amazon API Gateway to cache your endpoint’s responses. With caching, you can reduce the number of calls made to your endpoint and also improve the latency of requests to your API. When you enable caching for a stage, API Gateway caches responses from your endpoint for a specified time-to-live (TTL) period, in seconds. API Gateway then responds to the request by looking up the endpoint response from the cache instead of making a request to your endpoint. The default TTL value for API caching is 300 seconds. The maximum TTL value is 3600 seconds. TTL=0 means caching is disabled.

The maximum size of a response that can be cached is 1048576 bytes. Cache data encryption may increase the size of the response when it is being cached.

This is a HIPAA Eligible Service. For more information about AWS, U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), and using AWS services to process, store, and transmit protected health information (PHI), see HIPAA Overview.
Important
When you enable caching for a stage, only GET methods have caching enabled by default. This helps to ensure the safety and availability of your API. You can enable caching for other methods by overriding method settings (p. 501).

Important
Caching is charged by the hour and is not eligible for the AWS free tier.

Enable Amazon API Gateway Caching

In API Gateway, you can enable caching for a specified stage.

When you enable caching, you must choose a cache capacity. In general, a larger capacity gives a better performance, but also costs more.

API Gateway enables caching by creating a dedicated cache instance. This process can take up to 4 minutes.

API Gateway changes caching capacity by removing the existing cache instance and creating a new one with a modified capacity. All existing cached data is deleted.

In the API Gateway console, you configure caching in the Settings tab of a named Stage Editor.

To configure API caching for a given stage:

1. Go to the API Gateway console.
2. Choose the API.
3. Choose Stages.
4. In the Stages list for the API, choose the stage.
5. Choose the Settings tab.
6. Choose Enable API cache.
7. Wait for the cache creation to complete.

Note
Creating or deleting a cache takes about 4 minutes for API Gateway to complete. When a cache is created, the Cache status value changes from CREATE_IN_PROGRESS to AVAILABLE. When cache deletion is completed, the Cache status value changes from DELETE_IN_PROGRESS to an empty string.

When you enable caching within a stage's Cache Settings, only GET methods are cached. To ensure the safety and availability of your API, we recommend that you not change this setting. However, you can enable caching for other methods by overriding method settings (p. 501).

If you would like to verify if caching is functioning as expected, you have two general options:

• Inspect the CloudWatch metrics of CacheHitCount and CacheMissCount for your API and stage.
• Put a timestamp in the response.

Note
You should not use the X-Cache header from the CloudFront response to determine if your API is being served from your API Gateway cache instance.

Override API Gateway Stage-Level Caching for Method Caching

You can override stage-level cache settings by enabling or disabling caching for a specific method; by increasing or decreasing its TTL period; or by turning encryption on or off for cached responses.
If you anticipate that a method that you are caching will receive sensitive data in its responses, in **Cache Settings**, choose **Encrypt cache data**.

**To configure API caching for individual methods using the console:**

2. Go to the API Gateway console.
3. Choose the API.
4. Choose **Stages**.
5. In the **Stages** list for the API, expand the stage and choose a method in the API.
6. Choose **Override for this method** in **Settings**.
7. In the **Cache Settings** area, you can set or clear **Enable Method Cache** or customize any other desired options. (This section is shown only if stage-level caching (p. 501) is enabled.)

**Use Method or Integration Parameters as Cache Keys to Index Cached Responses**

When a cached method or integration has parameters, which can take the form of custom headers, URL paths, or query strings, you can use some or all of the parameters to form cache keys. API Gateway can cache the method's responses, depending on the parameter values used.

**Note**

Cache keys are required when setting up caching on a resource.

For example, suppose you have a request in the following format:

```
GET /users?type=... HTTP/1.1
host: example.com
...
```

In this request, `type` can take a value of `admin` or `regular`. If you include the `type` parameter as part of the cache key, the responses from `GET /users?type=admin` will be cached separately from those from `GET /users?type=regular`.

When a method or integration request takes more than one parameter, you can choose to include some or all of the parameters to create the cache key. For example, you can include only the `type` parameter in the cache key for the following request, made in the listed order within a TTL period:

```
GET /users?type=admin&department=A HTTP/1.1
host: example.com
...
```

The response from this request will be cached and will be used to serve the following request:

```
GET /users?type=admin&department=B HTTP/1.1
host: example.com
...
```

To include a method or integration request parameter as part of a cache key in the API Gateway console, select **Caching** after you add the parameter.
Flush the API Stage Cache in API Gateway

When API caching is enabled, you can flush your API stage's entire cache to ensure your API's clients get the most recent responses from your integration endpoints.

To flush the API stage cache, you can choose the **Flush entire cache** button under the **Cache Settings** section in the **Settings** tab in a stage editor of the API Gateway console. The cache-flushing operation takes a couple of minutes, after which the cache status is **AVAILABLE** immediately after flushing.

**Note**
After the cache is flushed, responses are serviced from the integration endpoint until the cache is built up again. During this period, the number of requests sent to the integration endpoint may increase. This may temporarily increase the overall latency of your API.

Invalidate an API Gateway Cache Entry

A client of your API can invalidate an existing cache entry and reload it from the integration endpoint for individual requests. The client must send a request that contains the **Cache-Control: max-age=0** header. The client receives the response directly from the integration endpoint instead of the cache, provided that the client is authorized to do so. This replaces the existing cache entry with the new response, which is fetched from the integration endpoint.

To grant permission for a client, attach a policy of the following format to an IAM execution role for the user.

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "execute-api:InvalidateCache"
    ],
    "Resource": [
      "arn:aws:execute-api:region:account-id:api-id/stage-name/GET/resource-path-specifier"
    ]
  }
]}

This policy allows the API Gateway execution service to invalidate the cache for requests on the specified resource (or resources). To specify a group of targeted resources, use a wildcard (*) character for account-id, api-id, and other entries in the ARN value of Resource. For more information on how to set permissions for the API Gateway execution service, see Control Access to an API with IAM Permissions (p. 362)

If you do not impose an InvalidateCache policy (or choose the Require authorization checkbox in the console), any client can invalidate the API cache. If most or all of the clients invalidate the API cache, this could significantly increase the latency of your API.

When the policy is in place, caching is enabled, and authorization is required, you can control how unauthorized requests are handled by choosing an option from Handle unauthorized requests in the API Gateway console.
The three options result in the following behaviors:

- **Fail the request with 403 status code**: returns a 403 Unauthorized response.
  
  To set this option using the API, use `FAIL_WITH_403`.

- **Ignore cache control header; Add a warning in response header**: process the request and add a warning header in the response.
  
  To set this option using the API, use `SUCCEED_WITH_RESPONSE_HEADER`.

- **Ignore cache control header**: process the request and do not add a warning header in the response.
  
  To set this option using the API, use `SUCCEED_WITHOUT_RESPONSE_HEADER`.

### Throttle API Requests for Better Throughput

To prevent your API from being overwhelmed by too many requests, Amazon API Gateway throttles requests to your API using the token bucket algorithm, where a token counts for a request. Specifically,
API Gateway sets a limit on a steady-state rate and a burst of request submissions against all APIs in your account. In the token bucket algorithm, the burst is the maximum bucket size.

When request submissions exceed the steady-state request rate and burst limits, API Gateway fails the limit-exceeding requests and returns 429 Too Many Requests error responses to the client. Upon catching such exceptions, the client can resubmit the failed requests in a rate-limiting fashion, while complying with the API Gateway throttling limits.

As an API developer, you can set the limits for individual API stages or methods to improve overall performance across all APIs in your account. Alternatively, you can enable usage plans (p. 432) to restrict client request submissions to within specified request rates and quotas. This restricts the overall request submissions so that they don't go significantly past the account-level throttling limits.

Topics
- How Throttling Limit Settings Are Applied in API Gateway (p. 506)
- Account-Level Throttling (p. 506)
- Default Method Throttling and Overriding Default Method Throttling (p. 507)
- Configuring API-level and Stage-Level Throttling in a Usage Plan (p. 508)
- Configuring Method-Level Throttling in a Usage Plan (p. 508)

How Throttling Limit Settings Are Applied in API Gateway

Before you configure limit settings for your API in your stage settings and optionally a usage plan (p. 432), it's useful to understand Amazon API Gateway how throttling limit settings are applied.

Amazon API Gateway provides two basic types of throttling-related settings:

- **Server-side throttling limits** are applied across all clients. These limit settings exist to prevent your API — and your account — from being overwhelmed by too many requests.
- **Per-client throttling limits** are applied to clients that use API keys associated with your usage policy as client identifier.

API Gateway throttling-related settings are applied in the following order:

1. Per-client per-method throttling limits (p. 508) that you set for an API stage in a usage plan (p. 439)
2. Per-client throttling limits (p. 508) that you set in a usage plan
3. Default per-method limits and individual per-method limits (p. 507) that you set in API stage settings (p. 498)
4. Account-level throttling (p. 506)

Account-Level Throttling

By default, API Gateway limits the steady-state request rate to 10,000 requests per second (rps). It limits the burst (that is, the maximum bucket size) to 5,000 requests across all APIs within an AWS account. In API Gateway, the burst limit corresponds to the maximum number of concurrent request submissions that API Gateway can fulfill at any moment without returning 429 Too Many Requests error responses.

To help understand these throttling limits, here are a few examples, given the burst limit and the default account-level rate limit:

- If a caller submits 10,000 requests in a one second period evenly (for example, 10 requests every millisecond), API Gateway processes all requests without dropping any.
If the caller sends 10,000 requests in the first millisecond, API Gateway serves 5,000 of those requests and throttles the rest in the one-second period.

If the caller submits 5,000 requests in the first millisecond and then evenly spreads another 5,000 requests through the remaining 999 milliseconds (for example, about 5 requests every millisecond), API Gateway processes all 10,000 requests in the one-second period without returning 429 Too Many Requests error responses.

If the caller submits 5,000 requests in the first millisecond and waits until the 101st millisecond to submit another 5,000 requests, API Gateway processes 6,000 requests and throttles the rest in the one-second period. This is because at the rate of 10,000 rps, API Gateway has served 1,000 requests after the first 100 milliseconds and thus emptied the bucket by the same amount. Of the next spike of 5,000 requests, 1,000 fill the bucket and are queued to be processed. The other 4,000 exceed the bucket capacity and are discarded.

If the caller submits 5,000 requests in the first millisecond, submits 1,000 requests at the 101st millisecond, and then evenly spreads another 4,000 requests through the remaining 899 milliseconds, API Gateway processes all 10,000 requests in the one-second period without throttling.

More generally, at any given moment, when a bucket contains $b$ and the maximum bucket capacity is $B$, the maximum additional tokens that can be added to the bucket is $# = B - b$. This maximum number of additional tokens corresponds to the maximum number of additional concurrent requests that a client can submit without receiving any 429 error responses. In general, $#$ varies in time. The value ranges from zero when the bucket is full (that is, $b = B$) to $B$ when the bucket is empty (that is, $b = 0$). The range depends on the request-processing rate, which is the rate at which tokens are removed from the bucket, and the rate limit rate, which is the rate at which tokens are added to the bucket.

The following schematic shows the general behaviors of $#$, the maximum additional concurrent requests, as a function of time. The schematic assumes that the tokens in the bucket decrease at a combined rate of $r$, starting from an empty bucket.

The account-level rate limit can be increased upon request. To request an increase of account-level throttling limits, contact the AWS Support Center. For more information, see API Gateway Limits (p. 687).

**Default Method Throttling and Overriding Default Method Throttling**

You can set the default method throttling to override the account-level request throttling limits for a specific stage or for individual methods in your API. The default method throttling limits are bounded by the account-level rate limits, even if you set the default method throttling limits higher than the account-level limits.
You can set the default method throttling limits in the API Gateway console by using the **Default Method Throttling** setting in Stages. For instructions on using the console, see Update Stage Settings (p. 498).

You can also set the default method throttling limits by calling the API Gateway V1 and V2 API References (p. 686).

### Configuring API-level and Stage-Level Throttling in a Usage Plan

In a [usage plan](p. 432), you can set a default per-method throttling limit for all methods at the API or stage level under Create Usage Plan as shown in Create a Usage Plan (p. 439).

### Configuring Method-Level Throttling in a Usage Plan

You can set additional throttling limits at the method level in Usage Plans as shown in Create a Usage Plan (p. 439). In the API Gateway console, these are set by specifying `Resource=<resource>, Method=<method>` in the **Configure Method Throttling** setting. For example, for the PetStore example (p. 56), you might specify `Resource=/pets, Method=GET`.

### Set Up Client-Side SSL Authentication in API Gateway

You can use API Gateway to generate an SSL certificate and use its public key in the backend to verify that HTTP requests to your backend system are from API Gateway. You can also enable client-side SSL authentication for an API using the API Gateway console. For more information, see the section called “Configure an API to Use SSL Certificates” (p. 412).

### Set Up AWS WAF in API Gateway

You can use AWS WAF to protect your web applications and APIs from attacks by configuring a set of rules (called a web access control list, or web ACL) that allow, block, or count web requests based on customizable web security rules and conditions that you define. For more information, see the section called “Use AWS WAF to Protect Your API from Common Web Exploits” (p. 430).

### Set Up Tags for an API Stage in API Gateway

In API Gateway, you can add a tag to an API stage, remove the tag from the stage, or view the tag. To do this, you can use the API Gateway console, the AWS CLI/SDK, or the API Gateway REST API.

A stage can also inherit tags from its parent REST API. For more information, see the section called “Tag Inheritance in the Amazon API Gateway V1 API” (p. 681).

For more information about tagging API Gateway resources, see Tagging Your API Gateway Resources (p. 680).

#### Topics
- Set up Tags for an API Stage Using the API Gateway Console (p. 508)
- Set up Tags for an API Stage Using the API Gateway REST API (p. 509)

### Set up Tags for an API Stage Using the API Gateway Console

The following procedure describes how to set up tags for an API stage.

**To set up tags for an API stage by using the API Gateway console**

1. Sign in to the API Gateway console.
2. Choose an existing API, or create a new API that includes resources, methods, and the corresponding integrations.
3. Choose a stage or deploy the API to a new stage.
4. In the **Stage Editor**, choose the **Configure Tags** button.
5. In the **Tag Editor**, choose **Add New Tag**. Type a tag key (for example, Department) in the **Key** field, and type a tag value (for example, Sales) in the **Value** field. Choose the checkmark icon to save the tag.
6. If needed, repeat Step 5 to add more tags to the API stage. The maximum number of tags per stage is 50.
7. To remove an existing tag from the stage, choose the trash bin icon next to the tag.
8. Choose **Save Changes** to finish setting up the stage tags.

If the API has been deployed previously in the API Gateway console, you'll need to redeploy it for the changes to take effect.

### Set up Tags for an API Stage Using the API Gateway REST API

You can set up tags for an API stage using the API Gateway REST API by doing one of the following:

- Call `tags:tag` to tag an API stage.
- Call `tags:untag` to delete one or more tags from an API stage.
- Call `stage:create` to add one or more tags to an API stage that you’re creating.

You can also call `tags:get` to describe tags in an API stage.

#### Tag an API Stage

After you deploy an API (m5zr3vnks7) to a stage (test), tag the stage by calling `tags:tag`. The required stage Amazon Resource Name (ARN) (arn:aws:apigateway:us-east-1::/restapis/m5zr3vnks7/stages/test) must be URL encoded (arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftest).

```plaintext
PUT /tags/arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftest
{
  "tags" : {
    "Department" : "Sales"
  }
}
```

You can also use the previous request to update an existing tag to a new value.

You can add tags to a stage when calling `stage:create` to create the stage:

```plaintext
POST /restapis/<restapi_id>/stages
{
  "stageName" : "test",
  "deploymentId" : "adr134",
  "description" : "test deployment",
  "cacheClusterEnabled" : "true",
  "cacheClusterSize" : "500",
  "variables" : {
    "sv1" : "val1"
  },
  "documentationVersion" : "test",
```
Untag an API Stage

To remove the Department tag from the stage, call tags:untag:

```
DELETE /tags/arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftest?tagKeys=Department
Host: apigateway.us-east-1.amazonaws.com
Authorization: ...
```

To remove more than one tag, use a comma-separated list of tag keys in the query expression—for example, ?tagKeys=Department,Division,....

Describe Tags for an API Stage

To describe existing tags on a given stage, call tags:get:

```
GET /tags/arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftags
Host: apigateway.us-east-1.amazonaws.com
Authorization: ...
```

The successful response is similar to the following:

```
200 OK
{
   "_links": {
      "curies": {
         "href": "http://docs.aws.amazon.com/apigateway/latest/developerguide/restapi-tags-{rel}.html",
         "name": "tags",
         "templated": true
      },
      "tags:tag": {
         "href": "/tags/arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftags",
         "tags:untag": {
            "href": "/tags/arn%3Aaws%3Aapigateway%3Aus-east-1%3A%3A%2Frestapis%2Fm5zr3vnks7%2Fstages%2Ftags{?tagKeys}",
            "templated": true
         }
      },
      "tags": {
         "Department": "Sales"
      }
   }
}
```

Set Up CloudWatch API Logging in API Gateway

To help debug issues related to request execution or client access to your API, you can enable Amazon CloudWatch Logs to log API calls. Once enabled, API Gateway will log API calls in CloudWatch. For more information, see the section called “Monitor API Execution with Amazon CloudWatch” (p. 569).
CloudWatch Log Formats for API Gateway

There are two types of API logging in CloudWatch: execution logging and access logging. In execution logging, API Gateway manages the CloudWatch Logs. The process includes creating log groups and log streams, and reporting to the log streams any caller's requests and responses. The logged data includes errors or execution traces (such as request or response parameter values or payloads), data used by Lambda authorizers (formerly known as custom authorizers), whether API keys are required, whether usage plans are enabled, and so on.

When you deploy an API, API Gateway creates a log group and log streams under the log group. The log group is named following the `API-Gateway-Execution-Logs_{rest-api-id}/{stage_name}` format. Within each log group, the logs are further divided into log streams, which are ordered by Last Event Time as logged data is reported.

In access logging, you, as an API developer, want to log who has accessed your API and how the caller accessed the API. You can create your own log group or choose an existing one, which could be managed by API Gateway. You can specify the access details by selecting `#context` (p. 293) variables, expressed in a format of your choosing, and by choosing a log group as the destination. To preserve uniqueness of each log, access log format must include `#context.requestId`.

Note
Only `#context` variables are supported, not `#input`, etc.

Choose a log format that is also adopted by your analytic backend, such as Common Log Format (CLF), JSON, XML, or CSV. You can then feed the access logs to it directly to have your metrics computed and rendered. To define the log format, set the log group ARN on the accessLogSettings/destinationArn property on the stage. You can obtain a log group ARN in the CloudWatch console, provided that the ARN column is selected for display. To define the access log format, set a chosen format on the accessLogSetting/format property on the stage.

Examples of some commonly used access log formats are shown in the API Gateway console and listed as follows.

- **CLF** (Common Log Format):

  ```
  $context.identity.sourceIp $context.identity.caller \ 
  $context.identity.user [#$context.requestTime] \ 
  "$context.httpMethod $context.resourcePath $context.protocol" \ 
  $context.status $context.responseLength $context.requestId
  ```

  The continuation characters (\) are meant as a visual aid and the log format cannot have any line breaks.

- **JSON**:

  ```
  { "requestId": "$context.requestId", \ 
    "ip": "$context.identity.sourceIp", \ 
    "caller": "$context.identity.caller", \ 
    "user": "$context.identity.user", \ 
    "requestTime": "$context.requestTime", \ 
    "httpMethod": "$context.httpMethod", \ 
    "resourcePath": "$context.resourcePath", \ 
    "status": "$context.status", \ 
    "protocol": "$context.protocol", \ 
    "responseLength": "$context.responseLength" \ 
  }
  ```

  The continuation characters (\) are meant as a visual aid and the log format cannot have any line breaks.

- **XML**
The continuation characters (\) are meant as a visual aid and the log format cannot have any line breaks.

**CSV (comma-separated values):**

```
<context.identity.sourceIp>,<context.identity.caller>,
<context.identity.user>,<context.requestTime>,<context.httpMethod>,
<context.resourcePath>,<context.protocol>,<context.status>,
<context.responseLength>,<context.requestId>
```

The continuation characters (\) are meant as a visual aid and the log format cannot have any line breaks.

### Permissions for CloudWatch Logging

To enable CloudWatch Logs, you must grant API Gateway permission to read and write logs to CloudWatch for your account. The `AmazonAPIGatewayPushToCloudWatchLogs` managed policy (with an ARN of `arn:aws:iam::aws:policy/service-role/AmazonAPIGatewayPushToCloudWatchLogs`) has all the required permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents",
                "logs:GetLogEvents",
                "logs:FilterLogEvents"
            ],
            "Resource": "*
        }
    ]
}
```

**Note**

API Gateway will call AWS Security Token Service in order to assume the IAM role, so make sure that AWS STS is enabled for the region. For more information, see Managing AWS STS in an AWS Region.

To grant these permissions to your account, create an IAM role with `apigateway.amazonaws.com` as its trusted entity, attach the preceding policy to the IAM role, and set the IAM role ARN on the `cloudWatchRoleArn` property on your Account.
If you receive an error when setting the IAM role ARN, check your AWS Security Token Service account settings to make sure that AWS STS is enabled in the region that you are using. For more information about enabling AWS STS, see Managing AWS STS in an AWS Region in the IAM User Guide.

Set up API Logging Using the API Gateway Console

To set up API logging, you must have deployed the API to a stage. You must also have configured an appropriate CloudWatch Logs role (p. 512) ARN for your account.

2. Choose Settings from the primary navigation panel and type an ARN of an IAM role with appropriate permissions in CloudWatch log role ARN. You need to do this once.
3. Do one of the following:
   a. Choose an existing API and then choose a stage.
   b. Create an API and deploy it to a stage.
4. Choose Logs/Tracing in the Stage Editor.
5. To enable execution logging:
   a. Choose Enable CloudWatch Logs under CloudWatch Settings.
   b. Choose Error or Info from the dropdown menu.
   c. If desired, choose Enable Detailed CloudWatch Metrics.
   For more information about CloudWatch metrics, see the section called “Monitor API Execution with Amazon CloudWatch” (p. 569).
6. To enable access logging:
   b. Type the ARN of a log group in CloudWatch Group. The ARN format is `arn:aws:logs:{region}:{account-id}:log-group:API-Gateway-Execution-Logs_{rest-api-id}/(stage-name}`.
   c. Type a log format in Log Format. You can choose CLF, JSON, XML, or CSV to use one of the provided examples as a guide.
7. Choose Save Changes.

Note
You can enable execution logging and access logging independent of each other.

API Gateway is now ready to log requests to your API. You do not need to redeploy the API when you update the stage settings, logs, or stage variables.

Set Up X-Ray Tracing in API Gateway

To help debug issues related to API request latency, you can enable AWS X-Ray tracing to trace API requests and downstream services. Once enabled, API Gateway will trace API calls in X-Ray. For more information, see the section called “Setting Up AWS X-Ray” (p. 559).

Set Up CloudTrail Logging in API Gateway

There is nothing you need to do to enable CloudTrail logging for your API. It is enabled automatically. For more information, see the section called “Log Calls to Amazon API Gateway APIs with AWS CloudTrail” (p. 568).
Set up Stage Variables for a REST API Deployment

Stage variables are name-value pairs that you can define as configuration attributes associated with a deployment stage of a REST API. They act like environment variables and can be used in your API setup and mapping templates.

For example, you can define a stage variable in a stage configuration, and then set its value as the URL string of an HTTP integration for a method in your REST API. Later, you can reference the URL string using the associated stage variable name from the API setup. This way, you can use the same API setup with a different endpoint at each stage by resetting the stage variable value to the corresponding URLs. You can also access stage variables in the mapping templates, or pass configuration parameters to your AWS Lambda or HTTP backend.

For more information about mapping templates, see API Gateway Mapping Template and Access Logging Variable Reference (p. 293).

Use Cases

With deployment stages in API Gateway, you can manage multiple release stages for each API, such as alpha, beta, and production. Using stage variables you can configure an API deployment stage to interact with different backend endpoints. For example, your API can pass a GET request as an HTTP proxy to the backend web host (for example, http://example.com). In this case, the backend web host is configured in a stage variable so that when developers call your production endpoint, API Gateway calls example.com. When you call your beta endpoint, API Gateway uses the value configured in the stage variable for the beta stage, and calls a different web host (for example, beta.example.com). Similarly, stage variables can be used to specify a different AWS Lambda function name for each stage in your API.

You can also use stage variables to pass configuration parameters to a Lambda function through your mapping templates. For example, you may want to re-use the same Lambda function for multiple stages in your API, but the function should read data from a different Amazon DynamoDB table depending on which stage is being called. In the mapping templates that generate the request for the Lambda function, you can use stage variables to pass the table name to Lambda.

Stage variables are not applied to the security definitions section of the API specification. For example, you cannot use different Amazon Cognito user pools for different stages.

Examples

To use a stage variable to customize the HTTP integration endpoint, you must first configure a stage variable of a specified name, e.g., url, and then assign it a value, e.g., example.com. Next, from your method configuration, set up an HTTP proxy integration, and instead of entering the endpoint's URL, you can tell API Gateway to use the stage variable value, http://${stageVariables.url}. This value tells API Gateway to substitute your stage variable ${} at runtime, depending on which stage your API is running. You can reference stage variables in a similar way to specify a Lambda function name, an AWS Service Proxy path, or an AWS role ARN in the credentials field.

When specifying a Lambda function name as a stage variable value, you must configure the permissions on the Lambda function manually. You can use the AWS Command Line Interface to do this.

```
```

The following example assigns API Gateway permission to invoke a Lambda function named helloWorld hosted in the US West (Oregon) region of an AWS account on behalf of the API method.
Here is the same command using the AWS CLI.

```
```

Set Stage Variables Using the Amazon API Gateway Console

In this tutorial, you will learn how to set stage variables for two deployment stages of a sample API, using the Amazon API Gateway console. Before you begin, make sure the following prerequisites are met:

- You must have an API available in API Gateway. Follow the instructions in Creating a REST API in Amazon API Gateway (p. 177).
- You must have deployed the API at least once. Follow the instructions in Deploying a REST API in Amazon API Gateway (p. 494).
- You must have created the first stage for a deployed API. Follow the instructions in Create a New Stage (p. 497).

To Declare Stage Variables Using the API Gateway Console

2. Create an API, create a GET method on the API's root resource, if you have not already done so. Set the HTTP Endpoint URL value as "http://${stageVariables.url}" and then choose Save.
3. Choose Deploy API. Choose New Stage and enter "beta" for Stage name. Choose Deploy.
4. In the beta Stage Editor panel; choose the Stage Variables tab; and then choose Add Stage Variable.
5. Enter the "url" string in the Name field and the "httpbin.org/get" in the Value field. Choose the checkmark icon to save the setting for the stage variable.
6. Repeat the above step to add two more stage variables: version and function. Set their values as "v-beta" and "HelloWorld", respectively.

   **Note**
   When setting a Lambda function as the value of a stage variable, use the function's local name, possibly including its alias or version specification, as in HelloWorld, HelloWorld:1 or HelloWorld:alpha. Do not use the function's ARN (for example, arn:aws:lambda:us-east-1:123456789012:function:HelloWorld). The API Gateway console assumes the stage variable value for a Lambda function as the unqualified function name and will expand the given stage variable into an ARN.
7. From the Stages navigation pane, choose Create. For Stage name, type prod. Select a recent deployment from Deployment and then choose Create.
8. As with the beta stage, set the same three stage variables (url, version, and function) to different values ("petstore-demo-endpoint.execute-api.com/petstore/pets", "v-prod", and "HelloEveryone"), respectively.

Use Amazon API Gateway Stage Variables

You can use API Gateway stage variables to access the HTTP and Lambda backends for different API deployment stages and to pass stage-specific configuration metadata into an HTTP backend as a query parameter and into a Lambda function as a payload generated in an input mapping template.
Prerequisites

You must create two stages with a url variable set to two different HTTP endpoints: a function stage variable assigned to two different Lambda functions, and a version stage variable containing stage-specific metadata. Follow the instructions in Set Stage Variables Using the Amazon API Gateway Console (p. 515).

Access an HTTP endpoint through an API with a stage variable

1. In the Stages navigation pane, choose beta. In beta Stage Editor, choose the Invoke URL link. This starts the beta stage GET request on the root resource of the API.

   Note
   The Invoke URL link points to the root resource of the API in its beta stage. Navigating to the URL by choosing the link calls the beta stage GET method on the root resource. If methods are defined on child resources and not on the root resource itself, choosing the Invoke URL link will return a {"message":"Missing Authentication Token"} error response. In this case, you must append the name of a specific child resource to the Invoke URL link.

2. The response you get from the beta stage GET request is shown next. You can also verify the result by using a browser to navigate to http://httpbin.org/get. This value was assigned to the url variable in the beta stage. The two responses are identical.

3. In the Stages navigation pane, choose the prod stage. From prod Stage Editor, choose the Invoke URL link. This starts the prod stage GET request on the root resource of the API.

4. The response you get from the prod stage GET request is shown next. You can verify the result by using a browser to navigate to http://petstore-demo-endpoint-execute-api.com/petstore/pets. This value was assigned to the url variable in the prod stage. The two responses are identical.

Pass stage-specific metadata to an HTTP backend via a stage variable in a query parameter expression

This procedure describes how to use a stage variable value in a query parameter expression to pass stage-specific metadata into an HTTP back end. We will use the version stage variable declared in Set Stage Variables Using the Amazon API Gateway Console (p. 515).

1. In the Resource navigation pane, choose the GET method. To add a query string parameter to the method's URL, in Method Execution, choose Method Request. Type version for the parameter name.

2. In Method Execution choose Integration Request. Edit the Endpoint URL value to append ?version=${stageVariables.version} to the previously defined URL value, which, in this case, is also expressed with the url stage variable. Choose Deploy API to deploy these changes.

3. In the Stages navigation pane, choose the beta stage. From beta Stage Editor, verify that the current stage is in the most recent deployment, and then choose the Invoke URL link.

   Note
   We use the beta stage here because the HTTP endpoint, as specified by the url variable, "http://httpbin.org/get", accepts query parameter expressions and returns them as the args object in its response.

4. The response is shown next. Notice that v-beta, assigned to the version stage variable, is passed in the backend as the version argument.
Set up a Stage

Call Lambda function through API with a stage variable

This procedure describes how to use a stage variable to call a Lambda function as a back end of your API. We will use the function stage variable declared earlier. For more information, see Set Stage Variables Using the Amazon API Gateway Console (p. 515).

1. In the Resources pane, create a /lambdasv1 child resource under the root directory, and then create a GET method on the child resource. Set the Integration type to Lambda Function, and in Lambda Function, type ${stageVariables.function}. Choose Save.

Tip
When prompted with Add Permission to Lambda Function, make a note of the AWS CLI command before choosing OK. You must run the command on each Lambda function that is or will be assigned to the function stage variable for each of the newly created API methods. For example, if the $stageVariables.function value is HelloWorld and you have not added permission to this function yet, you must run the following AWS CLI command:

```json
{
    "args": {
        "version": "v-beta"
    },
    "headers": {
        "Accept": "application/json",
        "Host": "httpbin.org",
        "User-Agent": "AmazonAPIGateway_h4ah70cvm6"
    },
    "origin": "52.91.42.97",
    "url": "http://httpbin.org/get?version=v-beta"
}
```

Failing to do so results in a 500 Internal Server Error response when invoking the method. Make sure to replace `${stageVariables.function}` with the Lambda function name that is assigned to the stage variable.

2. Deploy the API to available stages.
3. In the Stages navigation pane, choose the beta stage. Verify that your most recent deployment is in beta Stage Editor. Copy the Invoke URL link, paste it into the address bar of your browser, and append `/lambdasv1` to that URL. This calls the underlying Lambda function through the GET method on the LambdaSv1 child resource of the API.

**Note**
Your HelloWorld Lambda function implements the following code.

```
exports.handler = function(event, context, callback) {
  if (event.version)
    callback(null, 'Hello, World! (' + event.version + ')');
  else
    callback(null, "Hello, world! (v-unknown)");
};
```

This implementation results in the following response.

"Hello, world! (v-unknown)"

**Pass stage-specific metadata to a Lambda function via a stage variable**

This procedure describes how to use a stage variable to pass stage-specific configuration metadata into a Lambda function. We will use a POST method and an input mapping template to generate payload using the version stage variable declared earlier.

1. In the Resources pane, choose the `/lambdasv1` child resource. Create a POST method on the child resource, set the Integration type to Lambda Function, and type `${stageVariables.function}` in Lambda Function. Choose Save.

**Tip**
This step is similar to the step we used to create the GET method. For more information, see Call Lambda function through API with a stage variable (p. 517).
2. From the /Method Execution pane, choose Integration Request. In the Integration Request pane, expand Mapping Templates, and then choose Add mapping template to add a template for the application/json content-type, as shown in the following.

Note
In a mapping template, a stage variable must be referenced within quotes (as in "$stageVariables.version" or "${stageVariables.version}"), whereas elsewhere it must be referenced without quotes (as in ${stageVariables.function}).

3. Deploy the API to available stages.

4. In the Stages navigation pane, choose beta. In beta Stage Editor, verify that the current stage has the most recent deployment. Copy the Invoke URL link, paste it into the URL input field of a REST API client, append /lambdasv1 to that URL, and then submit a POST request to the underlying Lambda function.

Note
You will get the following response.

"Hello, world! (v-beta)"

Amazon API Gateway Stage Variables Reference

You can use API Gateway stage variables in the following cases.
Parameter Mapping Expressions

A stage variable can be used in a parameter mapping expression for an API method's request or response header parameter, without any partial substitution. In the following example, the stage variable is referenced without the $ and the enclosing {...}.

- stageVariables.<variable_name>

Mapping Templates

A stage variable can be used anywhere in a mapping template, as shown in the following examples.

- { "name" : "$stageVariables.<variable_name>"}
- { "name" : "#{stageVariables.<variable_name>}"}

HTTP Integration URIs

A stage variable can be used as part of an HTTP integration URL, as shown in the following examples.

- A full URI without protocol, e.g., http://${stageVariables.<variable_name}>
- A full domain: e.g., http://${stageVariables.<variable_name>}/resource/operation
- A subdomain: e.g., http://${stageVariables.<variable_name>}.example.com/resource/operation
- A path, e.g., http://example.com/${stageVariables.<variable_name>}/bar
- A query string, e.g., http://example.com/foo?q=${stageVariables.<variable_name>}

AWS Integration URIs

A stage variable can be used as part of AWS URI action or path components, as shown in the following example.

- arn:aws:apigateway:<region>:<service>:${stageVariables.<variable_name>}

AWS Integration URIs (Lambda Functions)

A stage variable can be used in place of a Lambda function name, or version/alias, as shown in the following examples.


AWS Integration Credentials

A stage variable can be used as part of AWS user/role credential ARN, as shown in the following example.

- arn:aws:iam::<account_id>:${stageVariables.<variable_name>}

520
Generate an SDK for a REST API in API Gateway

To call your REST API in a platform- or language-specific way, you must generate the platform- or language-specific SDK of the API. Currently, API Gateway supports generating an SDK for an API in Java, JavaScript, Java for Android, Objective-C or Swift for iOS, and Ruby.

This section explains how to generate an SDK of an API Gateway API and demonstrates how to use the generated SDK in a Java app, a Java for Android app, Objective-C and Swift for iOS apps, and a JavaScript app.

To facilitate the discussion, we use this API Gateway API (p. 527), which exposes this Simple Calculator (p. 525) Lambda function.

Before proceeding, create or import the API and deploy it at least once in API Gateway. For instructions, see Deploying a REST API in Amazon API Gateway (p. 494).

Topics
- Generate SDKs for an API Using the API Gateway Console (p. 521)
- Generate SDKs for an API Using AWS CLI Commands (p. 524)
- Simple Calculator Lambda Function (p. 525)
- Simple Calculator API in API Gateway (p. 527)
- Simple Calculator API OpenAPI Definition (p. 531)

Generate SDKs for an API Using the API Gateway Console

To generate a platform- or language-specific SDK for an API in API Gateway, you must first create, test, and deploy the API in a stage. For illustration purposes, we use the Simple Calculator (p. 531) API as an example to generate language-specific or platform-specific SDKs throughout this section. For instructions on how to create, test, and deploy this API, see Create the Simple Calculator API (p. 527).

Topics
- Generate the Java SDK of an API (p. 521)
- Generate the Android SDK of an API (p. 522)
- Generate the iOS SDK of an API (p. 522)
- Generate the JavaScript SDK of an API (p. 523)
- Generate the Ruby SDK of an API (p. 523)

Generate the Java SDK of an API

To generate the Java SDK of an API in API Gateway

2. In the box that contains the name of the API for the stage, choose Stages.
3. In the Stages pane, choose the name of the stage.
4. On the SDK Generation tab, for Platform, choose Java and do the following:
   a. For Service Name, specify the name of your SDK. For example, SimpleCalcSdk. This becomes the name of your SDK client class. The name corresponds to the <name> tag under <project> in the pom.xml file, which is in the SDK's project folder. Do not include hyphens.
   b. For Java Package Name, specify a package name for your SDK. For example, examples.aws.apig.simpleCalc.sdk. This package name is used as the namespace of your SDK library. Do not include hyphens.
c. For **Java Build System**, type `maven` or `gradle` to specify the build system.

d. For **Java Group Id**, type a group identifier for your SDK project. For example, `my-apig-api-examples`. This identifier corresponds to the `<groupId>` tag under `<project>` in the pom.xml file, which is in the SDK's project folder.

e. For **Java Artifact Id**, type an artifact identifier for your SDK project. For example, `simple-calc-sdk`. This identifier corresponds to the `<artifactId>` tag under `<project>` in the pom.xml file, which is in the SDK's project folder.

f. For **Java Artifact Version**, type a version identifier string. For example, `1.0.0`. This version identifier corresponds to the `<version>` tag under `<project>` in the pom.xml file, which is in the SDK's project folder.

g. For **Source Code License Text**, type the license text of your source code, if any.

5. Choose **Generate SDK**, and then follow the on-screen directions to download the SDK generated by API Gateway.

6. Follow the instructions in **Use a Java SDK Generated by API Gateway for a REST API (p. 538)** to use the generated SDK.

Every time you update an API, you must redeploy the API and regenerate the SDK to have the updates included.

**Generate the Android SDK of an API**

**To generate the Android SDK of an API in API Gateway**


2. In the box that contains the name of the API for the stage, choose **Stages**.

3. In the **Stages** pane, choose the name of the stage.

4. On the **SDK Generation** tab, for **Platform**, choose the Android platform.

   a. For **Group ID**, type the unique identifier for the corresponding project. This is used in the pom.xml file (for example, `com.mycompany`).

   b. For **Invoker package**, type the namespace for the generated client classes (for example, `com.mycompany.clientsdk`).

   c. For **Artifact ID**, type the name of the compiled .jar file without the version. This is used in the pom.xml file (for example, `aws-apigateway-api-sdk`).

   d. For **Artifact version**, type the artifact version number for the generated client. This is used in the pom.xml file and should follow a `major.minor.patch` pattern (for example, `1.0.0`).

5. Choose **Generate SDK**, and then follow the on-screen directions to download the SDK generated by API Gateway.

6. Follow the instructions in **Use an Android SDK Generated by API Gateway for a REST API (p. 542)** to use the generated SDK.

Every time you update an API, you must redeploy the API and regenerate the SDK to have the updates included.

**Generate the iOS SDK of an API**

**To generate the iOS SDK of an API in API Gateway**


2. In the box that contains the name of the API for the stage, choose **Stages**.

3. In the **Stages** pane, choose the name of the stage.


4. On the **SDK Generation** tab, for **Platform**, choose the **iOS (Objective-C)** or **iOS (Swift)** platform.

   - Type a unique prefix in the **Prefix** box.

     The effect of prefix is as follows: if you assign, for example, `SIMPLE_CALC` as the prefix for the SDK of the SimpleCalc (p. 527) API with Input, Output, and Result models, the generated SDK will contain the `SIMPLE_CALC_SimpleCalcClient` class that encapsulates the API, including the method requests/responses. In addition, the generated SDK will contain the `SIMPLE_CALC_Input`, `SIMPLE_CALC_Output`, and `SIMPLE_CALC_Result` classes to represent the input, output, and results, respectively, to represent the request input and response output. For more information, see Use iOS SDK Generated by API Gateway for a REST API in Objective-C or Swift (p. 548).

5. Choose **Generate SDK**, and then follow the on-screen directions to download the SDK generated by API Gateway.

6. Follow the instructions in Use iOS SDK Generated by API Gateway for a REST API in Objective-C or Swift (p. 548) to use the generated SDK.

Every time you update an API, you must redeploy the API and regenerate the SDK to have the updates included.

**Generate the JavaScript SDK of an API**

**To generate the JavaScript SDK of an API in API Gateway**

2. In the box that contains the name of the API for the stage, choose **Stages**.
3. In the **Stages** pane, choose the name of the stage.
4. On the **SDK Generation** tab, for **Platform**, choose **JavaScript**.
5. Choose **Generate SDK**, and then follow the on-screen directions to download the SDK generated by API Gateway.
6. Follow the instructions in Use a JavaScript SDK Generated by API Gateway for a REST API (p. 543) to use the generated SDK.

Every time you update an API, you must redeploy the API and regenerate the SDK to have the updates included.

**Generate the Ruby SDK of an API**

**To generate the Ruby SDK of an API in API Gateway**

2. In the box that contains the name of the API for the stage, choose **Stages**.
3. In the **Stages** pane, choose the name of the stage.
4. On the **SDK Generation** tab, for **Platform**, choose **Ruby**.

   - For **Service Name**, specify the name of your SDK. For example, `SimpleCalc`. This is used to generate the Ruby Gem namespace of your API. The name must be all letters, (a-zA-Z), without any other special characters or numbers.

   - For **Ruby Gem Name**, specify the name of the Ruby Gem to contain the generated SDK source code for your API. By default it is the lower-cased service name plus the `−sdk` suffix; for example `simplecalc−sdk`.

   - For **Ruby Gem Version**, specify a version number for the generated Ruby Gem. By default, it is set to `1.0.0`. 

---

523
5. Choose **Generate SDK**, and then follow the on-screen directions to download the SDK generated by API Gateway.

6. Follow the instructions in Use a Ruby SDK Generated by API Gateway for a REST API (p. 545) to use the generated SDK.

Every time you update an API, you must redeploy the API and regenerate the SDK to have the updates included.

**Generate SDKs for an API Using AWS CLI Commands**

You can use AWS CLI to generate and download an SDK of an API for a supported platform by calling the `get-sdk` command. We demonstrate this for some of the supported platforms in the following.

**Topics**

- Generate and Download the Java for Android SDK Using AWS CLI (p. 524)
- Generate and Download the JavaScript SDK Using AWS CLI (p. 524)
- Generate and Download the Ruby SDK Using AWS CLI (p. 524)

**Generate and Download the Java for Android SDK Using AWS CLI**

To generate and download a Java for Android SDK generated by API Gateway of an API (**udpuvvzbkc**) at a given stage (**test**), call the command as follows:

```bash
aws apigateway get-sdk \\
    --rest-api-id udpuvvzbkc \\
    --stage-name test \\
    --sdk-type android \\
    --parameters groupId='com.mycompany',
    invokerPackage='com.mycompany.myApiSdk',
    artifactId='myApiSdk',
    artifactVersion='0.0.1' \\
    ~/apps/myApi/myApi-android-sdk.zip
```

The last input of `~/apps/myApi/myApi-android-sdk.zip` is the path to the downloaded SDK file named `myApi-android-sdk.zip`.

**Generate and Download the JavaScript SDK Using AWS CLI**

To generate and download a JavaScript SDK generated by API Gateway of an API (**udpuvvzbkc**) at a given stage (**test**), call the command as follows:

```bash
aws apigateway get-sdk \\
    --rest-api-id udpuvvzbkc \\
    --stage-name test \\
    --sdk-type javascript \\
    ~/apps/myApi/myApi-js-sdk.zip
```

The last input of `~/apps/myApi/myApi-js-sdk.zip` is the path to the downloaded SDK file named `myApi-js-sdk.zip`.

**Generate and Download the Ruby SDK Using AWS CLI**

To generate and download a Ruby SDK of an API (**udpuvvzbkc**) at a given stage (**test**), call the command as follows:

```bash
aws apigateway get-sdk \\
    --rest-api-id udpuvvzbkc \\
    --stage-name test \\
    --sdk-type javascript \\
    ~/apps/myApi/myApi-ruby-sdk.zip
```

The last input of `~/apps/myApi/myApi-ruby-sdk.zip` is the path to the downloaded SDK file named `myApi-ruby-sdk.zip`.
aws apigateway get-sdk \
  --rest-api-id udpuvvzbkc \
  --stage-name test \
  --sdk-type ruby \
  --parameters service.name=myApiRubySdk,ruby.gem-name=myApi,ruby.gem-\n  version=0.01 \
  ~/apps/myApi/myApi-ruby-sdk.zip

The last input of ~/apps/myApi/myApi-ruby-sdk.zip is the path to the downloaded SDK file named myApi-ruby-sdk.zip.

Next, we show how to use the generated SDK to call the underlying API. For more information, see Call REST API through Generated SDKs (p. 538).

**Simple Calculator Lambda Function**

As an illustration, we will use a Node.js Lambda function that performs the binary operations of addition, subtraction, multiplication and division.

Topics
- Simple Calculator Lambda Function Input Format (p. 525)
- Simple Calculator Lambda Function Output Format (p. 525)
- Simple Calculator Lambda Function Implementation (p. 525)
- Create the Simple Calculator Lambda Function (p. 526)

**Simple Calculator Lambda Function Input Format**

This function takes an input of the following format:

```
{ "a": "Number", "b": "Number", "op": "string"}
```

where `op` can be any of `(+, -, *, /, add, sub, mul, div)`.

**Simple Calculator Lambda Function Output Format**

When an operation succeeds, it returns the result of the following format:

```
{ "a": "Number", "b": "Number", "op": "string", "c": "Number"}
```

where `c` holds the result of the calculation.

**Simple Calculator Lambda Function Implementation**

The implementation of the Lambda function is as follows:

```
console.log('Loading the calculator function');
exports.handler = function(event, context, callback) {
  console.log('Received event:', JSON.stringify(event, null, 2));
  if (event.a === undefined || event.b === undefined || event.op === undefined) {
    callback("400 Invalid Input");
  }
```
var res = {};
res.a = Number(event.a);
res.b = Number(event.b);
res.op = event.op;

if (isNaN(event.a) || isNaN(event.b)) {
    callback("400 Invalid Operand");
}

switch(event.op)
{
    case "+";
    case "add":
        res.c = res.a + res.b;
        break;
    case "-";
    case "sub":
        res.c = res.a - res.b;
        break;
    case "*";
    case "mul":
        res.c = res.a * res.b;
        break;
    case "/";
    case "div":
        res.c = res.b===0 ? NaN : Number(event.a) / Number(event.b);
        break;
    default:
        callback("400 Invalid Operator");
        break;
}

callback(null, res);

Create the Simple Calculator Lambda Function

You can use the AWS Lambda console at https://console.aws.amazon.com/lambda/ to create the function, pasting the above code listing into the online code editor as follows.
Simple Calculator API in API Gateway

Our simple calculator API exposes three methods (GET, POST, GET) to invoke the Simple Calculator Lambda Function (p. 525). A graphical representation of this API is shown as follows:

These three methods show different ways to supply the input for the backend Lambda function to perform the same operation:

- The GET /a=...&b=...&op=... method uses the query parameters to specify the input.
- The POST / method uses a JSON payload of {"a":"Number", "b":"Number", "op":"string"} to specify the input.
- The GET /{a}/{b}/{op} method uses the path parameters to specify the input.

If not defined, API Gateway generates the corresponding SDK method name by combining the HTTP method and path parts. The root path part (/) is referred to as Api Root. For example, the default Java SDK method name for the API method of GET /a=...&b=...&op=... is getABOp, the default SDK method name for POST / is postApiRoot, and the default SDK method name for GET /{a}/{b}/{op} is getABOp. Individual SDKs may customize the convention. Consult the documentation in the generated SDK source for SDK specific method names.

You can, and should, override the default SDK method names by specifying the operationName property on each API method. You can do so when creating the API method or updating the API method using the API Gateway REST API. In the API Swagger definition, you can set the operationId to achieve the same result.
Before showing how to call these methods using an SDK generated by API Gateway for this API, let's recall briefly how to set them up. For detailed instructions, see Creating a REST API in Amazon API Gateway (p. 177). If you're new to API Gateway, see Build an API Gateway API with Lambda Integration (p. 26) first.

Create Models for Input and Output

To specify strongly typed input in the SDK, we create an Input model for the API:

```json
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "properties": {
      "c": {"type":"number"}
   },
   "title": "Input"
}
```

Similarly, to describe the response body data type, we create the following models in the API Gateway:

```json
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "properties": {
      "input": {
         "$ref": "https://apigateway.amazonaws.com/restapis/t7dve4zn36/models/Input"
      },
      "output": {
         "$ref": "https://apigateway.amazonaws.com/restapis/t7dve4zn36/models/Output"
      }
   },
   "title": "Result"
}
```
Set Up GET / Method Query Parameters

For the GET /?a=..&b=..&op=.. method, the query parameters are declared in **Method Request**:

```
/ - GET - Method Execution
```

Set Up Data Model for the Payload as Input to the Backend

For the POST / method, we create the **Input** model and add it to the method request to define the shape of input data.
With this model, your API customers can call the SDK to specify the input by instantiating an `Input` object. Without this model, your customers would be required to create a dictionary object to represent the JSON input to the Lambda function.

**Set Up Data Model for the Result Output from the Backend**

For all three methods, we create the `Result` model and add it to the method's `Method Response` to define the shape of output returned by the Lambda function.
With this model, your API customers can parse a successful output by reading properties of a `Result` object. Without this model, customers would be required to create dictionary object to represent the JSON output.

In addition, you can also create and set up the API following the Swagger API definitions (p. 531).

**Simple Calculator API OpenAPI Definition**

The following is the OpenAPI definition of the simple calculator API. You can import it into your account. However, you need to reset the resource-based permissions on the Lambda function (p. 525) after the import. To do so, re-select the Lambda function that you created in your account from the **Integration Request** in the API Gateway console. This will cause the API Gateway console to reset the required permissions. Alternatively, you can use AWS Command Line Interface for Lambda command of `add-permission`.

OpenAPI 2.0

```json
{
  "swagger": "2.0",
  "info": {
    "version": "2016-09-29T20:27:30Z",
    "title": "SimpleCalc"
  },
  "host": "t6dve4zn25.execute-api.us-west-2.amazonaws.com",
  "basePath": "/demo",
  "schemes": ["https"],
  "paths": {
    ":\{\}/\{op\}": {
      "get": {
        "consumes": [
          "application/json"
        ]
      }
    }
  }
}
```
"parameters": [
  {
    "name": "op",
    "in": "query",
    "required": false,
    "type": "string"
  },
  {
    "name": "a",
    "in": "query",
    "required": false,
    "type": "string"
  },
  {
    "name": "b",
    "in": "query",
    "required": false,
    "type": "string"
  }
],
"responses": {
  "200": {
    "description": "200 response",
    "schema": {
      "$ref": "#/definitions/Result"
    }
  }
},
"x-amazon-apigateway-integration": {
  "requestTemplates": {
    "application/json": "#set($inputRoot = $input.path('$$'))\n{\n  "a" : $input.params('a'), \n  "b" : $input.params('b'), \n  "op" : $input.params('op')\n}\n"},
  "passthroughBehavior": "when_no_templates",
  "httpMethod": "POST",
  "responses": {
    "default": {
      "statusCode": "200",
      "responseTemplates": {
        "application/json": "#set($inputRoot = $input.path('$$'))\n{\n  "input" : {\n    "a" : $inputRoot.a, \n    "b" : $inputRoot.b, \n    "op" : $inputRoot.op\n  }, \n  "output" : {\n    "c" : $inputRoot.c\n  }}\n"}
    }
  }
},
"type": "aws"}
"required": true,
"schema": {
"$ref": "#/definitions/Input"
}
],
"responses": {
"200": {
"description": "200 response",
"schema": {
"$ref": "#/definitions/Result"
}
}
},
"x-amazon-apigateway-integration": {
"passthroughBehavior": "when_no_match",
"httpMethod": "POST",
"responses": {
"default": {
"statusCode": "200",
"responseTemplates": {
"application/json": "#set($inputRoot = $input.path('\\$'))\\n{\\n"input" : {\\n  "a" : $inputRoot.a,\\n  "b" : $inputRoot.b,\\n  "op" : $inputRoot.op\\n },\\n"output" : {\\n  "c" : $inputRoot.c\\n}}\\n}\\n}
},
"type": "aws"
}
},
"/{a}": {
"x-amazon-apigateway-any-method": {
"consumes": [
"application/json"
],
"produces": [
"application/json"
],
"parameters": [
{
"name": "a",
"in": "path",
"required": true,
"type": "string"
}
],
"responses": {
"404": {
"description": "404 response"
}
},
"x-amazon-apigateway-integration": {
"requestTemplates": {
"application/json": "{"statusCode": 200}"
},
"passthroughBehavior": "when_no_match",
"responses": {
"default": {
"statusCode": "404",
"responseTemplates": {
"application/json": "{ "Message" : "$context.httpMethod $context.resourcePath" }"}
}
}
"/\{a\}/\{b\}\": {
  "x-amazon-apigateway-any-method": {
    "consumes": [
      "application/json"
    ],
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "a",
        "in": "path",
        "required": true,
        "type": "string"
      },
      {
        "name": "b",
        "in": "path",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "404": {
        "description": "404 response"
      }
    },
    "x-amazon-apigateway-integration": {
      "requestTemplates": {
        "application/json": "{\\"statusCode\\": 200}"
      },
      "passthroughBehavior": "when_no_match",
      "responses": {
        "default": {
          "statusCode": "404",
          "responseTemplates": {
            "application/json": "{ \"Message\": \"Can't \$context.httpMethod \$context.resourcePath\" }"}
        }
      }
    }
  }
},
"type": "mock"
},
"/\{a\}/\{b\}/\{op\}\": {
  "get": {
    "consumes": [
      "application/json"
    ],
    "produces": [
      "application/json"
    ],
    "parameters": [
      {
        "name": "a",
        "in": "path",
        "required": true,
        "type": "string"
      },
      {
        "name": "b",
        "in": "path",
        "required": true,
        "type": "string"
      }
    ],
    "responses": {
      "404": {
        "description": "404 response"
      }
    },
    "x-amazon-apigateway-integration": {
      "requestTemplates": {
        "application/json": "{\\"statusCode\\": 200}"
      },
      "passthroughBehavior": "when_no_match",
      "responses": {
        "default": {
          "statusCode": "404",
          "responseTemplates": {
            "application/json": "{ \"Message\": \"Can't \$context.httpMethod \$context.resourcePath\" }"}
        }
      }
    }
  }
},
"type": "mock"
}
{  
"name": "b",  
"in": "path",  
"required": true,  
"type": "string" 
},  
{  
"name": "op",  
"in": "path",  
"required": true,  
"type": "string" 
},  
"responses": {  
"200": {  
"description": "200 response",  
"schema": {  
"$ref": "#/definitions/Result" 
}  
}  
},  
"x-amazon-apigateway-integration": {  
"requestTemplates": {  
"application/json": "#set($inputRoot = $input.path('$'))\n{\n  "a" : $input.params('a'),\n  "b" : $input.params('b'),\n  "op" : $input.params('op')\n}\n"},  
"passthroughBehavior": "when_no_templates",  
"httpMethod": "POST",  
"responses": {  
"default": {  
"statusCode": "200",  
"responseTemplates": {  
"application/json": "#set($inputRoot = $input.path('$'))\n{\n  "input": {\n    "a" : $inputRoot.a,\n    "b" : $inputRoot.b,\n    "op" : $inputRoot.op\n  },\n  "output": {\n    "c" : $inputRoot.c\n  }\n}\n"  
}  
}  
},  
"definitions": {  
"Input": {  
"type": "object",  
"properties": {  
  "a": {  
    "type": "number"  
  },  
  "b": {  
    "type": "number"  
  },  
  "op": {  
    "type": "string"  
  }  
}  
},  
"title": "Input"  
},  
"Output": {  
"type": "object",  
"properties": {  
  "c": {  
    "type": "number"  
  }  
}  
}  
}
Invoking a REST API in Amazon API Gateway

Calling a deployed API involves submitting requests to the URL for the API Gateway component service for API execution, known as execute-api.

The base URL for REST APIs is in the following format:

```
https://{restapi_id}.execute-api.{region}.amazonaws.com/{stage_name}/
```

where `{restapi_id}` is the API identifier, `{region}` is the region, and `{stage_name}` is the stage name of the API deployment.

**Important**

Before you can invoke an API, you must deploy it in API Gateway. To do that, follow the instructions in Deploying a REST API in Amazon API Gateway (p. 494).

**Topics**

- Obtain an API's Invoke URL in the API Gateway Console (p. 536)
- Use the API Gateway Console to Test a REST API Method (p. 537)
- Use Postman to Call a REST API (p. 538)
- Call REST API through Generated SDKs (p. 538)
- Call REST API through AWS Amplify JavaScript Library (p. 556)
- How to Invoke a Private API (p. 556)

Obtain an API's Invoke URL in the API Gateway Console

You can find a REST API's root URL in the **Stage Editor** for the API in the API Gateway console. It is listed as the **Invoke URL** at the top. If the API's root resource exposes a GET method without requiring user authentication, you can call the method by clicking the **Invoke URL** link. You can also construct this root URL by combining the `host` and `basePath` fields of an exported OpenAPI definition file of the API.

If an API permits anonymous access, you can use any web browser to invoke any GET method calls by copying and pasting an appropriate invocation URL to the browser's address bar. For other methods or any authentication-required calls, the invocation will be more involved because you must specify a
payload or sign the requests. You can handle these in a script behind an HTML page or in a client app using one of the AWS SDKs.

For testing, you can use the API Gateway console to call an API using the API Gateway's TestInvoke feature, which bypasses the Invoke URL and allows API testing before the API is deployed. Alternatively, you can use the Postman app to test a successfully deployed API, without writing a script or a client.

**Note**
Query string parameter values in an invocation URL cannot contain %%.

## Use the API Gateway Console to Test a REST API Method

Use the API Gateway console to test a REST API method.

### Topics
- Prerequisites (p. 537)
- Test a Method with the API Gateway Console (p. 537)

### Prerequisites
- You must specify the settings for the methods you want to test. Follow the instructions in Set up REST API Methods in API Gateway (p. 199).

### Test a Method with the API Gateway Console

**Important**
Testing methods with the API Gateway console may result in changes to resources that cannot be undone. Testing a method with the API Gateway console is the same as calling the method outside of the API Gateway console. For example, if you use the API Gateway console to call a method that deletes an API's resources, if the method call is successful, the API's resources will be deleted.

2. In the box that contains the name of the API for the method, choose Resources.
3. In the Resources pane, choose the method you want to test.
4. In the Method Execution pane, in the Client box, choose TEST. Type values in any of the displayed boxes (such as Query Strings, Headers, and Request Body). The console includes these values in the method request in default application/json form.

   For additional options you may need to specify, contact the API owner.

5. Choose Test. The following information will be displayed:

   - **Request** is the resource's path that was called for the method.
   - **Status** is the response's HTTP status code.
   - **Latency** is the time between the receipt of the request from the caller and the returned response.
   - **Response Body** is the HTTP response body.
   - **Response Headers** are the HTTP response headers.

   **Tip**
Depending on the mapping, the HTTP status code, response body, and response headers may be different from those sent from the Lambda function, HTTP proxy, or AWS service proxy.
• **Logs** are the simulated Amazon CloudWatch Logs entries that would have been written if this method were called outside of the API Gateway console.

**Note**
Although the CloudWatch Logs entries are simulated, the results of the method call are real.

In addition to using the API Gateway console, you can use AWS CLI or an AWS SDK for API Gateway to test invoking a method. To do so using AWS CLI, see test-involve-method.

# Use Postman to Call a REST API

The Postman app is a convenient tool to test a REST API in API Gateway. The following instructions walk you through the essential steps of using the Postman app to call an API. For more information, see the Postman help.

1. Launch Postman.
2. Enter the endpoint URL of a request in the address bar and choose the appropriate HTTP method from the drop-down list to the left of the address bar.
3. If required, choose the **Authorization** tab. Choose **AWS Signature** for the authorization **Type**. Enter your AWS IAM user’s access key ID in the **AccessKey** input field. Enter your IAM user secret key in **SecretKey**. Specify an appropriate AWS region that matches the region specified in the invocation URL. Enter `execute-api` in **Service Name**.
4. Choose the **Headers** tab. Optionally, delete any existing headers. This can clear any stale settings that may cause errors. Add any required custom headers. For example, if API keys are enabled, you can set the `x-api-key:{api_key}` name/value pair here.
5. Choose **Send** to submit the request and receive a response.

For an example of using Postman, see Call an API with API Gateway Lambda Authorizers (p. 392).

# Call REST API through Generated SDKs

This section shows how to call an API through a generated SDK in a client app written in Java, Java for Android, JavaScript, Ruby, Objective-C and Swift.

**Topics**
- Use a Java SDK Generated by API Gateway for a REST API (p. 538)
- Use an Android SDK Generated by API Gateway for a REST API (p. 542)
- Use a JavaScript SDK Generated by API Gateway for a REST API (p. 543)
- Use a Ruby SDK Generated by API Gateway for a REST API (p. 545)
- Use iOS SDK Generated by API Gateway for a REST API in Objective-C or Swift (p. 548)

## Use a Java SDK Generated by API Gateway for a REST API

In this section, we outline the steps to use a Java SDK generated by API Gateway for a REST API, by using the Simple Calculator (p. 531) API as an example. Before proceeding, you must complete the steps in Generate SDKs for an API Using the API Gateway Console (p. 521).

**To install and use a Java SDK generated by API Gateway**

1. Extract the contents of the API Gateway-generated .zip file that you downloaded earlier.
2. Download and install [Apache Maven](https://maven.apache.org/) (must be version 3.5 or later).
3. Download and install JDK 8.
4. Set the `JAVA_HOME` environment variable.
5. Go to the unzipped SDK folder where the pom.xml file is located. This folder is generated—code by default. Run the `mvn install` command to install the compiled artifact files to your local Maven repository. This creates a target folder containing the compiled SDK library.
6. Type the following command in an empty directory to create a client project stub to call the API using the installed SDK library.

```
mvn -B archetype:generate \
-DarchetypeGroupId=org.apache.maven.archetypes \
-DgroupId=examples.aws.apig.simpleCalc.sdk.app \
-DartifactId=SimpleCalc-sdkClient
```

**Note**

The separator `\` in the preceding command is included for readability. The whole command should be on a single line without the separator.

This command creates an application stub. The application stub contains a `pom.xml` file and an `src` folder under the project's root directory (`SimpleCalc-sdkClient` in the preceding command). Initially, there are two source files: `src/main/java/{package-path}/App.java` and `src/test/java/{package-path}/AppTest.java`. In this example, `{package-path}` is `examples/aws/apig/simpleCalc/sdk/app`. This package path is derived from the DarchetypeGroupId value. You can use the `App.java` file as a template for your client application, and you can add others in the same folder if needed. You can use the `AppTest.java` file as a unit test template for your application, and you can add other test code files to the same test folder as needed.

7. Update the package dependencies in the generated `pom.xml` file to the following, substituting your project's `groupId`, `artifactId`, `version`, and `name` properties, if necessary:

```xml
<dependencies>
  <dependency>
    <groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-core</artifactId>
    <version>1.11.94</version>
  </dependency>
  <dependency>
    <groupId>my-apig-api-examples</groupId>
    <artifactId>simple-calc-sdk</artifactId>
    <version>1.0.0</version>
  </dependency>
  <dependency>
    <groupId>junit</groupId>
    <artifactId>junit</artifactId>
    <version>4.12</version>
    <scope>test</scope>
  </dependency>
  <dependency>
    <groupId>commons-io</groupId>
    <artifactId>commons-io</artifactId>
    <version>2.9</version>
  </dependency>
</dependencies>
```
Note
When a newer version of dependent artifact of aws-java-sdk-core is incompatible with
the version specified above (1.11.94), you must update the <version> tag to the new
version.

8. Next, we show how to call the API using the SDK by calling the getABOp(GetABOpRequest
req), getApiRoot(GetApiRootRequest req), and postApiRoot(PostApiRootRequest
req) methods of the SDK. These methods correspond to the GET /{a}/{b}/{op}, GET /?
a={x}&b={y}&op={operator}, and POST / methods, with a payload of {"a": x, "b": y,
"op": "operator"} API requests, respectively.

Update the App.java file as follows:

```java
package examples.aws.apig.simpleCalc.sdk.app;

import java.io.IOException;

import com.amazonaws.opensdk.config.ConnectionConfiguration;
import com.amazonaws.opensdk.config.TimeoutConfiguration;

import examples.aws.apig.simpleCalc.sdk.*;
import examples.aws.apig.simpleCalc.sdk.model.*;
import examples.aws.apig.simpleCalc.sdk.SimpleCalcSdk.*;

public class App
{
    SimpleCalcSdk sdkClient;

    public App() {
        initSdk();
    }

    // The configuration settings are for illustration purposes and may not be a
    // recommended best practice.
    private void initSdk() {
        sdkClient = SimpleCalcSdk.builder()
            .connectionConfiguration(
                new ConnectionConfiguration()
                    .maxConnections(100)
                    .connectionMaxIdleMillis(1000)
            )
            .timeoutConfiguration(
                new TimeoutConfiguration()
                    .httpRequestTimeout(3000)
                    .totalExecutionTimeout(10000)
            );
    }
}
```
```java
.socketTimeout(2000))
        .build();
    }
    // Calling shutdown is not necessary unless you want to exert explicit control of
    // this resource.
    public void shutdown() {
        sdkClient.shutdown();
    }

    // GetABOpResult getABOp(GetABOpRequest getABOpRequest)
    public Output getResultWithPathParameters(String x, String y, String operator) {
        operator = operator.equals("+") ? "add" : operator;
        operator = operator.equals("") ? "div" : operator;

        GetABOpResult abopResult = sdkClient.getABOp(new
            GetABOpRequest().a(x).b(y).op(operator));
        return abopResult.getResult().getOutput();
    }

    public Output getResultWithQueryParameters(String a, String b, String op) {
        GetApiRootResult rootResult = sdkClient.getApiRoot(new
            GetApiRootRequest().a(a).b(b).op(op));
        return rootResult.getResult().getOutput();
    }

    public Output geResultByPostInputBody(Double x, Double y, String o) {
        PostApiRootResult postResult = sdkClient.postApiRoot(
            new PostApiRootRequest().input(new Input().a(x).b(y).op(o)));
        return postResult.getResult().getOutput();
    }

    public static void main( String[] args ) {
        System.out.println( "Simple calc" );
        // to begin
        App calc = new App();
        // call the SimpleCalc API
        Output res = calc.getResultWithPathParameters("1", "2", "+");
        System.out.printf("GET /1/2/+ : %s\n", res.getC());

        // Use the type query parameter
        res = calc.getResultWithQueryParameters("1", "2", "++");
        System.out.printf("GET ?a=1&b=2&op=++ : %s\n", res.getC());

        // Call POST with an Input body.
        res = calc.geResultByPostInputBody(1.0, 2.0, "*");
        System.out.printf("PUT /\n\n{"a":1,"b":2,"op":"*"}\n %s\n", res.getC());
    }
}
```

In the preceding example, the configuration settings used to instantiate the SDK client are
for illustration purposes and are not necessarily recommended best practice. Also, calling
`sdkClient.shutdown()` is optional, especially if you need precise control on when to free up
resources.

We have shown the essential patterns to call an API using a Java SDK. You can extend the instructions to
calling other API methods.
Use an Android SDK Generated by API Gateway for a REST API

In this section, we will outline the steps to use an Android SDK generated by API Gateway for a REST API. Before proceeding further, you must have already completed the steps in Generate SDKs for an API Using the API Gateway Console (p. 521).

Note
The generated SDK is not compatible with Android 4.4 and earlier. For more information, see the section called “Important Notes” (p. 692).

To install and use an Android SDK Generated by API Gateway

1. Extract the contents of the API Gateway-generated .zip file that you downloaded earlier.
2. Download and install Apache Maven (preferably version 3.x).
3. Download and install JDK 8.
4. Set the JAVA_HOME environment variable.
5. Run the maven install command to install the compiled artifact files to your local Maven repository. This creates a target folder containing the compiled SDK library.
6. Copy the SDK file (the name of which is derived from the Artifact Id and Artifact Version you specified when generating the SDK, e.g., simple-calcsdk-1.0.0.jar) from the target folder, along with all of the other libraries from the target/lib folder, into your project's lib folder.

If you use Android Studio, create a libs folder under your client app module and copy the required .jar file into this folder. Verify that the dependencies section in the module's gradle file contains the following.

```
compile fileTree(include: ['*.jar'], dir: 'libs')
compile fileTree(include: ['*.jar'], dir: 'app/libs')
```

Make sure no duplicated .jar files are declared.
7. Use the ApiClientFactory class to initialize the API Gateway-generated SDK. For example:

```java
ApiClientFactory factory = new ApiClientFactory();

// Create an instance of your SDK. Here, 'SimpleCalcClient.java' is the compiled java class for the SDK generated by API Gateway.
final SimpleCalcClient client = factory.build(SimpleCalcClient.class);

// Invoke a method:
// For the 'GET /?a=1&b=2&op=+' method exposed by the API, you can invoke it by calling the following SDK method:
Result output = client.rootGet("1", "2", "+");

// where the Result class of the SDK corresponds to the Result model of the API.

// For the 'GET /{a}/{b}/{op}' method exposed by the API, you can call the following SDK method to invoke the request,
Result output = client.aBOpGet(a, b, c);

// where a, b, c can be "1", "2", "add", respectively.

// For the following API method:
// POST /
// host: ...
// Content-Type: application/json
// ```
//        { "a": 1, "b": 2, "op": "+" }
// you can call invoke it by calling the rootPost method of the SDK as follows:
Input body = new Input();
input.a=1;
input.b=2;
input.op="*";
Result output = client.rootPost(body);
// where the Input class of the SDK corresponds to the Input model of the API.

// Parse the result:
//     If the 'Result' object is { "a": 1, "b": 2, "op": "add", "c":3"}, you retrieve
// the result 'c') as
String result=output.c;

8. To use an Amazon Cognito credentials provider to authorize calls to your API, use the
ApiClientFactory class to pass a set of AWS credentials by using the SDK generated by API
Gateway, as shown in the following example.

// Use CognitoCachingCredentialsProvider to provide AWS credentials
// for the ApiClientFactory
AWSCredentialsProvider credentialsProvider = new CognitoCachingCredentialsProvider(
    context,          // activity context
    "identityPoolId", // Cognito identity pool id
    Regions.US_EAST_1 // region of Cognito identity pool
);

ApiClientFactory factory = new ApiClientFactory()
    .credentialsProvider(credentialsProvider);

9. To set an API key by using the API Gateway-generated SDK, use code similar to the following.

ApiClientFactory factory = new ApiClientFactory()
    .apiKey("YOUR_API_KEY");

Use a JavaScript SDK Generated by API Gateway for a REST API

Note
These instructions assume you have already completed the instructions in Generate SDKs for an
API Using the API Gateway Console (p. 521).

Important
If your API only has ANY methods defined, the generated SDK package will not contain an
apigClient.js file, and you will need to define the ANY methods yourself.

To install, initiate and call a JavaScript SDK generated by API Gateway for a REST API

1. Extract the contents of the API Gateway-generated .zip file you downloaded earlier.
2. Enable cross-origin resource sharing (CORS) for all of the methods the SDK generated by API
   Gateway will call. For instructions, see Enable CORS for a REST API Resource (p. 405).
3. In your web page, include references to the following scripts.
4. In your code, initialize the SDK generated by API Gateway by using code similar to the following.

```javascript
var apigClient = apigClientFactory.newClient();
```

To initialize the SDK generated by API Gateway with AWS credentials, use code similar to the following. If you use AWS credentials, all requests to the API will be signed.

```javascript
var apigClient = apigClientFactory.newClient({
  accessKey: 'ACCESS_KEY',
  secretKey: 'SECRET_KEY',
});
```

To use an API key with the SDK generated by API Gateway, pass the API key as a parameter to the Factory object by using code similar to the following. If you use an API key, it is specified as part of the `x-api-key` header and all requests to the API will be signed. This means you must set the appropriate CORS Accept headers for each request.

```javascript
var apigClient = apigClientFactory.newClient({
  apiKey: 'API_KEY'
});
```

5. Call the API methods in API Gateway by using code similar to the following. Each call returns a promise with a success and failure callbacks.

```javascript
var params = {
  // This is where any modeled request parameters should be added.
  // The key is the parameter name, as it is defined in the API in API Gateway.
  param0: '',
  param1: ''
};

var body = {
  // This is where you define the body of the request,
};

var additionalParams = {
  // If there are any unmodeled query parameters or headers that must be
  // sent with the request, add them here.
  headers: {
    param0: '',
    param1: ''
  },
  queryParams: {
    param0: '',
    param1: ''
  }
};
```
Here, the `methodName` is constructed from the method request’s resource path and the HTTP verb. For the SimpleCalc API, the SDK methods for the API methods of

1. GET /?a=...&b=...&op=...
2. POST /
   
   { "a": ..., "b": ..., "op": ... }
3. GET /{a}/{b}/{op}

the corresponding SDK methods are as follows:

1. rootGet(params);      // where params={"a": ..., "b": ..., "op": ...} is resolved to
   the query parameters
2. rootPost(null, body); // where body={"a": ..., "b": ..., "op": ...}
3. aBOpGet(params);      // where params={"a": ..., "b": ..., "op": ...} is resolved to
   the path parameters

Use a Ruby SDK Generated by API Gateway for a REST API

**Note**
These instructions assume you already completed the instructions in Generate SDKs for an API Using the API Gateway Console (p. 521).

To install, instantiate, and call a Ruby SDK generated by API Gateway for a REST API

1. Unzip the downloaded Ruby SDK file. The generated SDK source is shown as follows.
2. Build a Ruby Gem from the generated SDK source, using the following shell commands in a terminal window:

```bash
# change to /simplecalc-sdk directory
cd simplecalc-sdk

# build the generated gem
gem build simplecalc-sdk.gemspec
```

After this, `simplecalc-sdk-1.0.0.gem` becomes available.

3. Install the gem:

```bash
gem install simplecalc-sdk-1.0.0.gem
```

4. Create a client application. Instantiate and initialize the Ruby SDK client in the app:

```ruby
require 'simplecalc-sdk'
client = SimpleCalc::Client.new(
  http_wire_trace: true,
  retry_limit: 5,
  http_read_timeout: 50
)
```

If the API has authorization of the `AWS_IAM` type is configured, you can include the caller’s AWS credentials by supplying `accessKey` and `secretKey` during the initialization:

```ruby
require 'pet-sdk'
```
5. Make API calls through the SDK in the app.

**Tip**
If you are not familiar with the SDK method call conventions, you can review the `client.rb` file in the generated SDK `lib` folder. The folder contains documentation of each supported API method call.

To discover supported operations:

```ruby
# to show supported operations:
puts client.operation_names
```

This results in the following display, corresponding to the API methods of `GET /?a={.}&b={.}&op={.}` and `POST /`, plus a payload of the `{a:"...", b:"...", op:"..."}` format, respectively:

```
[:get_api_root, :get_ab_op, :post_api_root]
```

To invoke the `GET /?a=1&b=2&op=+` API method, call the following the Ruby SDK method:

```ruby
resp = client.get_api_root({a:"1", b:"2", op:"+"})
```

To invoke the `POST /` API method with a payload of `{a: "1", b: "2", "op": "+"}`, call the following Ruby SDK method:

```ruby
resp = client.post_api_root(input: {a:"1", b:"2", op:"+"})
```

To invoke the `GET /1/2/+` API method, call the following Ruby SDK method:

```ruby
resp = client.get_ab_op({a:"1", b:"2", op:"+"})
```

The successful SDK method calls return the following response:

```json
resp : {
  result: {
    input: {
      a: 1,
      b: 2,
      op: "+"
    },
    output: {
      c: 3
    }
  }
}
```
Use iOS SDK Generated by API Gateway for a REST API in Objective-C or Swift

In this tutorial, we will show how to use an iOS SDK generated by API Gateway for a REST API in an Objective-C or Swift app to call the underlying API. We will use the SimpleCalc API (p. 527) as an example to illustrate the following topics:

- How to install the required AWS Mobile SDK components into your Xcode project
- How to create the API client object before calling the API's methods
- How to call the API methods through the corresponding SDK methods on the API client object
- How to prepare a method input and parse its result using the corresponding model classes of the SDK

Topics
- Use Generated iOS SDK (Objective-C) to Call API (p. 548)
- Use Generated iOS SDK (Swift) to Call API (p. 552)

Use Generated iOS SDK (Objective-C) to Call API

Before beginning the following procedure, you must complete the steps in Generate SDKs for an API Using the API Gateway Console (p. 521) for iOS in Objective-C and download the .zip file of the generated SDK.

Install the AWS Mobile SDK and an iOS SDK generated by API Gateway in an Objective-C Project

The following procedure describes how to install the SDK.

To install and use an iOS SDK generated by API Gateway in Objective-C

1. Extract the contents of the API Gateway-generated .zip file you downloaded earlier. Using the SimpleCalc API (p. 527), you may want to rename the unzipped SDK folder to something like `sdk_objc_simple_calc`. In this SDK folder there is a `README.md` file and a `Podfile` file. The `README.md` file contains the instructions to install and use the SDK. This tutorial provides details about these instructions. The installation leverages CocoaPods to import required API Gateway libraries and other dependent AWS Mobile SDK components. You must update the `Podfile` to import the SDKs into your app's Xcode project. The unarchived SDK folder also contains a `generated-src` folder that contains the source code of the generated SDK of your API.

2. Launch Xcode and create a new iOS Objective-C project. Make a note of the project's target. You will need to set it in the Podfile.

3. To import the AWS Mobile SDK for iOS into the Xcode project by using CocoaPods, do the following:
   a. Install CocoaPods by running the following command in a terminal window:
b. Copy the Podfile file from the extracted SDK folder into the same directory containing your Xcode project file. Replace the following block:

```ruby
target '<YourXcodeTarget>' do
  pod 'AWSAPIGateway', ' ~> 2.4.7'
end
```

with your project's target name:

```ruby
target 'app_objc_simple_calc' do
  pod 'AWSAPIGateway', ' ~> 2.4.7'
end
```

If your Xcode project already contains a file named Podfile, add the following line of code to it:

```ruby
pod 'AWSAPIGateway', ' ~> 2.4.7'
```

c. Open a terminal window and run the following command:

```bash
pod install
```

This installs the API Gateway component and other dependent AWS Mobile SDK components.
d. Close the Xcode project and then open the .xcworkspace file to relaunch Xcode.
e. Add all of the .h and .m files from the extracted SDK's generated-src directory into your Xcode project.
To import the AWS Mobile SDK for iOS Objective-C into your project by explicitly downloading AWS Mobile SDK or using Carthage, follow the instructions in the README.md file. Be sure to use only one of these options to import the AWS Mobile SDK.

Call API Methods Using the iOS SDK generated by API Gateway in an Objective-C Project

When you generated the SDK with the prefix of SIMPLE_CALC for this SimpleCalc API (p. 527) with two models for input (Input) and output (Result) of the methods, in the SDK, the resulting API client class becomes SIMPLE_CALCSimpleCalcClient and the corresponding data classes are SIMPLE_CALCInput and SIMPLE_CALCRResult, respectively. The API requests and responses are mapped to the SDK methods as follows:

- The API request of

  ```
  GET /?a=...&b=...&op=...
  ```

  becomes the SDK method of

  ```
  (AWSTask *)rootGet:(NSString *)op a:(NSString *)a b:(NSString *)b
  ```

  The AWSTask.result property is of the SIMPLE_CALCRResult type if the Result model was added to the method response. Otherwise, the property is of the NSDictionary type.

- This API request of

  ```
  POST /
  {
  "a": "Number",
  "b": "Number",
  "op": "String"
  }
  ```

  becomes the SDK method of

  ```
  (AWSTask *)rootPost:(SIMPLE_CALCInput *)body
  ```

- The API request of

  ```
  GET /{a}/{b}/{op}
  ```

  becomes the SDK method of

  ```
  (AWSTask *)aBOpGet:(NSString *)a b:(NSString *)b op:(NSString *)op
  ```

  The following procedure describes how to call the API methods in Objective-C app source code; for example, as part of the viewDidLoad delegate in a ViewController.m file.

To call the API through the iOS SDK generated by API Gateway

1. Import the API client class header file to make the API client class callable in the app:
#import "SIMPLE_CALCSimpleCalc.h"

The #import statement also imports SIMPLE_CALCInput.h and SIMPLE_CALCRetult.h for the two model classes.

2. Instantiate the API client class:

   SIMPLE_CALCSimpleCalcClient *apiInstance = [SIMPLE_CALCSimpleCalcClient defaultClient];

To use Amazon Cognito with the API, set the defaultServiceConfiguration property on the default AWSServiceManager object, as shown in the following, before calling the defaultClient method to create the API client object (shown in the preceding example):

   AWSCognitoCredentialsProvider *creds = [[AWSCognitoCredentialsProvider alloc]
                                          initWithRegionType:AWSRegionUSEast1
                                          identityPoolId:your_cognito_pool_id];
   AWSServiceConfiguration *configuration = [[AWSServiceConfiguration alloc]
                                          initWithRegion:AWSRegionUSEast1
                                          credentialsProvider:creds];
   AWSServiceManager.defaultServiceManager.defaultServiceConfiguration = configuration;

3. Call the GET /?a=1&b=2&op=+ method to perform 1+2:

   [[apiInstance rootGet: @"+" a:@"1" b:@"2"] continueWithBlock:^id _Nullable(AWSTask * _Nonnull task) {
      _textField1.text = [self handleApiResponse:task];
      return nil;
   }];

where the helper function handleApiResponse:task formats the result as a string to be displayed in a text field (_textField1).

4. Call the POST / with a payload to perform 1-2:

   SIMPLE_CALCInput *input = [[SIMPLE_CALCInput alloc] init];
   input.a = [NSNumber numberWithInt:1];
   input.b = [NSNumber numberWithInt:2];
   input.op = @"-";
   [[apiInstance rootPost:input] continueWithBlock:^id _Nullable(AWSTask * _Nonnull task) {
      _textField2.text = [self handleApiResponse:task];
      return nil;
   }];

The resulting display is 1 + 2 = 3.

4. Call the POST / with a payload to perform 1-2:

   SIMPLE_CALCInput *input = [[SIMPLE_CALCInput alloc] init];
   input.a = [NSNumber numberWithInt:1];
   input.b = [NSNumber numberWithInt:2];
   input.op = @"-";
   [[apiInstance rootPost:input] continueWithBlock:^id _Nullable(AWSTask * _Nonnull task) {
      _textField2.text = [self handleApiResponse:task];
      return nil;
   }];

The resulting display is 1 - 2 = -1.

5. Call the GET /{a}/{b}/{op} to perform 1/2:

   //...
The resulting display is $1 \text{ div } 2 = 0.5$. Here, \text{div} is used in place of / because the simple Lambda function (p. 525) in the backend does not handle URL encoded path variables.

Use Generated iOS SDK (Swift) to Call API

Before beginning the following procedure, you must complete the steps in Generate SDKs for an API Using the API Gateway Console (p. 521) for iOS in Swift and download the .zip file of the generated SDK.

Topics

- Install AWS Mobile SDK and API Gateway-Generated SDK in a Swift Project (p. 552)
- Call API methods through the iOS SDK generated by API Gateway in a Swift Project (p. 554)

Install AWS Mobile SDK and API Gateway-Generated SDK in a Swift Project

The following procedure describes how to install the SDK.

To install and use an iOS SDK generated by API Gateway in Swift

1. Extract the contents of the API Gateway-generated .zip file you downloaded earlier. Using the SimpleCalc API (p. 527), you may want to rename the unzipped SDK folder to something like `sdk_swift_simple_calc`. In this SDK folder there is a README.md file and a Podfile file. The README.md file contains the instructions to install and use the SDK. This tutorial provides details about these instructions. The installation leverages CocoaPods to import required AWS Mobile SDK components. You must update the Podfile to import the SDKs into your Swift app's Xcode project. The unarchived SDK folder also contains a generated-src folder that contains the source code of the generated SDK of your API.

2. Launch Xcode and create a new iOS Swift project. Make a note of the project's target. You will need to set it in the Podfile.

3. To import the required AWS Mobile SDK components into the Xcode project by using CocoaPods, do the following:
   a. If it is not installed, install CocoaPods by running the following command in a terminal window:
b. Copy the Podfile file from the extracted SDK folder into the same directory containing your Xcode project file. Replace the following block:

```ruby
target '<YourXcodeTarget>' do
  pod 'AWSAPIGateway', '~> 2.4.7'
end
```

with your project's target name as shown:

```ruby
target 'app_swift_simple_calc' do
  pod 'AWSAPIGateway', '~> 2.4.7'
end
```

If your Xcode project already contains a Podfile with the correct target, you can simply add the following line of code to the do ... end loop:

```ruby
pod 'AWSAPIGateway', '~> 2.4.7'
```

c. Open a terminal window and run the following command in the app directory:

```bash
pod install
```

This installs the API Gateway component and any dependent AWS Mobile SDK components into the app's project.

d. Close the Xcode project and then open the *.xcworkspace file to relaunch Xcode.

e. Add all of the SDK's header files (.h) and Swift source code files (.swift) from the extracted generated-src directory to your Xcode project.

f. To enable calling the Objective-C libraries of the AWS Mobile SDK from your Swift code project, set the Bridging_Header.h file path on the Objective-C Bridging Header property under the Swift Compiler - General setting of your Xcode project configuration:
Tip
You can type `bridging` in the search box of Xcode to locate the Objective-C Bridging Header property.

g. Build the Xcode project to verify that it is properly configured before proceeding further. If your Xcode uses a more recent version of Swift than the one supported for the AWS Mobile SDK, you will get Swift compiler errors. In this case, set the Use Legacy Swift Language Version property to Yes under the Swift Compiler - Version setting:

To import the AWS Mobile SDK for iOS in Swift into your project by explicitly downloading the AWS Mobile SDK or using Carthage, follow the instructions in the README.md file that comes with the SDK package. Be sure to use only one of these options to import the AWS Mobile SDK.

Call API methods through the iOS SDK generated by API Gateway in a Swift Project

When you generated the SDK with the prefix of SIMPLE_CALC for this SimpleCalc API (p. 527) with two models to describe the input (Input) and output (Result) of the API’s requests and responses, in the SDK, the resulting API client class becomes SIMPLE_CALCSimpleCalcClient and the corresponding data classes are SIMPLE_CALCInput and SIMPLE_CALCResult, respectively. The API requests and responses are mapped to the SDK methods as follows:

- The API request of

  ```
  GET /?a=...&b=...&op=...
  ```

  becomes the SDK method of

  ```
  public func rootGet(op: String?, a: String?, b: String?) -> AWSTask
  ```
The AWSTask.result property is of the SIMPLE_CALCResult type if the Result model was added to the method response. Otherwise, it is of the NSDictionary type.

- This API request of

```swift
POST /
{
    "a": "Number",
    "b": "Number",
    "op": "String"
}
```

becomes the SDK method of

```swift
public func rootPost(body: SIMPLE_CALCInput) -> AWSTask
```

- The API request of

```swift
GET /{a}/{b}/{op}
```

becomes the SDK method of

```swift
public func aBOpGet(a: String, b: String, op: String) -> AWSTask
```

The following procedure describes how to call the API methods in Swift app source code; for example, as part of the viewDidLoad() delegate in a ViewController.m file.

**To call the API through the iOS SDK generated by API Gateway**

1. Instantiate the API client class:

   ```swift
   let client = SIMPLE_CALCSimpleCalcClient.defaultClient()
   ```

To use Amazon Cognito with the API, set a default AWS service configuration (shown following) before getting the defaultClient method (shown previously):

```swift
let credentialsProvider = AWSCognitoCredentialsProvider(regionType: AWSRegionType.USEast1, identityPoolId: "my_pool_id")
let configuration = AWSServiceConfiguration(region: AWSRegionType.USEast1, credentialsProvider: credentialsProvider)
AWSServiceManager.defaultServiceManager().defaultServiceConfiguration = configuration
```

2. Call the GET /?a=1&b=2&op=+ method to perform 1+2:

   ```swift
   client.rootGet("+", a: "1", b: "2").continueWithBlock {(task: AWSTask) -> AnyObject? in
       self.showResult(task)
       return nil
   }
   ```

   where the helper function `self.showResult(task)` prints the result or error to the console; for example:

   ```swift
   func showResult(task: AWSTask) {
   ```
In a production app, you can display the result or error in a text field. The resulting display is \(1 + 2 = 3\).

3. Call the `POST /` with a payload to perform \(1 - 2\):

```swift
let body = SIMPLE_CALCInput()
body.a=1
body.b=2
body.op="-"
client.rootPost(body).continueWithBlock {(task: AWSTask) -> AnyObject? in
    self.showResult(task)
    return nil
}
```

The resultant display is \(1 - 2 = -1\).

4. Call the `GET /{a}/{b}/{op}` to perform \(1/2\):

```swift
client.aBOpGet("1", b:"2", op:"div").continueWithBlock {(task: AWSTask) -> AnyObject? in
    self.showResult(task)
    return nil
}
```

The resulting display is \(1 \div 2 = 0.5\). Here, \(\text{div}\) is used in place of \(\div\) because the simple Lambda function (p. 525) in the backend does not handle URL encoded path variables.

---

**Call REST API through AWS Amplify JavaScript Library**

The AWS Amplify JavaScript Library can be used for making API requests to an API Gateway REST API. For more information, see the instructions in the AWS Amplify API Guide.

**How to Invoke a Private API**

Once you have deployed a private API (p. 194), you can access it via private DNS (if you've enabled private DNS naming) and via public DNS.

To get the DNS names for your private API, do the following:

1. Log in to the Amazon VPC console at [https://console.aws.amazon.com/vpc/](https://console.aws.amazon.com/vpc/).
2. In the left navigation pane, choose **Endpoints** and then choose your interface VPC endpoint for API Gateway.
3. In the Details pane, you’ll see 5 values in the DNS names field. The first 3 are the public DNS names for your API. The other 2 are the private DNS names for it.

## Invoking Your Private API Using Private DNS Names

If you’ve enabled private DNS, you can access your private API using the private DNS names as follows:

```
{restapi-id}.execute-api.{region}.amazonaws.com
```

The base URL to invoke the API is in the following format:

```
https://{restapi-id}.execute-api.{region}.amazonaws.com/{stage}
```

For example, assuming you set up the GET /pets and GET /pets/{petId} methods in this example, and assuming that your rest API ID was 0qzs2sy7bh and your region was us-west-2, you could test your API by typing the following URLs in a browser:

```
https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets
```

and

```
https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets/1
```

Alternatively, you could use the following cURL commands:

```
curl -X GET https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets
```

and

```
curl -X GET https://0qzs2sy7bh.execute-api.us-west-2.amazonaws.com/test/pets/2
```

## Invoking Your Private API Using Endpoint-Specific Public DNS Hostnames

You can access your private API using endpoint-specific DNS hostnames. These are public DNS hostnames containing the VPC endpoint ID or API ID for your private API.

The base URL is in the following format:

```
https://{public-dns-hostname}.execute-api.{region}.vpce.amazonaws.com/{stage}
```

For example, assuming you set up the GET /pets and GET /pets/{petId} methods in this example, and assuming that your API’s API ID was 0qzs2sy7bh, its public DNS hostname was vpce-0c1308d7312217cd7-01234567, and your region was us-west-2, you could test your API via its VPCE ID by using the Host header in a cURL command, as in the following example:

```
curl -v https://vpce-0c1308d7312217cd7-01234567.execute-api.us-east-1.vpce.amazonaws.com/test/pets -H 'Host: 0qzs2sy7bh.execute-api.us-west-2.amazonaws.com'
```
Alternatively, you can access your private API via its API ID by using the `x-apigw-api-id` header in a cURL command in the following format:

```
curl -v https://{vpce-id}.execute-api.{region}.vpce.amazonaws.com/test -H'x-apigw-api-id:{api-id}'
```

### Accessing Your Private API Using AWS Direct Connect

You can also use AWS Direct Connect to establish a dedicated private connection from an on-premises network to Amazon VPC and access your private API endpoint over that connection by using public DNS names.

You cannot use private DNS names to access your private API from an on-premises network.

## Tracing, Logging, and Monitoring an API Gateway API

AWS X-Ray, AWS CloudTrail, and Amazon CloudWatch are tools that Amazon API Gateway developers can use to trace, log, and monitor API execution and management operations.

AWS X-Ray is an AWS service that allows you to trace latency issues with your Amazon API Gateway APIs. X-Ray collects metadata from the API Gateway service and any downstream services that make up your API. X-Ray uses this metadata to generate a detailed service graph that illustrates latency spikes and other issues that impact the performance of your API.

Amazon CloudWatch logs API execution operations, which are calls that an API customer or client application makes against the API Gateway `execute-api` component. CloudWatch metrics include statistics about caching, latency, and detected errors. You can inspect CloudWatch logs to troubleshoot your API implementation or execution using the API dashboard in the API Gateway console or using the CloudWatch console.

AWS CloudTrail logs API Gateway API management operations, which are REST API calls that an API developer or owner makes against the API Gateway `apigateway` component. You can use CloudTrail logs to troubleshoot API creation, deployment, and updates. You can also use Amazon CloudWatch to monitor CloudTrail logs.

### Topics

- Trace API Gateway API Execution with AWS X-Ray (p. 558)
- Log Calls to Amazon API Gateway APIs with AWS CloudTrail (p. 568)
- Monitor API Execution with Amazon CloudWatch (p. 569)

### Trace API Gateway API Execution with AWS X-Ray

You can use AWS X-Ray to trace and analyze user requests as they travel through your Amazon API Gateway APIs to the underlying services. API Gateway supports AWS X-Ray tracing for all API Gateway endpoint types: regional, edge-optimized, and private. You can use AWS X-Ray with Amazon API Gateway in all regions where X-Ray is available.

X-Ray gives you an end-to-end view of an entire request, so you can analyze latencies in your APIs and their backend services. You can use an X-Ray service map to view the latency of an entire request and that of the downstream services that are integrated with X-Ray. And you can configure sampling rules to
tell X-Ray which requests to record, at what sampling rates, according to criteria that you specify. If you call an API Gateway API from a service that's already being traced, API Gateway passes the trace through, even if X-Ray tracing is not enabled on the API.

You can enable X-Ray for an API stage by using the API Gateway management console, or by using the API Gateway API or CLI.

**Topics**
- Setting Up AWS X-Ray with API Gateway (p. 559)
- Using AWS X-Ray Service Maps and Trace Views with API Gateway (p. 561)
- Configuring AWS X-Ray Sampling Rules for API Gateway APIs (p. 564)
- Understanding AWS X-Ray Traces for Amazon API Gateway APIs (p. 566)

### Setting Up AWS X-Ray with API Gateway

In this section you can find detailed information on how to set up AWS X-Ray with API Gateway.

**Topics**
- X-Ray Tracing Modes for API Gateway (p. 559)
- Permissions for X-Ray Tracing (p. 559)
- Enabling X-Ray tracing in the API Gateway console (p. 560)
- Enabling AWS X-Ray Tracing Using the API Gateway CLI (p. 560)

### X-Ray Tracing Modes for API Gateway

The path of a request through your application is tracked with a trace ID. A trace collects all of the segments generated by a single request, typically an HTTP **GET** or **POST** request.

There are two modes of tracing for an API Gateway API:

- **Passive**: This is the default setting if you have not enabled X-Ray tracing on an API stage. This approach means that the API Gateway API is only traced if X-Ray has been enabled on an upstream service.
- **Active**: When an API Gateway API stage has this setting, API Gateway automatically samples API invocation requests, based on the sampling algorithm specified by X-Ray.

When active tracing is enabled on a stage, API Gateway creates a service-linked role in your account, if the role does not exist already. The role is named `AWSServiceRoleForAPIGateway` and will have the `APIGatewayServiceRolePolicy` managed policy attached to it. For more information about service-linked roles, see [Using Service-Linked Roles](#).

**Note**

X-Ray applies a sampling algorithm to ensure that tracing is efficient, while still providing a representative sample of the requests that your API receives. The default sampling algorithm is 1 request per second, with 5 percent of requests sampled past that limit.

You can change the tracing mode for your API by using the API Gateway management console, the API Gateway CLI, or an AWS SDK.

### Permissions for X-Ray Tracing

When you enable X-Ray tracing on a stage, API Gateway creates a service-linked role in your account, if the role does not exist already. The role is named `AWSServiceRoleForAPIGateway` and will have the
APIGatewayServiceRolePolicy managed policy attached to it. For more information about service-linked roles, see Using Service-Linked Roles.

**Enabling X-Ray tracing in the API Gateway console**

You can use the Amazon API Gateway console to enable active tracing on an API stage.

These steps assume that you have already deployed the API to a stage.

2. In the APIs pane, choose the API, and then choose Stages.
3. In the Stages pane, choose the name of the stage.
4. In the Stage Editor pane, choose the Logs/Tracing tab.
5. To enable active X-Ray tracing, choose Enable X-Ray Tracing under X-Ray Tracing.
6. If desired, choose Set X-Ray Sampling Rules and go to the X-Ray console to configure sampling rules (p. 564).

Once you've enabled X-Ray for your API stage, you can use the X-Ray management console to view the traces and service maps.

**Enabling AWS X-Ray Tracing Using the API Gateway CLI**

To use the AWS CLI to enable active X-Ray tracing for an API stage when you create the stage, call the create-stage command as in the following example:

```bash
aws apigateway --endpoint-url {endpoint-url} create-stage \
  --rest-api-id {rest-api-id} \
  --stage-name {stage-name} \
  --deployment-id {deployment-id} \
  --region {region} \
  --tracing-enabled=true
```

Following is example output for a successful invocation:

```json
{
  "tracingEnabled": true,
  "stageName": "{stage-name},
  "cacheClusterEnabled": false,
  "cacheClusterStatus": "NOT_AVAILABLE",
  "deploymentId": "{deployment-id},
  "lastUpdatedDate": 1533849811,
  "createdDate": 1533849811,
  "methodSettings": {}
}
```

To use the AWS CLI to disable active X-Ray tracing for an API stage when you create the stage, call the create-stage command as in the following example:

```bash
aws apigateway --endpoint-url {endpoint-url} create-stage \
  --rest-api-id {rest-api-id} \
  --stage-name {stage-name} \
  --deployment-id {deployment-id} \
  --region {region} \
  --tracing-enabled=false
```
Following is example output for a successful invocation:

```json
{
    "tracingEnabled": false,
    "stageName": "(stage-name),
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "(deployment-id),
    "lastUpdatedDate": 1533849811,
    "createdDate": 1533849811,
    "methodSettings": {}
}
```

To use the AWS CLI to enable active X-Ray tracing for an API that's already been deployed, call the `update-stage` command as follows:

```bash
aws apigateway update-stage          \
   --rest-api-id {rest-api-id}          \
   --stage-name {stage-name}           \
   --patch-operations op=replace,path=/tracingEnabled,value=true
```

To use the AWS CLI to disable active X-Ray tracing for an API that's already been deployed, call the `update-stage` command as in the following example:

```bash
aws apigateway update-stage          \
   --endpoint-url {endpoint-url}       \
   --rest-api-id {rest-api-id}         \
   --stage-name {stage-name}           \
   --region {region}                   \
   --patch-operations op=replace,path=/tracingEnabled,value=false
```

Following is example output for a successful invocation:

```json
{
    "tracingEnabled": false,
    "stageName": "(stage-name),
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "(deployment-id),
    "lastUpdatedDate": 1533850033,
    "createdDate": 1533849811,
    "methodSettings": {} }
```

Once you've enabled X-Ray for your API stage, use the X-Ray CLI to retrieve trace information. For more information, see Using the AWS X-Ray API with the AWS CLI.

### Using AWS X-Ray Service Maps and Trace Views with API Gateway

In this section you can find detailed information on how to use AWS X-Ray service maps and trace views with API Gateway.

For detailed information about service maps and trace views, and how to interpret them, see AWS X-Ray Console.

**Topics**
Example X-Ray Service Map

AWS X-Ray service maps show information about your API and all of its downstream services. When X-Ray is enabled for an API stage in API Gateway, you’ll see a node in the service map containing information about the overall time spent in the API Gateway service. You can get detailed information about the response status and a histogram of the API response time for the selected timeframe. For APIs integrating with AWS services such as AWS Lambda and Amazon DynamoDB, you will see more nodes providing performance metrics related to those services. There will be a service map for each API stage.

The following example shows a service map for the test stage of an API called xray. This API has a Lambda integration with a Lambda authorizer function and a Lambda backend function. The nodes represent the API Gateway service, the Lambda service, and the two Lambda functions.

For a detailed explanation of service map structure, see Viewing the Service Map.

From the service map, you can zoom in to see a trace view of your API stage. The trace will display in-depth information regarding your API, represented as segments and subsegments. For example, the trace for the service map shown above would include segments for the Lambda service and Lambda function. For more information, see Lambda as an AWS X-Ray Trace.

If you choose a node or edge on an X-Ray service map, the X-Ray console shows a latency distribution histogram. You can use a latency histogram to see how long it takes for a service to complete its requests. Following is a histogram of the API Gateway stage named xray/test in the previous service map. For a detailed explanation of latency distribution histograms, see Using Latency Histograms in the AWS X-Ray Console.
Service details

Name: xray/test
Type: AWS::ApiGateway::Stage

Response distribution
Click and drag to select an area to zoom in on or use as a latency filter when viewing traces.

Response status
Choose response statuses to add to the filter when viewing traces.

- OK: 100%
- Error: 0%
- Fault: 0%
- Throttle: 0%
Example X-Ray Trace View

The following diagram shows a trace view generated for the example API described above, with a Lambda backend function and a Lambda authorizer function. A successful API method request is shown with a response code of 200.

For a detailed explanation of trace views, see Viewing Traces.

Configuring AWS X-Ray Sampling Rules for API Gateway APIs

You can use AWS X-Ray console or SDK to configure sampling rules for your Amazon API Gateway API. A sampling rule specifies which requests X-Ray should record for your API. By customizing sampling rules, you can control the amount of data that you record, and modify sampling behavior on the fly without modifying or redeploying your code.

Before you specify your X-Ray sampling rules, read the following topics in the X-Ray Developer Guide:

- Configuring Sampling Rules in the AWS X-Ray Console
- Using Sampling Rules with the X-Ray API

Topics

- X-Ray Sampling Rule Option Values for API Gateway APIs (p. 564)
- X-Ray Sampling Rule Examples (p. 565)

X-Ray Sampling Rule Option Values for API Gateway APIs

The following X-Ray sampling options are relevant for API Gateway. String values can use wildcards to match a single character (?) or zero or more characters (*). For more details, including a detailed explanation of how the Reservoir and Rate settings are used, Configuring Sampling Rules in the AWS X-Ray Console.

- **Rule name** (string) — A unique name for the rule.
- **Priority** (integer between 1 and 9999) — The priority of the sampling rule. Services evaluate rules in ascending order of priority, and make a sampling decision with the first rule that matches.
- **Reservoir** (nonnegative integer) — A fixed number of matching requests to instrument per second, before applying the fixed rate. The reservoir is not used directly by services, but applies to all services using the rule collectively.
• **Rate** (number between 0 and 100) — The percentage of matching requests to instrument, after the reservoir is exhausted.

• **Service name** (string) — API stage name, in the form `{api-name}/(stage-name)`. For example, if you were to deploy the PetStore (p. 42) sample API to a stage named `test`, the **Service name** value to specify in your sampling rule would be `pets/test`.

• **Service type** (string) — For an API Gateway API, either `AWS::ApiGateway::Stage` or `AWS::ApiGateway::*` can be specified.

• **Host** (string) — The hostname from the HTTP host header. Set this to * to match against all hostnames. Or you can specify a full or partial hostname to match, for example, `api.example.com` or `*.example.com`.

• **Resource ARN** (string) — The ARN of the API stage, in the format `arn:aws:execute-api:{region}:{account-id}:{api-id}/(stage-name)`, for example, `arn:aws:execute-api:us-east-1:123456789012:qsxrty/test`.

  The stage name can be obtained from the console or the API Gateway CLI or API. For more information about ARN formats, see the Amazon Web Services General Reference.

• **HTTP method** (string) — The method to be sampled, for example, `GET`.

• **URL path** (string) — This option is not supported for API Gateway.

• (optional) **Attributes** (key and value) — Headers from the original HTTP request, for example, `Connection`, `Content-Length`, or `Content-Type`. Each attribute value can be up to 32 characters long.

**X-Ray Sampling Rule Examples**

**Sampling Rule Example #1**

This rule samples all `GET` requests for the `testxray` API at the `test` stage.

• **Rule name** — `test-sampling`
• **Priority** — 17
• **Reservoir size** — 10
• **Fixed rate** — 10
• **Service name** — `testxray/test`
• **Service type** — `AWS::ApiGateway::Stage`
• **HTTP method** — `GET`
• **Resource ARN** — *
• **Host** — *

**Sampling Rule Example #2**

This rule samples all requests for the `testxray` API at the `prod` stage.

• **Rule name** — `prod-sampling`
• **Priority** — 478
• **Reservoir size** — 1
• **Fixed rate** — 60
• **Service name** — `testxray/prod`
• **Service type** — `AWS::ApiGateway::Stage`
• **HTTP method** — *
Understanding AWS X-Ray Traces for Amazon API Gateway APIs

This section discusses AWS X-Ray trace segments, subsegments, and other trace fields for Amazon API Gateway APIs.

Before you read this section, review the following topics in the X-Ray Developer Guide:

- AWS X-Ray Console
- AWS X-Ray Segment Documents
- X-Ray Concepts

**Topics**

- Examples of Trace Objects for an API Gateway API (p. 566)
- Understanding the Trace (p. 567)

Examples of Trace Objects for an API Gateway API

This section discusses some of the objects you may see in a trace for an API Gateway API.

**Annotations**

Annotations can appear in segments and subsegments. They are used as filtering expressions in sampling rules to filter traces. For more information, see Configuring Sampling Rules in the AWS X-Ray Console.

Following is an example of an `annotations` object, in which an API stage is identified by the API ID and the API stage name:

```json
"annotations": {
  "aws:api_id": "a1b2c3d4e5",
  "aws:api_stage": "dev"
}
```

**AWS Resource Data**

The `aws` object appears only in segments. Following is an example of an `aws` object that matches the Default sampling rule. For an in-depth explanation of sampling rules, see Configuring Sampling Rules in the AWS X-Ray Console.

```json
"aws": {
  "xray": {
    "sampling_rule_name": "Default"
  },
  "api_gateway": {
    "account_id": "123412341234",
    "rest_api_id": "a1b2c3d4e5",
    "stage": "dev",
    "request_id": "a1b2c3d4-a1b2-a1b2-a1b2c3d4e5f6"
  }
}
```
Understanding the Trace

Following is a trace segment for an API Gateway stage. For a detailed explanation of the fields that make up the trace segment, see AWS X-Ray Segment Documents in the AWS X-Ray Developer Guide.

```json
{
    "Document": {
        "id": "a1b2c3d4a1b2c3d4",
        "name": "testxray/dev",
        "start_time": 1533928226.229,
        "end_time": 1533928226.614,
        "metadata": {
            "default": {
                "extended_request_id": "abcde12345abcde=",
                "request_id": "a1b2c3d4-a1b2-a1b2-a1b2c3d4e5f6"
            }
        },
        "http": {
            "request": {
                "url": "https://example.com/dev?
username=demo&message=hellofromdemo/",
                "method": "GET",
                "client_ip": "192.0.2.0",
                "x_forwarded_for": true
            },
            "response": {
                "status": 200,
                "content_length": 0
            }
        },
        "aws": {
            "xray": {
                "sampling_rule_name": "Default"
            },
            "api_gateway": {
                "account_id": "123412341234",
                "rest_api_id": "a1b2c3d4e5",
                "stage": "dev",
                "request_id": "a1b2c3d4-a1b2-a1b2-a1b2c3d4e5f6"
            }
        },
        "annotations": {
            "aws:api_id": "a1b2c3d4e5",
            "aws:api_stage": "dev"
        },
        "trace_id": "1-a1b2c3d4a1b2c3d4a1b2c3d4a1b2c3d4",
        "origin": "AWS::ApiGateway::Stage",
        "resource_arn": "arn:aws:apigateway:us-east-1::/restapis/a1b2c3d4e5/stages/dev",
        "subsegments": [
            {
                "id": "abcdefgh12345678",
                "name": "Lambda",
                "start_time": 1533928226.233,
                "end_time": 1533928226.6130002,
                "http": {
                    "request": {
                        "url": "https://example.com/2015-03-31/functions/
                        "method": "GET"
                    },
                    "response": {
                        "status": 200,
                        "content_length": 62
                    }
                }
            }
        ]
    }
}
```
Log Calls to Amazon API Gateway APIs with AWS CloudTrail

Amazon API Gateway is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in API Gateway. CloudTrail captures all REST API calls for API Gateway as events, including calls from the API Gateway console and from code calls to the API Gateway APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for API Gateway. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to API Gateway, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

API Gateway Information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When activity occurs in Amazon API Gateway, that activity is recorded in a CloudTrail event along with other AWS service events in Event history. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for API Gateway, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all regions. The trail logs events from all regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

All Amazon API Gateway actions are logged by CloudTrail and are documented in the API Gateway V1 and V2 API References (p. 686). For example, calls to create a new API, resource, or method in API Gateway generate entries in CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:
• Whether the request was made with root or IAM user credentials.
• Whether the request was made with temporary security credentials for a role or federated user.
• Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

### Understanding API Gateway Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the API Gateway get resource action:

```json
{
  Records: [
    {
      eventVersion: "1.03",
      userIdentity: {
        type: "Root",
        principalId: "AKIAI44QH8DH8EXAMPLE",
        arn: "arn:aws:iam::123456789012:root",
        accountId: "123456789012",
        accessKeyId: "AKIAIOSFODNN7EXAMPLE",
        sessionContext: {
          attributes: {
            mfaAuthenticated: "false",
            creationDate: "2015-06-16T23:37:58Z"
          }
        }
      },
      eventTime: "2015-06-17T00:47:28Z",
      eventSource: "apigateway.amazonaws.com",
      eventName: "GetResource",
      awsRegion: "us-east-1",
      sourceIPAddress: "203.0.113.11",
      userAgent: "example-user-agent-string",
      requestParameters: {
        restApiId: "3rbEXAMPLE",
        resourceId: "5tfEXAMPLE",
        template: false
      },
      responseElements: null,
      requestID: "6d9c4bfc-148a-11e5-81b6-7577cEXAMPLE",
      eventID: "4d293154-a15b-4c33-9e0a-ff5eeEXAMPLE",
      readOnly: true,
      eventType: "AwsApiCall",
      recipientAccountId: "123456789012"
    },
    ... additional entries ...
  ]
}
```

### Monitor API Execution with Amazon CloudWatch

You can monitor API execution using CloudWatch, which collects and processes raw data from API Gateway into readable, near real-time metrics. These statistics are recorded for a period of 15 months, so
that you can access historical information and gain a better perspective on how your web application or service is performing. By default, API Gateway metric data is automatically sent to CloudWatch in one-minute periods. For more information, see What Is Amazon CloudWatch? in the Amazon CloudWatch User Guide.

The metrics reported by API Gateway provide information that you can analyze in different ways. The list below shows some common uses for the metrics. These are suggestions to get you started, not a comprehensive list.

- Monitor the **IntegrationLatency** metrics to measure the responsiveness of the backend.
- Monitor the **Latency** metrics to measure the overall responsiveness of your API calls.
- Monitor the **CacheHitCount** and **CacheMissCount** metrics to optimize cache capacities to achieve a desired performance.

### Topics
- Amazon API Gateway Dimensions and Metrics (p. 570)
- View CloudWatch Metrics with the API Dashboard in API Gateway (p. 572)
- View API Gateway Metrics in the CloudWatch Console (p. 573)
- View API Gateway Log Events in the CloudWatch Console (p. 573)
- Monitoring Tools in AWS (p. 574)

### Amazon API Gateway Dimensions and Metrics

The metrics and dimensions that API Gateway sends to Amazon CloudWatch are listed below. For more information, see Monitor API Execution with Amazon CloudWatch (p. 569).

#### API Gateway Metrics

Amazon API Gateway sends metric data to CloudWatch every minute.

The **AWS/ApiGateway** namespace includes the following metrics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4XXError</td>
<td>The number of client-side errors captured in a given period. The <strong>Sum</strong> statistic represents this metric, namely, the total count of the 4XXError errors in the given period. The <strong>Average</strong> statistic represents the 4XXError error rate, namely, the total count of the 4XXError errors divided by the total number of requests during the period. The denominator corresponds to the <strong>Count</strong> metric (below).</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>5XXError</td>
<td>The number of server-side errors captured in a given period. The <strong>Sum</strong> statistic represents this metric, namely, the total count of the 5XXError errors in the given period. The <strong>Average</strong> statistic represents the 5XXError error rate, namely, the total count of the 5XXError errors divided by the total number of requests during the period.</td>
</tr>
</tbody>
</table>
### Metric

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CacheHitCount</td>
<td>The number of requests served from the API cache in a given period. The SUM statistic represents this metric, namely, the total count of the cache hits in the given period. The AVERAGE statistic represents the cache hit rate, namely, the total count of the cache hits divided by the total number of requests during the period. The denominator corresponds to the Count metric (below).</td>
</tr>
<tr>
<td>CacheMissCount</td>
<td>The number of requests served from the backend in a given period, when API caching is enabled. The SUM statistic represents this metric, namely, the total count of the cache misses in the given period. The AVERAGE statistic represents the cache miss rate, namely, the total count of the cache misses divided by the total number of requests during the period. The denominator corresponds to the Count metric (below).</td>
</tr>
<tr>
<td>Count</td>
<td>The total number API requests in a given period. The SAMPLECOUNT statistic represents this metric.</td>
</tr>
<tr>
<td>IntegrationLatency</td>
<td>The time between when API Gateway relays a request to the backend and when it receives a response from the backend.</td>
</tr>
<tr>
<td>Latency</td>
<td>The time between when API Gateway receives a request from a client and when it returns a response to the client. The latency includes the integration latency and other API Gateway overhead.</td>
</tr>
</tbody>
</table>

### Dimensions for Metrics

You can use the dimensions in the following table to filter API Gateway metrics.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ApiName</td>
<td>Filters API Gateway metrics for the REST API with the specified API name.</td>
</tr>
</tbody>
</table>
### Dimension | Description
--- | ---
ApiName, Method, Resource, Stage | Filters API Gateway metrics for the API method with the specified API name, stage, resource, and method.

API Gateway will not send these metrics unless you have explicitly enabled detailed CloudWatch metrics. You can do this in the console by selecting **Enable CloudWatch Metrics** under a stage **Settings** tab. Alternatively, you can call the **update-stage** AWS CLI command to update the **metricsEnabled** property to true.

Enabling these metrics will incur additional charges to your account. For pricing information, see Amazon CloudWatch Pricing.

ApiName, Stage | Filters API Gateway metrics for the API stage resource with the specified API name and stage.

### View CloudWatch Metrics with the API Dashboard in API Gateway

You can use the API dashboard in the API Gateway Console to display the CloudWatch metrics of your deployed API in API Gateway. These are shown as a summary of API activity over time.

### Topics
- Prerequisites (p. 572)
- Examine API activities in the Dashboard (p. 572)

### Prerequisites

1. You must have an API created in API Gateway. Follow the instructions in Creating a REST API in Amazon API Gateway (p. 177).
2. You must have the API deployed at least once. Follow the instructions in Deploying a REST API in Amazon API Gateway (p. 494).
3. To get CloudWatch metrics for individual methods, you must have CloudWatch Logs enabled for those methods in a given stage as described in Update Stage Settings (p. 498). Your account will be charged for accessing method-level logs, but not for accessing API- or stage-level logs.

### Examine API activities in the Dashboard

2. Choose the name of the API.
3. Under the selected API, choose Dashboard.
4. To display a summary of API activity over time, for **Stage**, choose the desired stage.
5. Use From and To to enter the date range.
6. Refresh, if needed, and view individual metrics displayed in separate graphs titled **API Calls**, **Integration Latency**, **Latency**, **4xx Error** and **5xx Error**. The **CacheHitCount** and **CacheMissCount** graphs will be displayed only if API caching has been enabled.
Tip
To examine method-level CloudWatch metrics, make sure that you have enabled CloudWatch Logs on a method level. For more information about how to set up method-level logging, see Update Stage Settings Using the API Gateway Console (p. 498).

View API Gateway Metrics in the CloudWatch Console

Metrics are grouped first by the service namespace, and then by the various dimension combinations within each namespace.

To view API Gateway metrics using the CloudWatch console

2. If necessary, change the region. From the navigation bar, select the region where your AWS resources reside. For more information, see Regions and Endpoints.
3. In the navigation pane, choose Metrics.
4. In the All metrics tab, choose API Gateway.
5. To view metrics by stage, choose the By Stage panel. And then select desired APIs and metric names.
6. To view metrics by specific API, choose the By Api Name panel. And then select desired APIs and metric names.

To view metrics using the AWS CLI

1. At a command prompt, use the following command to list metrics:

   ```bash
   aws cloudwatch list-metrics --namespace "AWS/ApiGateway"
   ```

2. To view a specific statistics (for example, Average) over a period of time of a 5 minutes intervals, call the following command:

   ```bash
   aws cloudwatch get-metric-statistics --namespace AWS/ApiGateway --metric-name Count --start-time 2011-10-03T23:00:00Z --end-time 2017-10-05T23:00:00Z --period 300 --statistics Average
   ```

View API Gateway Log Events in the CloudWatch Console

To view logged API requests and responses using the CloudWatch console

1. In the navigation pane, choose Logs.
2. Under the Log Groups table, choose a log group of the API-Gateway-Execution-Logs_{rest-api-id}/ {stage-name} name.
3. Under the Log Streams table, choose a log stream. You can use the timestamp to help locate the log stream of your interest.
4. Choose Text to view raw text or choose Row to view the event row by row.

Important
CloudWatch lets you delete log groups or streams. Do not manually delete API Gateway API log groups or streams; let API Gateway manage these resources. Manually deleting log groups or streams may cause API requests and responses not to be logged. If that happens, you can delete
the entire log group for the API and redeploy the API. This is because API Gateway creates log
groups or log streams for an API stage at the time when it is deployed.

Monitoring Tools in AWS

AWS provides various tools that you can use to monitor API Gateway. You can configure some of these
tools to do the monitoring for you automatically, while other tools require manual intervention. We
recommend that you automate monitoring tasks as much as possible.

Automated Monitoring Tools in AWS

You can use the following automated monitoring tools to watch API Gateway and report when
something is wrong:

- **Amazon CloudWatch Alarms** – Watch a single metric over a time period that you specify, and
  perform one or more actions based on the value of the metric relative to a given threshold over a
  number of time periods. The action is a notification sent to an Amazon Simple Notification Service
  (Amazon SNS) topic or Amazon EC2 Auto Scaling policy. CloudWatch alarms do not invoke actions
  simply because they are in a particular state; the state must have changed and been maintained
  for a specified number of periods. For more information, see Monitor API Execution with Amazon
  CloudWatch (p. 569).

- **Amazon CloudWatch Logs** – Monitor, store, and access your log files from AWS CloudTrail or other
  sources. For more information, see Monitoring Log Files in the Amazon CloudWatch User Guide.

- **Amazon CloudWatch Events** – Match events and route them to one or more target functions or
  streams to make changes, capture state information, and take corrective action. For more information,
  see What is Amazon CloudWatch Events in the Amazon CloudWatch User Guide.

- **AWS CloudTrail Log Monitoring** – Share log files between accounts, monitor CloudTrail log files in real
time by sending them to CloudWatch Logs, write log processing applications in Java, and validate that
your log files have not changed after delivery by CloudTrail. For more information, see Working with
CloudTrail Log Files in the AWS CloudTrail User Guide.

Manual Monitoring Tools

Another important part of monitoring API Gateway involves manually monitoring those items that the
CloudWatch alarms don't cover. The API Gateway, CloudWatch, and other AWS console dashboards
provide an at-a-glance view of the state of your AWS environment. We recommend that you also check
the log files on API execution.

- API Gateway dashboard shows the following statistics for a given API stage during a specified period of
time:
  - **API Calls**
  - **Cache Hit**, only when API caching is enabled.
  - **Cache Miss**, only when API caching is enabled.
  - **Latency**
  - **Integration Latency**
  - **4XX Error**
  - **5XX Error**

- The CloudWatch home page shows:
  - Current alarms and status
  - Graphs of alarms and resources
  - Service health status

In addition, you can use CloudWatch to do the following:
• Create **customized dashboards** to monitor the services you care about
• Graph metric data to troubleshoot issues and discover trends
• Search and browse all your AWS resource metrics
• Create and edit alarms to be notified of problems

**Creating CloudWatch Alarms to Monitor API Gateway**

You can create a CloudWatch alarm that sends an Amazon SNS message when the alarm changes state. An alarm watches a single metric over a time period you specify, and performs one or more actions based on the value of the metric relative to a given threshold over a number of time periods. The action is a notification sent to an Amazon SNS topic or Auto Scaling policy. Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state; the state must have changed and been maintained for a specified number of periods.

**API Gateway Extensions to OpenAPI**

The API Gateway extensions support the AWS-specific authorization and API Gateway-specific API integrations. In this section, we will describe the API Gateway extensions to the OpenAPI specification for REST APIs.

**Tip**
To understand how the API Gateway extensions are used in an app, you can use the API Gateway console to create an API and export it to a OpenAPI definition file. For more information on how to export an API, see Export a REST API (p. 663).

**Topics**
• `x-amazon-apigateway-any-method Object (p. 576)`
• `x-amazon-apigateway-api-key-source Property (p. 576)`
• `x-amazon-apigateway-auth Object (p. 577)`
• `x-amazon-apigateway-authorizer Object (p. 578)`
• `x-amazon-apigateway-authtype Property (p. 581)`
• `x-amazon-apigateway-binary-media-types Property (p. 582)`
• `x-amazon-apigateway-documentation Object (p. 582)`
• `x-amazon-apigateway-gateway-responses Object (p. 583)`
• `x-amazon-apigateway-gateway-responses.gatewayResponse Object (p. 583)`
• `x-amazon-apigateway-gateway-responses.responseParameters Object (p. 584)`
• `x-amazon-apigateway-gateway-responses.responseTemplates Object (p. 585)`
• `x-amazon-apigateway-integration Object (p. 586)`
• `x-amazon-apigateway-integration.requestTemplates Object (p. 589)`
• `x-amazon-apigateway-integration.requestParameters Object (p. 590)`
• `x-amazon-apigateway-integration.responses Object (p. 591)`
• `x-amazon-apigateway-integration.response Object (p. 592)`
• `x-amazon-apigateway-integration.responseTemplates Object (p. 593)`
• `x-amazon-apigateway-integration.responseParameters Object (p. 594)`
• `x-amazon-apigateway-request-validator Property (p. 594)`
• `x-amazon-apigateway-request-validators Object (p. 595)`
• `x-amazon-apigateway-request-validators.requestValidator Object (p. 596)`
**x-amazon-apigateway-any-method Object**

Specifies the OpenAPI Operation Object for the API Gateway catch-all ANY method in a OpenAPI Path Item Object. This object can exist alongside other Operation objects and will catch any HTTP method that was not explicitly declared.

The following table lists the properties extended by API Gateway. For the other OpenAPI Operation properties, see the OpenAPI specification.

### Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>x-amazon-apigateway-integration</td>
<td>x-amazon-apigateway-integration Object</td>
<td>Specifies the integration of the method with the backend. This is an extended property of the OpenAPI Operation object. The integration can be of type AWS, AWS_PROXY, HTTP, HTTP_PROXY, or MOCK.</td>
</tr>
</tbody>
</table>

### x-amazon-apigateway-any-method Example

The following example integrates the ANY method on a proxy resource, `{proxy+}`, with a Lambda function, TestSimpleProxy.

```
"/proxy": {
  "x-amazon-apigateway-any-method": {
    "produces": ["application/json"],
    "parameters": [ {
      "name": "proxy",
      "in": "path",
      "required": true,
      "type": "string"
    }
   ],
   "responses": {},
}
```

### x-amazon-apigateway-api-key-source Property

Specify the source to receive an API key to throttle API methods that require a key. This API-level property is a String type.

Specify the source of the API key for requests. Valid values are:

- **HEADER** for receiving the API key from the X-API-Key header of a request.
• AUTHORIZER for receiving the API key from the UsageIdentifierKey from a Lambda authorizer (formerly known as a custom authorizer).

**x-amazon-apigateway-api-key-source Example**

The following example sets the X-API-Key header as the API key source.

OpenAPI 2.0

```json
{
    "swagger": "2.0",
    "info": {
        "title": "Test1"
    },
    "schemes": [ "https" ],
    "basePath": "/import",
    "x-amazon-apigateway-api-key-source": "HEADER",
    .
    .
    .
}
```

**x-amazon-apigateway-auth Object**

Defines an authentication type to be applied for authentication of method invocations in API Gateway.

**Properties**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>string</td>
<td>Specifies the authentication type. Specify &quot;NONE&quot; for open access. Specify &quot;AWS_IAM&quot; to use IAM permissions. Values are case-insensitive.</td>
</tr>
</tbody>
</table>

**x-amazon-apigateway-auth Example**

The following example sets the authentication type for a REST API method.

OpenAPI 3.0.1

```json
{
    "openapi": "3.0.1",
    "info": {
        "title": "openapi3",
        "version": "2018-12-04T05:22:50Z"
    },
    "servers": [
        {
            "url": "https://hs8l62bm7l.execute-api.us-west-2.amazonaws.com/{basePath}"
        }
    ],
    .
    .
    .
}
```
x-amazon-apigateway-authorizer Object

Defines a Lambda authorizer (formerly known as a custom authorizer) to be applied for authorization of method invocations in API Gateway. This object is an extended property of the OpenAPI Security Definitions object.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>string</td>
<td>The type of the authorizer. This is a required property.Specify &quot;token&quot; for an authorizer with the caller identity embedded in an authorization token. Specify &quot;request&quot; for an authorizer with the caller identity contained in request parameters.</td>
</tr>
<tr>
<td>authorizerUri</td>
<td>string</td>
<td>The Uniform Resource Identifier (URI) of the authorizer Lambda function. The syntax is as follows:</td>
</tr>
</tbody>
</table>

```
arn:aws:apigateway:us-east-1:lambda:path/2015-03-31/functions/arn:aws:lambda:us-east-1:account-```
### Property Name | Type | Description
--- | --- | ---
| id | function:auth_function_name/invocations |
| authorizerCredentials | string | Credentials required for invoking the authorizer, if any, in the form of an ARN of an IAM execution role. For example, "arn:aws:iam::account-id:IAM_role".

| identitySource | string | Comma-separated list of mapping expressions of the request parameters as the identity source. Applicable for the authorizer of the "request" type only.

| identityValidationExpression | string | A regular expression for validating the token as the incoming identity. For example, "^x-[a-z]+".

| authorizerResultTtlInSeconds | string | The number of seconds during which the resulting IAM policy is cached.

---

### x-amazon-apigateway-authorizer Examples

The following OpenAPI security definitions example specifies a Lambda authorizer of the "token" type and named test-authorizer.

```json
"securityDefinitions" : {
    "test-authorizer" : {
        "type" : "apiKey",                         // Required and the value must be "apiKey"
        "name" : "Authorization",                  // The name of the header containing the authorization token.
        "in" : "header",                           // Required and the value must be "header"
        "x-amazon-apigateway-authtype" : "oauth2", // Specifies the authorization mechanism for the client.
        "x-amazon-apigateway-authorizer" : {       // An API Gateway Lambda authorizer definition
            "type" : "token", // Required property and the value must be "token"
            "authorizerCredentials" : "arn:aws:iam::account-id:role",
            "identityValidationExpression" : "^x-[a-z]+",
            "authorizerResultTtlInSeconds" : 60
        }
    }
}
```

The following OpenAPI operation object snippet sets the GET /http to use the Lambda authorizer specified above.
The following OpenAPI security definitions example specifies a Lambda authorizer of the "request" type, with a single header parameter (auth) as the identity source. The securityDefinitions is named request_authorizer_single_header.

```
"securityDefinitions": { 
  "request_authorizer_single_header": { 
    "type": "apiKey",
    "name": "auth",    // The name of a single header or query parameter as the identity source.
    "in": "header",    // The location of the single identity source request parameter. The valid value is "header" or "query"
    "x-amazon-apigateway-authType": "custom",
    "x-amazon-apigateway-authorizer": { 
      "type": "request",
      "identitySource": "method.request.header.auth",    // Request parameter mapping expression of the identity source. In this example, it is the 'auth' header.
      "authorizerCredentials": "arn:aws:iam::123456789012:role/AWSepIntegTest-CS-LambdaRole",
      "authorizerResultTtlInSeconds": 300 
    } 
  } 
}
```

The following OpenAPI security definitions example specifies a Lambda authorizer of the "request" type, with one header (HeaderAuth1) and one query string parameter QueryString1 as the identity sources.

```
"securityDefinitions": { 
  "request_authorizer_header_query": { 
    "type": "apiKey",
    "name": "Unused",    // Must be "Unused" for multiple identity sources or non header or query type of request parameters.
    "in": "header",    // Must be "header" for multiple identity sources or non header or query type of request parameters.
    "x-amazon-apigateway-authType": "custom",
    "x-amazon-apigateway-authorizer": { 
      "type": "request",
```
The following OpenAPI security definitions example specifies an API Gateway Lambda authorizer of the "request" type, with a single stage variable (stage) as the identity source.

```
"securityDefinitions": {
  "request_authorizer_single_stagevar": {
    "type": "apiKey",
    "name": "Unused", // Must be "Unused", for multiple identity sources or non header or query type of request parameters.
    "in": "header", // Must be "header", for multiple identity sources or non header or query type of request parameters.
    "x-amazon-apigateway-authtype": "custom",
    "x-amazon-apigateway-authorizer": {
      "type": "request",
      "identitySource": "stageVariables.stage", // Request parameter mapping expression of the identity source. In this example, it is the stage variable.
      "authorizerCredentials": "arn:aws:iam::123456789012:role/AWSepIntegTest-CS-LambdaRole",
      "authorizerResultTtlInSeconds": 300
    }
  }
}
```

### x-amazon-apigateway-authtype Property

Specify an optional customer-defined information describing a Lambda authorizer (formerly known as a custom authorizer). It is used for API Gateway API import and export without functional impact.

This property is an extended property of the OpenAPI Security Definitions Operation object.

### x-amazon-apigateway-authtype Example

The following example sets the type of a Lambda authorizer using OAuth 2.

```
"cust-authorizer": {
  "type": "...", // required
  "name": "...", // name of the identity source header
  "in": "header", // must be header
  "x-amazon-apigateway-authtype": "oauth2", // Specifies the authorization mechanism for the client.
  "x-amazon-apigateway-authorizer": {
    ...
   }
}
```

The following security definition example specifies authorization using AWS Signature Version 4:
x-amazon-apigateway-binary-media-type

```json
"sigv4" : {
    "type" : "apiKey",
    "name" : "Authorization",
    "in" : "header",
    "x-amazon-apigateway-authtype" : "awsSigv4"
}
```

See Also
authorizer.authType

x-amazon-apigateway-binary-media-types Property

Specifies the list of binary media types to be supported by API Gateway, such as application/octet-stream, image/jpeg, etc. This extension is a JSON Array. It should be included as a top-level vendor extension to the OpenAPI document.

x-amazon-apigateway-binary-media-types Example

The following example shows the encoding lookup order of an API.

```
"x-amazon-apigateway-binary-media-types: [ "application/octet", "image/jpeg" ]
```

x-amazon-apigateway-documentation Object

Defines the documentation parts to be imported into API Gateway. This object is a JSON object containing an array of the DocumentationPart instances.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>documentationParts</td>
<td>Array</td>
<td>An array of the exported or imported DocumentationPart instances.</td>
</tr>
<tr>
<td>version</td>
<td>String</td>
<td>The version identifier of the snapshot of the exported documentation parts.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-documentation Example

The following example of the API Gateway extension to OpenAPI defines DocumentationParts instances to be imported to or exported from an API in API Gateway.

```
{ ... 
  "x-amazon-apigateway-documentation": {
    "version": "1.0.3",
    "documentationParts": [
      {
        "location": {
          "type": "API"
        }
      },
```
"properties": {
  "description": "API description",
  "info": {
    "description": "API info description 4",
    "version": "API info version 3"
  }
}
},
{
  // Another DocumentationPart instance
}

x-amazon-apigateway-gateway-responses Object

Defines the gateway responses for an API as a string-to-GatewayResponse map of key-value pairs.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>responseType</td>
<td>x-amazon-apigateway-gateway-responses.gatewayResponse</td>
<td>A GatewayResponse for the specified responseType.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-gateway-responses Example

The following API Gateway extension to OpenAPI example defines a GatewayResponses map containing two GatewayResponse instances, one for the DEFAULT_4XX type and another for the INVALID_API_KEY type.

```json
{
  "x-amazon-apigateway-gateway-responses": {
    "DEFAULT_4XX": {
      "responseParameters": {
        "gatewayresponse.header.Access-Control-Allow-Origin": "domain.com"
      },
      "responseTemplates": {
        "application/json": "{\"message\": test 4xx b}"
      }
    },
    "INVALID_API_KEY": {
      "statusCode": "429",
      "responseTemplates": {
        "application/json": "{\"message\": test forbidden}"}
    }
  }
}
```

x-amazon-apigateway-gateway-responses.gatewayResponse Object

Defines a gateway response of a given response type, including the status code, any applicable response parameters, or response templates.
Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>responseParameters</td>
<td>x-amazon-apigateway-gateway-</td>
<td>Specifies the GatewayResponse parameters, namely the header parameters. The parameter values can take any incoming request parameter (p. 289) value or a static custom value.</td>
</tr>
<tr>
<td></td>
<td>responses.responseParameters</td>
<td></td>
</tr>
<tr>
<td>responseTemplates</td>
<td>x-amazon-apigateway-gateway-</td>
<td>Specifies the mapping templates of the gateway response. The templates are not processed by the VTL engine.</td>
</tr>
<tr>
<td></td>
<td>responses.responseTemplates</td>
<td></td>
</tr>
<tr>
<td>statusCode</td>
<td>string</td>
<td>An HTTP status code for the gateway response.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-gateway-responses.gatewayResponse Example

The following example of the API Gateway extension to OpenAPI defines a GatewayResponse to customize the INVALID_API_KEY response to return the status code of 456, the incoming request's api-key header value, and "Bad api-key" message.

```
"INVALID_API_KEY": {
  "statusCode": "456",
  "responseParameters": {
    "gatewayresponse.header.api-key": "method.request.header.api-key"
  },
  "responseTemplates": {
    "application/json": "{"message": "Bad api-key" }"
  }
}
```

x-amazon-apigateway-gateway-responses.responseParameters Object

Defines a string-to-string map of key-value pairs to generate gateway response parameters from the incoming request parameters or using literal strings.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gatewayresponse.param-</td>
<td>string</td>
<td>param-position can be header, path or querystring. For more information, see Map Method Request Data to Integration Request Parameters (p. 289).</td>
</tr>
<tr>
<td>position.param-name</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**x-amazon-apigateway-gateway-responses.responseParameters Example**

The following OpenAPI extensions example shows a GatewayResponse response parameter mapping expression to enable CORS support for resources on the *.example.domain domains.

```
"responseParameters": {
    "gatewayresponse.header.Access-Control-Allow-Origin": '*example.domain',
    "gatewayresponse.header.from-request-header": method.request.header.Accept,
    "gatewayresponse.header.from-request-path": method.request.path.petId,
    "gatewayresponse.header.from-request-query": method.request.querystring.qname
}
```

**x-amazon-apigateway-gateway-responses.responseTemplates Object**

Defines GatewayResponse mapping templates, as a string-to-string map of key-value pairs, for a given gateway response. For each key-value pair, the key is the content type; for example, "application/json", and the value is a stringified mapping template for simple variable substitutions. A GatewayResponse mapping template is not processed by the Velocity Template Language (VTL) engine.

**Properties**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>content-type</td>
<td>string</td>
<td>A GatewayResponse body mapping template supporting only simple variable substitution to customize a gateway response body.</td>
</tr>
</tbody>
</table>

**x-amazon-apigateway-gateway-responses.responseTemplates Example**

The following OpenAPI extensions example shows a GatewayResponse mapping template to customize an API Gateway-generated error response into an app-specific format.

```
"responseTemplates": {
    "application/json": "{ "message": $context.error.messageString, "type": $context.error.responseType, "statusCode": '488' }
}
```

The following OpenAPI extensions example shows a GatewayResponse mapping template to override an API Gateway-generated error response with a static error message.

```
"responseTemplates": {
    "application/json": "{ "message": 'API-specific errors' }" }
```
x-amazon-apigateway-integration Object

Specifies details of the backend integration used for this method. This extension is an extended property of the OpenAPI Operation object. The result is an API Gateway integration object.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cacheKeyParameters</td>
<td>An array of string</td>
<td>A list of request parameters whose values are to be cached.</td>
</tr>
<tr>
<td>cacheNamespace</td>
<td>string</td>
<td>An API-specific tag group of related cached parameters.</td>
</tr>
<tr>
<td>connectionId</td>
<td>string</td>
<td>The ID of a VpcLink for the private integration.</td>
</tr>
<tr>
<td>connectionType</td>
<td>string</td>
<td>The integration connection type. The valid value is &quot;VPC_LINK&quot; for private integration or &quot;INTERNET&quot;, otherwise.</td>
</tr>
<tr>
<td>credentials</td>
<td>string</td>
<td>For AWS IAM role-based credentials, specify the ARN of an appropriate IAM role. If unspecified, credentials will default to resource-based permissions that must be added manually to allow the API to access the resource. For more information, see Granting Permissions Using a Resource Policy. Note: when using IAM credentials, please ensure that AWS STS regional endpoints are enabled for the region where this API is deployed for best performance.</td>
</tr>
<tr>
<td>contentHandling</td>
<td>string</td>
<td>Request payload encoding conversion types. Valid values are 1) CONVERT_TO_TEXT, for converting a binary payload into a Base64-encoded string or converting a text payload into a utf-8-encoded string or passing through the text payload natively without modification, and 2) CONVERT_TO_BINARY, for converting a text payload into Base64-decoded blob or passing through a binary payload natively without modification.</td>
</tr>
<tr>
<td>httpMethod</td>
<td>string</td>
<td>The HTTP method used in the integration request. For Lambda</td>
</tr>
<tr>
<td>Property Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>function invocations</td>
<td></td>
<td>function invocations, the value must be POST.</td>
</tr>
<tr>
<td>passthroughBehavior</td>
<td>string</td>
<td>Specifies how a request payload of unmapped content type is passed through the integration request without modification. Supported values are when_no_templates, when_no_match, and never. For more information, see Integration.passthroughBehavior.</td>
</tr>
<tr>
<td>requestParameters</td>
<td>x-amazon-apigateway-integration.requestParameters</td>
<td>Specifies mappings from method request parameters to integration request parameters. Supported request parameters are queryString, path, header, and body.</td>
</tr>
<tr>
<td>requestTemplates</td>
<td>x-amazon-apigateway-integration.requestTemplates</td>
<td>Mapping templates for a request payload of specified MIME types.</td>
</tr>
<tr>
<td>responses</td>
<td>x-amazon-apigateway-integration.responses</td>
<td>Defines the method’s responses and specifies desired parameter mappings or payload mappings from integration responses to method responses.</td>
</tr>
<tr>
<td>timeoutInMillis</td>
<td>integer</td>
<td>Integration timeouts between 50 ms and 29,000 ms.</td>
</tr>
</tbody>
</table>
## x-amazon-apigateway-integration

The type of integration with the specified backend. The valid value is:

- `http` or `http_proxy`: for integration with an HTTP backend;
- `aws_proxy`: for integration with AWS Lambda functions;
- `aws`: for integration with AWS Lambda functions or other AWS services, such as Amazon DynamoDB, Amazon Simple Notification Service or Amazon Simple Queue Service;
- `mock`: for integration with API Gateway without invoking any backend.

For more information about the integration types, see `integration:type`.

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| type          | string  | The type of integration with the specified backend. The valid value is:
- `http` or `http_proxy`: for integration with an HTTP backend;
- `aws_proxy`: for integration with AWS Lambda functions;
- `aws`: for integration with AWS Lambda functions or other AWS services, such as Amazon DynamoDB, Amazon Simple Notification Service or Amazon Simple Queue Service;
- `mock`: for integration with API Gateway without invoking any backend. |
| uri           | string  | The endpoint URI of the backend. For integrations of the `aws` type, this is an ARN value. For the HTTP integration, this is the URL of the HTTP endpoint including the `https` or `http` scheme. |

## x-amazon-apigateway-integration Example

The following example integrates an API's `POST` method with a Lambda function in the backend. For demonstration purposes, the sample mapping templates shown in `requestTemplates` and `responseTemplates` of the examples below are assumed to apply to the following JSON-formatted payload:

```json
{ "name":"value_1", "key":"value_2", "redirect": {"url" :"...") } to generate a JSON output of
{ "stage":"value_1", "user-id":"value_2" } or an XML output of
<stage>value_1</stage>.
```

```json
"x-amazon-apigateway-integration" : {
  "type" : "aws",
  "httpMethod" : "POST",
  "credentials" : "arn:aws:iam::012345678901:role/apigateway-invoke-lambda-exec-role",
  "requestTemplates" : {  
    "application/json" : "#set ($root=$input.path('')) { "$root.name": "$root.name\", "$user-id": "$root.key\" }",
    "application/xml" : "#set ($root=$input.path('')) <stage>$root.name</stage> "
  },
```

588
"requestParameters" : {
  "integration.request.path.stage" : "method.request.querystring.version",
  "integration.request.querystring.provider" : "method.request.querystring.vendor"
},
"cacheNamespace" : "cache namespace",
"cacheKeyParameters" : [],
"responses" : {
  "\d(2)" : {
    "statusCode" : "200",
    "responseParameters" : {
      "method.response.header.requestId" : "integration.response.header.cid"
    },
    "responseTemplates" : {
      "application/json" : "#{set ($root=$input.path('')) \"stage\": \\
      \"$root.name\", \"user-id\": \"$root.key\" }",
      "application/xml" : "#{set ($root=$input.path('')) <stage>$root.name</
      stage> "
    }
  },
  "302" : {
    "statusCode" : "302",
    "responseParameters" : {
      "method.response.header.Location" : "integration.response.body.redirect.url"
    }
  },
  "default" : {
    "statusCode" : "400",
    "responseParameters" : {
      "method.response.header.test-method-response-header" : "'static value'"
    }
  }
}

Note that double quotes (\") of the JSON string in the mapping templates must be string-escaped (\").
x-amazon-apigateway-integration.requestParameters Object

Specifies mappings from named method request parameters to integration request parameters. The
method request parameters must be defined before being referenced.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>integration.request.&lt;param-string type&gt;,&lt;param-name&gt;</td>
<td></td>
<td>The value is typically a predefined method request parameter of the method.request.&lt;param-type&gt;.&lt;param-name&gt; format, where &lt;param-type&gt; can be querystring, path, header, or body. However, $context.VARIABLE_NAME, $stageVariables.VARIABLE_NAME, and STATIC_VALUE are also valid. For the body parameter, the &lt;param-name&gt; is a JSON path expression without the $ prefix.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-integration.requestParameters Example

The following request parameter mappings example translates a method request's query (version), header (x-user-id) and path (service) parameters to the integration request's query (stage), header (x-userid), and path parameters (op), respectively.

Note
If you are creating resources via OpenAPI or AWS CloudFormation, static values should be enclosed in single quotes.
To add this value from the console, enter application/json in the box, without quotation marks.

"requestParameters" : {
    "integration.request.querystring.stage" : "method.request.querystring.version",
    "integration.request.header.x-userid" : "method.request.header.x-user-id",
    "integration.request.path.op" : "method.request.path.service"
}
### x-amazon-apigateway-integration.responses Object

Defines the method's responses and specifies parameter mappings or payload mappings from integration responses to method responses.

**Properties**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Response status pattern | x-amazon-apigateway-integration.response Object (p. 592) | Selection regular expression used to match the integration response to the method response. For HTTP integrations, this regex applies to the integration response status code. For Lambda invocations, the regex applies to the errorMessage field of the error information object returned by AWS Lambda as a failure response body when the Lambda function execution throws an exception.

**Note**
The `Response status pattern` property name refers to a response status code or regular expression describing a group of response status codes. It does not correspond to any identifier of an IntegrationResponse resource in the API Gateway REST API.

### x-amazon-apigateway-integration.responses Example

The following example shows a list of responses from 2xx and 302 responses. For the 2xx response, the method response is mapped from the integration response's payload of the application/json or application/xml MIME type. This response uses the supplied mapping templates. For the 302 response, the method response returns a Location header whose value is derived from the redirect.url property on the integration response's payload.

```json
"responses" : {
   "2\d{2}" : {
      "statusCode" : "200",
      "responseTemplates" : {
         "application/json" : "#set ($root=$input.path('$')) { "$root.name": "$root.name", "$user-id": "$root.key" }",
         "application/xml" : "#set ($root=$input.path('$')) <stage>$root.name</stage>"
      }
   },
   "302" : {
```
x-amazon-apigateway-integration.response Object

Defines a response and specifies parameter mappings or payload mappings from the integration response to the method response.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>statusCode</td>
<td>string</td>
<td>HTTP status code for the method response; for example, &quot;200&quot;. This must correspond to a matching response in the OpenAPI Operation responses field.</td>
</tr>
<tr>
<td>responseParameters</td>
<td>x-amazon-apigateway-integration.responseParameters Object (p. 594)</td>
<td>Specifies parameter mappings for the response. Only the header and body parameters of the integration response can be mapped to the header parameters of the method.</td>
</tr>
<tr>
<td>contentHandling</td>
<td>string</td>
<td>Response payload encoding conversion types. Valid values are 1) CONVERT_TO_TEXT, for converting a binary payload into a Base64-encoded string or converting a text payload into a utf-8-encoded string or passing through the text payload natively without modification, and 2) CONVERT_TO_BINARY, for converting a text payload into Base64-decoded blob or passing through a binary payload natively without modification.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-integration.response Example

The following example defines a 302 response for the method that derives a payload of the application/json or application/xml MIME type from the backend. The response uses the
supplied mapping templates and returns the redirect URL from the integration response in the method's Location header.

```
{
    "statusCode": "302",
    "responseTemplates": {
        "application/json": "#set ($root=$input.path('')) { "stage":"$root.name ", "user-id":"$root.key" }",
        "application/xml": "#set ($root=$input.path('')) <stage>$root.name</stage> "
    },
    "responseParameters": {
        "method.response.header.Location": "integration.response.body.redirect.url"
    }
}
```

**x-amazon-apigateway-integration.responseTemplates Object**

Specifies mapping templates for a response payload of the specified MIME types.

**Properties**

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIME type</td>
<td>string</td>
<td>Specifies a mapping template to transform the integration response body to the method response body for a given MIME type. For information about creating a mapping template, see Mapping Templates (p. 266). An example of the MIME type is application/json.</td>
</tr>
</tbody>
</table>

**x-amazon-apigateway-integration.responseTemplate Example**

The following example sets mapping templates for a request payload of the application/json and application/xml MIME types.

```
"responseTemplates": {
    "application/json": "#set ($root=$input.path('')) { "stage": "$root.name ", "user-id": "$root.key" }",
    "application/xml": "#set ($root=$input.path('')) <stage>$root.name</stage> "
}
```
x-amazon-apigateway-integration.responseParameters Object

Specifies mappings from integration method response parameters to method response parameters. Only the header and body types of the integration response parameters can be mapped to the header type of the method response.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>method.response.header.&lt;param-name&gt;</td>
<td>string</td>
<td>The named parameter value can be derived from the header and body types of the integration response parameters only.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-integration.responseParameters Example

The following example maps body and header parameters of the integration response to two header parameters of the method response.

```
"responseParameters" : {
   "method.response.header.Location" : "integration.response.body.redirect.url",
   "method.response.header.x-user-id" : "integration.response.header.x-userid"
}
```

x-amazon-apigateway-request-validator Property

Specifies a request validator, by referencing a request_validator_name of the x-amazon-apigateway-request-validators Object (p. 595) map, to enable request validation on the containing API or a method. The value of this extension is a JSON string.

This extension can be specified at the API level or at the method level. The API-level validator applies to all of the methods unless it is overridden by the method-level validator.

x-amazon-apigateway-request-validator Example

The following example applies the basic request validator at the API level while applying the parameter-only request validator on the POST /validation request.

OpenAPI 2.0

```
{
   "swagger": "2.0",
   "x-amazon-apigateway-request-validators" : {
      "basic" : {
         "validateRequestBody" : true,
         "validateRequestParameters" : true
      },
      "params-only" : {
         "validateRequestBody" : false,
         "validateRequestParameters" : true
      }
   }
}
```
x-amazon-apigateway-request-validators Object

Defines the supported request validators for the containing API as a map between a validator name and the associated request validation rules. This extension applies to an API.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>request_validator_name</td>
<td>x-amazon-apigateway-request-validators.requestValidator Object (p. 596)</td>
<td>Specifies the validation rules consisting of the named validator. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;basic&quot; : {</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;validateRequestBody&quot; : true,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;validateRequestParameters&quot; : true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>},</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To apply this validator to a specific method, reference the validator name (basic) as the value of the x-amazon-apigateway-request-validator Property (p. 594) property.</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-request-validators Example

The following example shows a set of request validators for an API as a map between a validator name and the associated request validation rules.

OpenAPI 2.0

```json
{
   "swagger": "2.0",
   ...
   "x-amazon-apigateway-request-validators" : {
      "basic" : {
         "validateRequestBody" : true,
         "validateRequestParameters" : true
      },
      "params-only" : {
         "validateRequestBody" : false,
```
x-amazon-apigateway-request-validators.requestValidator Object

Specifies the validation rules of a request validator as part of the x-amazon-apigateway-request-validators Object (p. 595) map definition.

Properties

<table>
<thead>
<tr>
<th>Property Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>validateRequestBody</td>
<td>Boolean</td>
<td>Specifies whether to validate the request body (true) or not (false).</td>
</tr>
<tr>
<td>validateRequestParameters</td>
<td>Boolean</td>
<td>Specifies whether to validate the required request parameters (true) or not (false).</td>
</tr>
</tbody>
</table>

x-amazon-apigateway-request-validators.requestValidator Example

The following example shows a parameter-only request validator:

```
"params-only": {
    "validateRequestBody" : false,
    "validateRequestParameters" : true
}
```
Creating, Deploying, and Invoking a WebSocket API in Amazon API Gateway

For a brief introduction to WebSocket support in API Gateway, see the section called "Use API Gateway to Create WebSocket APIs" (p. 3).

Topics
- About WebSocket APIs in API Gateway (p. 597)
- Create a WebSocket API in API Gateway (p. 602)
- Set up Routes for a WebSocket API in API Gateway (p. 603)
- Set up WebSocket API Integrations in API Gateway (p. 605)
- Set up Route Responses for a WebSocket API in API Gateway (p. 609)
- Deploy a WebSocket API in API Gateway (p. 610)
- Invoke a WebSocket API (p. 612)
- Control Access to a WebSocket API in API Gateway (p. 614)
- Monitor WebSocket API Execution with CloudWatch (p. 617)
- WebSocket Selection Expressions in API Gateway (p. 618)
- API Gateway WebSocket API Mapping Template Reference (p. 625)

About WebSocket APIs in API Gateway

In API Gateway you can create a WebSocket API as a stateful frontend for an AWS service (such as Lambda or DynamoDB) or for an HTTP endpoint. The WebSocket API invokes your backend based on the content of the messages it receives from client apps.

Unlike a REST API, which receives and responds to requests, a WebSocket API supports two-way communication between client apps and your backend. The backend can send callback messages to connected clients.

In your WebSocket API, incoming JSON messages are directed to backend integrations based on routes that you configure. (Non-JSON messages are directed to a $default route that you configure.)

A route includes a route key, which is the value that is expected once a route selection expression is evaluated. The routeSelectionExpression is an attribute defined at the API level. It specifies a JSON property that is expected to be present in the message payload. For more information about route selection expressions, see the section called "" (p. 619).

For example, if your JSON messages contain an action property, and you want to perform different actions based on this property, your route selection expression might be ${request.body.action}. Your routing table would specify which action to perform by matching the value of the action property against the custom route key values that you have defined in the table.
There are three predefined routes that can be used: $connect, $disconnect, and $default. In addition, you can create custom routes:

- API Gateway calls the $connect route when a persistent connection between the client and a WebSocket API is being initiated.
- API Gateway calls the $disconnect route when the client or the server disconnects from the API.
- API Gateway calls a custom route after the route selection expression is evaluated against the message if a matching route is found; the match determines which integration is invoked.
- API Gateway calls the $default route if the route selection expression cannot be evaluated against the message or if no matching route is found.

For more information about the $connect and $disconnect routes, see the section called “Managing Connected Users and Client Apps” (p. 598).

For more information about the $default route and custom routes, see the section called “Invoking Your Backend Integration” (p. 599).

Backend services can send data to connected client apps. For more information, see the section called “Sending Data from Backend Services to Connected Clients” (p. 602).

Managing Connected Users and Client Apps: $connect and $disconnect Routes

Topics
- The $connect Route (p. 598)
- The $disconnect Route (p. 599)

The $connect Route

Client apps connect to your WebSocket API by sending a WebSocket upgrade request. If the request succeeds, the $connect route is executed while the connection is being established.

Because the WebSocket connection is a stateful connection, you can configure authorization on the $connect route only. AuthN/AuthZ will be performed only at connection time.

Until execution of the integration associated with the $connect route is completed, the upgrade request is pending and the actual connection will not be established. If the $connect request fails (e.g., due to AuthN/AuthZ failure or an integration failure), the connection will not be made.

Note
If authorization fails on $connect, the connection will not be established, and the client will receive a 401 or 403 response.

Setting up an integration for $connect is optional. However, doing so can be useful, because the backend receives the user ID of clients that connect. You should consider setting up a $connect integration if:

- You want to be notified when clients connect and disconnect.
- You want to throttle connections or control who connects.
- You want your backend to send messages back to clients using a callback URL.
- You want to store each connection ID and other information into a database (e.g., Amazon DynamoDB).
The $disconnect Route

The $disconnect route is executed after the connection is closed.

The connection can be closed by the server or by the client. As the connection is already closed when it is executed, $disconnect is a best-effort event. API Gateway will try its best to deliver the $disconnect event to your integration, but it cannot guarantee delivery.

The backend can initiate disconnection by using the @connections API. For more information, see the section called “Use @connections Commands in Your Backend Service” (p. 613).

Invoking Your Backend Integration: $default Route and Custom Routes

Topics
  • Using Routes to Process Messages (p. 599)
  • The $default Route (p. 600)
  • Custom Routes (p. 600)
  • Using API Gateway WebSocket API Integrations to Connect to Your Business Logic (p. 600)
  • Important Differences Between WebSocket APIs and REST APIs (p. 600)
  • Handling Binary Payloads (p. 601)

Using Routes to Process Messages

In API Gateway WebSocket APIs, messages can be sent from the client to your backend service and vice versa. Unlike HTTP's request/response model, in WebSocket the backend can send messages to the client without the client taking any action.

Messages can be JSON or non-JSON. However, only JSON messages can be routed to specific integrations based on message content. Non-JSON messages are passed through to the backend by the $default route.

Note

API Gateway supports message payloads up to 128 KB with a maximum frame size of 32 KB. If a message exceeds 32 KB, you must split it into multiple frames, each 32 KB or smaller. If a larger message (or frame) is received, the connection is closed with code 1009. Currently binary payloads are not supported. If a binary frame is received, the connection is closed with code 1003. However, it is possible to convert binary payloads to text. See the section called “Handling Binary Payloads” (p. 601).

With WebSocket APIs in API Gateway, JSON messages can be routed to execute a specific backend service based on message content. When a client sends a message over its WebSocket connection, this results in a route request to the WebSocket API. The request will be matched to the route with the corresponding route key in API Gateway. You can set up a route request for a WebSocket API in the API Gateway console, by using the AWS CLI, or by using an AWS SDK.

Note

In the AWS CLI and AWS SDKs, you can create routes before or after you create integrations. Currently the console does not support reuse of integrations, so you must create the route first and then create the integration for that route.

You can configure API Gateway to perform validation on a route request before proceeding with the integration request. If the validation fails, API Gateway fails the request without calling your backend,
Amazon API Gateway Developer Guide
Invoking Your Backend Integration

sends a "Bad request body" gateway response similar to the following to the client, and publishes
the validation results in CloudWatch Logs:
{"message" : "Bad request body", "connectionId": "{connectionId}", "messageId":
"{messageId}"}

This reduces unnecessary calls to your backend and lets you focus on the other requirements of your API.
You can also deﬁne a route response for your API's routes to enable two-way communication. A
route response describes what data will be sent to your client upon completion of a particular route's
integration. It is not necessary to deﬁne a response for a route if, for example, you want a client to send
messages to your backend without receiving a response (one-way communication). However, if you don't
provide a route response, API Gateway won't send any information about the result of your integration
to your clients.

The $default Route
Every API Gateway WebSocket API can have a $default route. This is a special routing value that can be
used in the following ways:
• You can use it together with deﬁned route keys, to specify a "fallback" route (for example, a generic
mock integration that returns a particular error message) for incoming messages that don't match any
of the deﬁned route keys.
• You can use it without any deﬁned route keys, to specify a proxy model that delegates routing to a
backend component.
• You can use it to specify a route for non-JSON payloads.

Custom Routes
If you want to invoke a speciﬁc integration based on message content, you can do so by creating a
custom route.
A custom route uses a route key and integration that you specify. When an incoming message contains
a JSON property, and that property evaluates to a value that matches the route key value, API Gateway
invokes the integration. (For more information, see the section called “About WebSocket APIs” (p. 597).)
For example, suppose you wanted to create a chat room application. You might start by creating a
WebSocket API whose route selection expression is $request.body.action. You could then deﬁne
two routes: joinroom and sendmessage. A client app might invoke the joinroom route by sending a
message such as the following:
{"action":"joinroom","roomname":"developers"}

And it might invoke the sendmessage route by sending a message such as the following:
{"action":"sendmessage","message":"Hello everyone"}

Using API Gateway WebSocket API Integrations to Connect to
Your Business Logic
After setting up a route for an API Gateway WebSocket API, you must specify the integration you'd
like to use. As with a route, which can have a route request and a route response, an integration can
have an integration request and an integration response. An integration request contains the information
expected by your backend in order to process the request that came from your client. An integration

600


response contains the data that your backend returns to API Gateway, and that may be used to construct
a message to send to the client (if a route response is defined).

For more information about setting up integrations, see the section called "Set up WebSocket API
Integrations" (p. 605).

Important Differences Between WebSocket APIs and REST APIs

Integrations for WebSocket APIs are similar to integrations for REST APIs, except for the following
differences:

• Currently, in the API Gateway console you must create a route first and then create an integration as
that route's target. However, in the API and CLI, you can create routes and integrations independently,
in any order.

• You can use a single integration for multiple routes. For example, if you have a set of actions that
closely relate to each other, you may want all of those routes to go to a single Lambda function.
Rather than defining the details of the integration multiple times, you can specify it once and assign it
to each of the related routes.

  Note
  Currently the console does not support reuse of integrations, so you must create the route
  first and then create the integration for that route.
  In the AWS CLI and AWS SDKs, you can reuse an integration by setting the route's target to a
  value of "integrations/{integration-id}", where {integration-id} is the unique
  ID of the integration to be associated with the route.

• API Gateway provides multiple selection expressions (p. 618) you can use in your routes and
integrations. You don't need to rely on the content type to select an input template or output
mapping. As with route selection expressions, you can define a selection expression to be evaluated
by API Gateway to choose the right item. All of them will fall back to the $default template if a
matching template is not found.

• In integration requests, the template selection expression supports
  $request.body.<json_path_expression> and static values.

• In integration responses, the template selection expression supports
  $request.body.<json_path_expression>, $integration.response.statuscode, and
  $integration.response.header.<headerName>.

In the HTTP protocol, in which requests and responses are sent synchronously; communication is
essentially one-way. In the WebSocket protocol, communication is two-way. Responses are asynchronous
and are not necessarily received by the client in the same order as the client's messages were sent. In
addition, the backend can send messages to the client.

  Note
  For a route that is configured to use AWS_PROXY or LAMBDA_PROXY integration, communication
  is one-way, and API Gateway will not pass the backend response through to the route response
  automatically. For example, in the case of LAMBDA_PROXY integration, the body that the
  Lambda function returns will not be returned to the client. If you want the client to receive
  integration responses, you must define a route response to make two-way communication
  possible.

Handling Binary Payloads

API Gateway WebSocket APIs don't currently support binary frames in incoming message payloads. If a
client app sends a binary frame, API Gateway rejects it and disconnects the client with code 1003.

There is a workaround for this behavior. If the client sends a text-encoded binary data (e.g.,
Base64) as a text frame, you can set the integration's contentHandlingStrategy property to
CONVERT_TO_BINARY to convert the payload from Base64-encoded string to binary.
To return a route response for a binary payload in non-proxy integrations, you can set the integration response's `contentHandlingStrategy` property to `CONVERT_TO_TEXT` to convert the payload from binary to Base64-encoded string.

**Sending Data from Backend Services to Connected Clients**

API Gateway WebSocket APIs offer the following ways for you to send data from backend services to connected clients:

- An integration can send a response, which is returned to the client by a route response that you have defined.
- You can use the `@connections` API to send a POST request. For more information, see the section called "Use @connections Commands in Your Backend Service" (p. 613).

**Create a WebSocket API in API Gateway**

You can create a WebSocket API in the API Gateway console, by using the AWS CLI `create-api` command, or by using the `CreateApi` command in an AWS SDK. The following procedures show how to create a new WebSocket API.

**Note**

WebSocket APIs only support TLS 1.2. Earlier TLS versions are not supported.

### Create a WebSocket API Using AWS CLI Commands

Creating a WebSocket API using the AWS CLI requires calling the `create-api` command as shown in the following example, which creates an API with the `$request.body.action` route selection expression:

```bash
aws apigatewayv2 --region us-east-1 create-api --name "myWebSocketApi3" --protocol-type WEBSOCKET --route-selection-expression '$request.body.action'
```

**Example output:**

```
{
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "Name": "myWebSocketApi3",
  "CreatedDate": "2018-11-15T06:23:51Z",
  "ProtocolType": "WEBSOCKET",
  "RouteSelectionExpression": "'$request.body.action'",
  "ApiId": "aabbccddeee"
}
```

### Create a WebSocket API Using the API Gateway Console

You can create a WebSocket API in the console by choosing the WebSocket protocol and giving the API a name.

**Important**

Once you have created the API, you cannot change the protocol you have chosen for it. There is no way to convert a WebSocket API into a REST API or vice versa.
To create a WebSocket API using the API Gateway console
1. Sign in to the API Gateway console and choose Create API.
2. Under Choose the protocol, choose WebSocket.
3. Under Create a new API, choose New API.
4. Under Settings, in the API name field, type the name of your API, for example, PetStore.
5. Enter a Route Selection Expression for your API, for example, $request.body.action.

For more information about route selection expressions, see the section called “” (p. 619).
6. If desired, type a Description for your API.
7. Choose Create API.

Set up Routes for a WebSocket API in API Gateway

Topics
• Set up Routes for a WebSocket API in API Gateway (p. 603)
• Specify Route Request Settings (p. 604)

Set up Routes for a WebSocket API in API Gateway

When you first create a new WebSocket API, there are three predefined routes: $connect, $disconnect, and $default. You can create them by using the console, API, or AWS CLI. If desired, you can create custom routes. For more information, see the section called “About WebSocket APIs” (p. 597).

Note
In the CLI, you can create routes before or after you create integrations, and you can reuse the same integration for multiple routes.

Topics
• Create a Route Using the API Gateway Console (p. 603)
• Create a Route Using the AWS CLI (p. 603)

Create a Route Using the API Gateway Console

To create a route using the API Gateway console
1. Sign in to the API Gateway console, choose the API, and choose Routes.
2. To create one of the predefined routes ($connect, $disconnect, and $default), choose its name.
3. If desired, you can create custom routes. To do so, enter the route key name in the New Route Key text box and choose the checkmark icon.

Note
When you create a custom route, do not use the $ prefix in the route key name. This prefix is reserved for predefined routes.

Create a Route Using the AWS CLI

To create a route using the AWS CLI, call create-route as shown in the following example:
Specify Route Request Settings

Specify Route Request Settings for $connect

When you set up the $connect route for your API, the following optional settings are available to enable authorization for your API. For more information, see the section called "The $connect Route" (p. 598).

- **Authorization**: If no authorization is needed, you can specify NONE. Otherwise, you can specify:
  - AWS_IAM to use standard AWS IAM policies to control access to your API.
  - CUSTOM to implement authorization for an API by specifying a Lambda authorizer function that you have previously created. The authorizer can reside in your own AWS account or a different AWS account. For more information about Lambda authorizers, see Use API Gateway Lambda Authorizers (p. 380).

  **Note**
  In the API Gateway console, the CUSTOM setting is visible only after you have set up an authorizer function as described in the section called "Configure a Lambda Authorizer Using the Console" (p. 387).

- **API Key Required**: You can optionally require an API key for an API's $connect route. You can use API keys together with usage plans to control and track access to your APIs. For more information, see the section called "Use Usage Plans with API Keys" (p. 432).

Set up the $connect Route Request Using the API Gateway Console

To set up the $connect route request for a WebSocket API using the API Gateway console:

1. Sign in to the API Gateway console, choose the API, and choose Routes.
2. Under Routes, choose $connect.
3. Choose Route Request in the route overview pane.
4. Under Access Settings, configure the route settings as follows:
   a. To edit the Authorization setting, choose the pencil icon. Choose the desired setting from the dropdown menu and choose the checkmark icon to save the new setting.
   b. To edit the API Key Required setting, choose the pencil icon. Choose true or false from the dropdown menu and choose the checkmark icon to save the new setting.
Set up WebSocket API Integrations in API Gateway

Topics

- Set up a WebSocket API Integration Request in API Gateway (p. 605)
- Set up WebSocket API Integration Responses in API Gateway (p. 607)

Set up a WebSocket API Integration Request in API Gateway

Setting up an integration request involves the following:

- Choosing a route key to integrate to the backend.
- Specifying the backend endpoint to invoke, such as an AWS service or HTTP endpoint.
- Configuring how to transform the route request data, if necessary, into integration request data by specifying one or more request templates.

Set up a WebSocket API Integration Request Using the API Gateway Console

To add an integration request to a route in a WebSocket API using the API Gateway console

1. Sign in to the API Gateway console, choose the API, and choose Routes.
2. Under Routes, choose the route.
3. In the Route Overview pane, choose Integration Request.
4. For Integration Type, choose one of the following:
   - Choose Lambda Function only if your API will be integrated with an AWS Lambda function that you have already created in this account or in another account.
   - Choose HTTP if your API will be integrated with an existing HTTP endpoint. For more information, see Set up HTTP Integrations in API Gateway (p. 239).
   - Choose Mock if you want to generate API responses from API Gateway directly, without the need for an integration backend. For more information, see Set up Mock Integrations in API Gateway (p. 250).
   - Choose AWS Service if your API will be integrated with an AWS service.
   - Choose VPC Link if your API will use a VpcLink as a private integration endpoint. For more information, see Set up API Gateway Private Integrations (p. 244).
5. If you chose Lambda Function, do the following:
   a. For Lambda Region, choose the region identifier that corresponds to the region where you created the Lambda function. For example, if you created the Lambda function in the US East (N. Virginia) region, choose us-east-1. For a list of region names and identifiers, see AWS Lambda in the Amazon Web Services General Reference.
   b. For Use Lambda Proxy integration, choose the checkbox if you intend to use Lambda proxy integration (p. 220) or cross-account Lambda proxy integration (p. 31).
   c. For Lambda Function, specify the function in one of the following ways:
• If your Lambda function is in the same account, start typing the function name and then choose the function from the dropdown list.

  **Note**
The function name can optionally include its alias or version specification, as in HelloWorld, HelloWorld:1, or HelloWorld:alpha.

• If the function is in a different account, type the ARN for the function.

d. Choose **Invoke with caller credentials** if you want API Gateway to invoke your Lambda function using credentials received in the incoming request.

e. For **Execution role**, type the ARN of the Lambda invocation role that enables API Gateway to invoke your Lambda functions.

f. To use the default timeout value of 29 seconds, leave **Use Default Timeout** selection checked. To set a custom timeout, uncheck the box, and enter a timeout value between 50 and 29000 milliseconds.

g. Choose **Save**.

6. If you chose **HTTP**, follow the instructions in step 4 of the section called “Set up Integration Request Using the Console” (p. 216).

7. If you chose **Mock**, proceed to the **Request Templates** step.

8. If you chose **AWS Service**, follow the instructions in step 6 of the section called “Set up Integration Request Using the Console” (p. 216).

9. If you chose **VPC Link**, do the following:

   a. For **Use Proxy integration**, choose the checkbox if you want requests to be proxied to your VPCLink's endpoint.

   b. From the **VPC Link** dropdown list, choose **[Use Stage Variables]** and type ${stageVariables.vpcLinkId} in the text box below the list.

      We will define the vpcLinkId stage variable after deploying the API to a stage and set its value to the ID of the VPCLink.

   c. For **HTTP method**, choose the HTTP method type that most closely matches the method in the HTTP backend.

   d. For **Endpoint URL**, type the URL of the HTTP backend you want this integration to use.

   e. To use the default timeout value of 29 seconds, leave **Use Default Timeout** selection checked. To set a custom timeout, uncheck the box, and enter a timeout value between 50 and 29000 milliseconds.

10. Under **Request Templates**, do the following:

   a. For **Template Selection Expression**, choose the pencil icon and replace the word *template* with a template selection expression. This is an expression that API Gateway looks for in the message payload. If it is found, it is evaluated, and the result is a template key value that is used to select the data mapping template to be applied to the data in the message payload.

   For information about template selection expressions, see the section called “” (p. 620).

---

**Set up an Integration Request Using the AWS CLI**

You can set up an integration request for a route in a WebSocket API by using the AWS CLI as in the following example, which creates a mock integration:

1. Create a file named `integration-params.json`, with the following contents:
Set up WebSocket API Integration Responses in API Gateway

Topics
- Overview of Integration Responses (p. 608)
- Set up an Integration Response Using the API Gateway Console (p. 608)
Overview of Integration Responses

API Gateway's integration response is a way of modeling and manipulating the response from a backend service. There are some differences in setup of a REST API versus a WebSocket API integration response, which are outlined below, but conceptually the behavior is the same.

WebSocket routes can be configured for two-way or one-way communication. If a route has a route response, it is configured for two-way communication. Otherwise, it is configured for one-way communication.

- When a route is configured for two-way communication, an integration response allows you to configure transformations on the returned message payload, similar to Integration Responses for REST APIs.
- If a route is configured for one-way communication, then regardless of any integration response configuration, no response will be returned over the WebSocket channel after the message is processed.

The remainder of this document assumes you have chosen to configure a route with two-way communication.

Integrations can be divided into proxy integrations and non-proxy integrations.

**Important**
For proxy integrations, API Gateway automatically passes the backend output to the caller as the complete payload. There is no integration response.

For non-proxy integrations, you must set up at least one integration response:

- Ideally, one of your integration responses should act as a catch-all when no explicit choice can be made. This default case is represented by setting an integration response key of $default.
- In all other cases, the integration response key functions as a regular expression. It should follow a format of "/expression/".

For non-proxy HTTP integrations:

- API Gateway will attempt to match the HTTP status code of the backend response. The integration response key will function as a regular expression in this case. If a match cannot be found, then $default is chosen as the integration response.
- The template selection expression, as described above, functions identically. For example:
  
  - /2\d\d/: Receive and transform successful responses
  - /4\d\d/: Receive and transform bad request errors
  - $default: Receive and transform all unexpected responses

For current limitations of template selection expressions, see the section called “” (p. 620).

Set up an Integration Response Using the API Gateway Console

To set up a route integration response for a WebSocket API using the API Gateway console:

1. Sign in to the API Gateway console, choose the API, and choose Routes.
2. Choose the route.
3. Choose **Integration Response**.
4. Under **Integration Responses**, enter a value in the **Response Selection Expression** text box.
5. Under **Response Key**, choose **Add Response**.
   a. To define an integration response key, enter a key name in the **New Response Key** text box and choose the checkmark icon.
   b. Choose the pencil icon next to **Template Selection Expression** and enter an expression for API Gateway to look for in your outgoing message. This expression should evaluate to an integration response key value that maps to one of your response templates.

   For information about template selection expressions, see the section called “” (p. 620).

**Set up an Integration Response Using the AWS CLI**

To set up an integration response for a WebSocket API using the AWS CLI call the `create-integration-response` command. The following CLI command shows an example of setting a response of 200:

```
aws apigatewayv2 create-integration-response \
  --api-id vaz7da9626 \
  --integration-response-key 200
```

**Set up Route Responses for a WebSocket API in API Gateway**

WebSocket routes can be configured for two-way or one-way communication. If a route has a route response, it is configured for two-way communication. Otherwise, it is configured for one-way communication. **Route responses** are used to enable two-way communication, in which your API can send a response back to the client in the context of the client's message.

You can configure route responses and response selection expressions by using the API Gateway console or the AWS CLI or an AWS SDK. For more information about route responses, see the section called “Invoking Your Backend Integration” (p. 599).

For more information about route response selection expressions, see the section called “” (p. 621).

**Topics**
- Set up a Route Response Using the API Gateway Console (p. 609)
- Set up a Route Response Using the AWS CLI (p. 610)

**Set up a Route Response Using the API Gateway Console**

To set up a route response for a WebSocket API using the API Gateway console:

1. Sign in to the API Gateway console, choose the API.
2. Under **Routes**, choose the route.
3. Choose **Route Response** in the route overview pane.
4. Under **Response Modeling**, in the **Response Selection Expression** box, enter the desired response selection expression and choose the checkmark icon.

5. Under **Route Responses**, under **Response Key**, choose **Add Response**.

   **Note**
   Currently only $default is supported in route responses for WebSocket APIs.

6. Enter the response key name and choose the checkmark icon.

### Set up a Route Response Using the AWS CLI

To set up a route response for a WebSocket API using the AWS CLI, call the `create-route-response` command as shown in the following example.

```bash
aws apigatewayv2 --region us-east-1 create-route-response --api-id aabbccddeee --route-id 1122334 --route-response-key $default
```

Example output:

```json
{
   "RouteResponseId": "abcdef",
   "RouteResponseKey": "$default"
}
```

### Deploy a WebSocket API in API Gateway

After creating your WebSocket API, you must deploy it to make it available for your users to invoke.

To deploy an API, you create an API deployment (p. 6) and associate it with a stage (p. 6). Each stage is a snapshot of the API and is made available for client apps to call.

**Important**
Every time you update an API, which includes modification of routes, methods, integrations, authorizers, and anything else other than stage settings, you must redeploy the API to an existing stage or to a new stage.
By default you are limited to 10 stages per API, so it is good practice to reuse them.

To call a deployed WebSocket API, the client sends a message to the API's URL. The URL is determined by the API's hostname and stage name.

**Note**
API Gateway will support payloads up to 128 KB with a maximum frame size of 32 KB. If a message exceeds 32 KB, it must be split into multiple frames, each 32 KB or smaller.

Using the API's default domain name, the URL of (for example) a WebSocket API in a given stage (`{stageName}`) is in the following format:

```text
wss://{api-id}.execute-api.{region}.amazonaws.com/{stageName}
```

To make the WebSocket API's URL more user-friendly, you can create a custom domain name (e.g., api.example.com) to replace the default host name of the API. The configuration process is the same as for REST APIs. For more information, see the section called “Set up an API Custom Domain Name” (p. 641).
Stages enable robust version control of your API. For example, you can deploy an API to a test stage and a prod stage, and use the test stage as a test build and use the prod stage as a stable build. After the updates pass the test, you can promote the test stage to the prod stage. The promotion can be done by redeploying the API to the prod stage.

Topics
- Create a WebSocket API Deployment Using the AWS CLI (p. 611)
- Create a WebSocket API Deployment Using the API Gateway Console (p. 612)

Create a WebSocket API Deployment Using the AWS CLI

To use AWS CLI to create a deployment, use the `create-deployment` command as shown in the following example:

```bash
aws apigatewayv2 --region us-east-1 create-deployment --api-id aabbccddee
```

Example output:

```
{
  "DeploymentId": "fedcba",
  "DeploymentStatus": "DEPLOYED",
  "CreatedDate": "2018-11-15T06:49:09Z"
}
```

The deployed API is not callable until you associate the deployment with a stage. You can create a new stage or reuse a stage that you have previously created.

To create a new stage and associate it with the deployment, use the `create-stage` command as shown in the following example:

```bash
aws apigatewayv2 --region us-east-1 create-stage --api-id aabbccddee --deployment-id fedcba --stage-name test
```

Example output:

```
{
  "StageName": "test",
  "CreatedDate": "2018-11-15T06:50:28Z",
  "DeploymentId": "fedcba",
  "DefaultRouteSettings": {
    "MetricsEnabled": false,
    "ThrottlingBurstLimit": 5000,
    "DataTraceEnabled": false,
    "ThrottlingRateLimit": 10000.0
  },
  "LastUpdatedDate": "2018-11-15T06:50:28Z",
  "StageVariables": {},
  "RouteSettings": {}
}
```

To reuse an existing stage, update the stage's `deploymentId` property with the newly created deployment ID (`{deployment-id}`) by using the `update-stage` command.

```bash
aws apigatewayv2 update-stage --region {region} \
```

611
Create a WebSocket API Deployment Using the API Gateway Console

To use the API Gateway console to create a deployment for a WebSocket API:

1. Sign in to the API Gateway console and choose the API.
2. From the Actions dropdown menu, choose Deploy API.
3. Choose the desired stage from the dropdown list or enter the name of a new stage.

Invoke a WebSocket API

Once you have deployed your WebSocket API, client applications can connect to it and send messages to it, and your backend can send messages to connected client applications:

- You can use wscat to connect to your WebSocket API and send messages to it to simulate client behavior. See the section called “Use wscat to Connect to a WebSocket API and Send Messages to It” (p. 612).
- You can use the @connections API from your backend service to send a callback message to a connected client, get connection information, or disconnect the client. See the section called “Use @connections Commands in Your Backend Service” (p. 613).
- A client application can use its own WebSocket library to invoke your WebSocket API.

Use wscat to Connect to a WebSocket API and Send Messages to It

The wscat utility is a convenient tool for testing a WebSocket API that you have created and deployed in API Gateway. You can install and use wscat as follows:

2. Install it by running the following command:

```
npm install -g wscat
```
3. To connect to your API, run the wscat command as shown in the following example. Note that this example assumes that the Authorization setting is NONE.

```
wscat -c wss://aabbccddee.execute-api.us-east-1.amazonaws.com/test/
```

You'll need to replace aabbccddee with the actual API ID, which is displayed the API Gateway console or returned by the AWS CLI create-api command.

In addition, if your API is in a region other than us-east-1, you'll need to substitute the correct region.
4. To test your API, type a message such as the following while connected:

```
612
```
Use @connections Commands in Your Backend Service

Your backend service can use the following WebSocket connection HTTP requests to send a callback message to a connected client, get connection information, or disconnect the client.

**Important**
These requests use IAM authorization (p. 614), so you must sign them with Signature Version 4 (SigV4). To do this, you can use the API Gateway Management API. For more information, see ApiGatewayManagementApi.

In the following command, you’ll need to replace \( \text{api-id} \) with the actual API ID, which is displayed in the API Gateway console or returned by the AWS CLI create-api command. In addition, if your API is in a region other than us-east-1, you’ll need to substitute the correct region.

To send a callback message to the client, use:

```
POST https://\{api-id\}.execute-api.us-east-1.amazonaws.com/\{stage\}/
@connections/{connection_id}
```

You can test this request by using Postman or by calling awscurl as in the following example:

```
awscurl --service execute-api -X POST -d "hello world" https://\{prefix\}.execute-api.us-east-1.amazonaws.com/\{stage\}/@connections/{connection_id}
```

You’ll need to URL-encode the command as in the following example:

```
awscurl --service execute-api -X POST -d "hello world" https://aabbccddee.execute-api.us-east-1.amazonaws.com/prod/%40connections/R0oXAdfD0kwCH6w%3D
```

To get the latest connection status of the client, use:

```
GET https://\{api-id\}.execute-api.us-east-1.amazonaws.com/\{stage\}/
@connections/{connection_id}
```

To disconnect the client, use:

```
DELETE https://\{api-id\}.execute-api.us-east-1.amazonaws.com/\{stage\}/
@connections/{connection_id}
```
Control Access to a WebSocket API in API Gateway

Topics
- Use IAM Authorization (p. 614)
- Create a Lambda REQUEST Authorizer Function (p. 615)

Use IAM Authorization

IAM authorization in WebSocket APIs is similar to that for REST APIs (p. 369), with the following exceptions:

- The `execute-api` action supports `ManageConnections` in addition to existing actions (Invoke, InvalidateCache). `ManageConnections` controls access to the @connections API.
- WebSockets routes use a different ARN format:

  arn:aws:execute-api:region:account-id:api-id/stage-name/route-key

- The @connections API uses the same ARN format as REST APIs:

  arn:aws:execute-api:region:account-id:api-id/stage-name/POST/@connections

For example, you could set up the following policy to the client. This example allows everyone to send a message (Invoke) for all routes except for a secret route in the prod stage and prevents everyone from sending a message back to connected clients (ManageConnections) for all stages.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [ "execute-api:Invoke" ],
      }
   ]
}
```
Create a Lambda REQUEST Authorizer Function

A Lambda authorizer function in WebSocket APIs is similar to that for REST APIs (p. 382), with the following exceptions:

- You cannot use path variables (event.pathParameters), because the path is fixed.
- event.methodArn is different from its REST API equivalent, because it has no HTTP method. In the case of $connect, methodArn ends with "$connect":
  
  \[
  \text{arn:aws:execute-api:region:account-id:api-id/stage-name/$connect}
  \]

- The context variables in event.requestContext are different from those for REST APIs.

The following example Lambda authorizer function is a WebSocket version of the Lambda authorizer function for REST APIs in the section called "Create a Lambda Authorizer Function in the Lambda Console" (p. 382):

```javascript
exports.handler = function(event, context, callback) {

    console.log('Received event:', JSON.stringify(event, null, 2));

    // A simple REQUEST authorizer example to demonstrate how to use request parameters to allow or deny a request. In this example, a request is authorized if the client-supplied HeaderAuth1 header, QueryString1 query parameter, stage variable of StageVar1 and the accountId in the request context all match specified values of 'headerValue1', 'queryValue1', 'stageValue1', and '123456789012', respectively.

    // Retrieve request parameters from the Lambda function input:
    var headers = event.headers;
    var queryStringParameters = event.queryStringParameters;
    var stageVariables = event.stageVariables;
    var requestContext = event.requestContext;

    // Parse the input for the parameter values
    var tmp = event.methodArn.split(':');
    var apiGatewayArnTmp = tmp[5].split('/');
    var awsAccountId = tmp[4];
    var region = tmp[3];

    // The contextArn is a unique identifier for the API gateway to which the methodArn belongs. In the case of a WebSocket API, the contextArn includes the API gateway's region, account, and stage.
    var contextArn = tmp[5];

    // Check the client-supplied request parameters against the specified values.
    var allowed = true;
    allowed = allowed && (headers['HeaderAuth1'] == 'headerValue1');
    allowed = allowed && (queryStringParameters['QueryString1'] == 'queryValue1');
    allowed = allowed && (stageVariables['StageVar1'] == 'stageValue1');
    allowed = allowed && (requestContext['accountId'] == '123456789012');

    // If the request is not allowed, deny it.
    if (!allowed) {
        callback(new Error('Unauthorized request.'));
    }
    else {
        callback(null, {statusCode: 200, body: 'Request allowed.'});
    }
};
```
```
var restApiId = apiGatewayArnTmp[0];
var stage = apiGatewayArnTmp[1];
var route = apiGatewayArnTmp[2];

// Perform authorization to return the Allow policy for correct parameters and
// the 'Unauthorized' error, otherwise.
var authResponse = {};
var condition = {}
condition.IpAddress = {};

if (headers.HeaderAuth1 === "headerValue1"
&& queryStringParameters.QueryString1 === "queryValue1"
&& stageVariables.StageVar1 === "stageValue1"
&& requestContext.accountId === "123456789012") {
    callback(null, generateAllow('me', event.methodArn));
} else {
    callback("Unauthorized");
}

// Help function to generate an IAM policy
var generatePolicy = function(principalId, effect, resource) {
    // Required output:
    var authResponse = {};
    authResponse.principalId = principalId;
    if (effect && resource) {
        var policyDocument = {};
        policyDocument.Version = '2012-10-17'; // default version
        policyDocument.Statement = [];
        var statementOne = {};
        statementOne.Action = 'execute-api:Invoke'; // default action
        statementOne.Effect = effect;
        statementOne.Resource = resource;
        policyDocument.Statement[0] = statementOne;
        authResponse.policyDocument = policyDocument;
    }
    // Optional output with custom properties of the String, Number or Boolean type.
    authResponse.context = {
        "stringKey": "stringval",
        "numberKey": 123,
        "booleanKey": true
    };
    return authResponse;
}

var generateAllow = function(principalId, resource) {
    return generatePolicy(principalId, 'Allow', resource);
}
var generateDeny = function(principalId, resource) {
    return generatePolicy(principalId, 'Deny', resource);
}
```

To configure the preceding Lambda function as a REQUEST authorizer function for a WebSocket API, follow the same procedure as for REST APIs (p. 387).

To configure the $connect route to use this Lambda authorizer in the console, select or create the $connect route. Choose the route request and choose your authorizer in the Authorization dropdown menu.

To test the authorizer, you'll need to create a new connection. Changing authorizer in $connect does not affect the already connected client. When you connect to your WebSocket API, you'll need to provide values for any configured identity sources. For example, you can connect by sending a valid query string and header using wscat as in the following example:
Monitor WebSocket API Execution with CloudWatch

You can use Amazon CloudWatch metrics and logs to monitor the execution of WebSocket APIs. The configuration is similar to that used for REST APIs.

For instructions on how to set up CloudWatch access and execution logging, see the section called “Set up API Logging Using the API Gateway Console” (p. 513).

When you specify the Log Format, you can choose which context variables to log. Here is an example of a JSON-formatted list of context variables for a WebSocket API:

```json
{
    "apiId" : "$context.apiId",
    "routeKey" : "$context.routeKey",
    "authorizer" : "$context.authorizer",
    "messageId" : "$context.messageId",
    "integrationLatency" : "$context.integrationLatency",
    "eventType" : "$context.eventType",
    "error" : "$context.error",
    "extendedRequestId" : "$context.extendedRequestId",
    "requestTime" : "$context.requestTime",
    "stage" : "$context.stage",
    "connectedAt" : "$context.connectedAt",
    "requestTimeEpoch" : "$context.requestTimeEpoch",
    "requestId" : "$context.requestId",
    "connectionId" : "$context.connectionId"
}
```

You can find WebSocket-specific context variables here: the section called "WebSocket Mapping Template Reference" (p. 625)

The following metrics are supported for WebSocket APIs:

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConnectCount</td>
<td>Number of messages sent to the $connect route integration.</td>
</tr>
<tr>
<td>MessageCount</td>
<td>Number of messages sent to the WebSocket API, either from or to the client.</td>
</tr>
<tr>
<td>IntegrationError</td>
<td>Number of requests that return a 4XX/5XX response from the integration.</td>
</tr>
</tbody>
</table>
### Metric and Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ClientError</td>
<td>Number of requests that have a 4XX response returned by API Gateway before the integration is invoked.</td>
</tr>
<tr>
<td>ExecutionError</td>
<td>Errors that occurred when calling the integration.</td>
</tr>
<tr>
<td>IntegrationLatency</td>
<td>The time difference between API Gateway sending the request to the integration and API Gateway receiving the response from the integration. Suppressed for callbacks and mock integrations.</td>
</tr>
</tbody>
</table>

You can use the dimensions in the following table to filter API Gateway metrics.

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apid</td>
<td>Filters API Gateway metrics for an API with the specified API ID.</td>
</tr>
<tr>
<td>Apid, Stage</td>
<td>Filters API Gateway metrics for an API stage with the specified API ID and stage ID.</td>
</tr>
<tr>
<td>Apid, Stage, Route</td>
<td>Filters API Gateway metrics for an API method with the specified API ID, stage ID, and route ID.</td>
</tr>
</tbody>
</table>

API Gateway will not send these metrics unless you have explicitly enabled detailed CloudWatch metrics. You can do this by calling the UpdateStage action of the API Gateway V2 REST API to update the metricsEnabled property to true. Enabling such metrics will incur additional charges to your account. For pricing information, see Amazon CloudWatch Pricing.

---

**WebSocket Selection Expressions in API Gateway**

**Topics**

- Route Selection Expressions (p. 619)
- Model Selection Expressions (p. 620)
- Template Selection Expressions (p. 620)
- Route Response Selection Expressions (p. 621)
API Gateway uses selection expressions as a way to evaluate request and response context and produce a key. The key is then used to select from a set of possible values, typically provided by you, the API developer. The exact set of supported variables will vary depending on the particular expression. Each expression is discussed in more detail below.

For all of the expressions, the language follows the same set of rules:

- A variable is prefixed with "$".
- Curly braces can be used to explicitly define variable boundaries, e.g., "${request.body.version}-beta".
- Multiple variables are supported, but evaluation occurs only once (no recursive evaluation).
- A dollar sign ($) can be escaped with "\". This is most useful when defining an expression that maps to the reserved $default key, e.g., "\$default".
- In some cases, a pattern format is required. In this case, the expression should be wrapped with forward slashes ("/"), e.g. "/2\d\d/" to match 2XX status codes.

## Route Selection Expressions

A route selection expression is evaluated when the service is selecting the route to follow for an incoming message. The service will use the route whose routeKey exactly matches the evaluated value. If none match, and a route with the $default route key exists, that will be selected. If no routes match the evaluated value and there is no $default route, the service will return an error. For WebSocket-based APIs, the expression should be of the form $request.body.{path_to_body_element}.

For example, suppose you are sending the following JSON message:

```json
{
    "service" : "chat",
    "action" : "join",
    "data" : {
        "room" : "room1234"
    }
}
```

You might want to select your API's behavior based on the action property. In that case, you might define the following route selection expression:

```sql
#request.body.action
```

In this example, request.body refers to your message's JSON payload, and .action is a JSONPath expression. You can use any JSON path expression after request.body, but keep in mind that the result will be stringified. For example, if your JSONPath expression returns an array of two elements, that will be presented as the string "[item1, item2]". For this reason, it is good practice to have your expression evaluate to a value and not an array or an object.

You can simply use a static value, or you can use multiple variables. The following table shows examples and their evaluated results against the above payload.
Model Selection Expressions

When you define a route (p. 604) for a WebSocket API, you can optionally specify a model selection expression. This expression is evaluated to select the model to be used for body validation when a request is received. The expression evaluates to one of the entries in a route's requestmodels.

A model is expressed as a JSON schema and describes the data structure of the request body. The nature of this selection expressions allows you to dynamically choose the model to validate against at runtime for a particular route. For information about how to create a model, see the section called “Create Models and Mapping Templates” (p. 262).

Template Selection Expressions

When you define an integration request (p. 605) or integration response (p. 607) for a WebSocket API, you can optionally specify a template selection expression. This expression is evaluated to determine the input or output template (if any) to use to transform either the request body into the integration request body (via an input template) or the integration response body to the route response body (via an output template).
Integration.TemplateSelectionExpression supports ${request.body.jsonPath} and static values.

IntegrationResponse.TemplateSelectionExpression supports ${request.body.jsonPath}, ${integration.response.statuscode}, ${integration.response.header.headerName}, ${integration.response.multivalueheader.headerName}, and static values.

Route Response Selection Expressions

A route response (p. 609) is used for modeling a response from the backend to the client. For WebSocket APIs, a route response is optional. When defined, it signals to API Gateway that it should return a response to a client upon receiving a WebSocket message.

Evaluation of the route response selection expression produces a route response key. Eventually, this key will be used to choose from one of the RouteResponses associated with the API. However, currently only the $default key is supported.

API Key Selection Expressions

This expression is evaluated when the service determines the given request should proceed only if the client provides a valid API key (p. 6).

Currently the only two supported values are $request.header.x-api-key and $context.authorizer.usageIdentifierKey.

API Mapping Selection Expressions

This expression is evaluated to determine which API stage is selected when a request is made using a custom domain.

Currently, the only supported value is $request.basepath.

Integration Response Selection Expressions

When you set up an integration response (p. 607) for a WebSocket API, you can optionally specify an integration response selection expression. This expression determines what IntegrationResponse should be selected when an integration returns. The value of this expression is currently restricted by API Gateway, as defined below. Realize that this expression is only relevant for non-proxy integrations; a proxy integration simply passes the response payload back to the caller without modeling or modification.

Unlike the other selection expressions outlined above, this expression currently supports a pattern-matching format. The expression should be wrapped with forward slashes.

Currently the value is fixed depending on the integrationType:

- For Lambda-based integrations, it is $integration.response.body.errorMessage.
- For HTTP and MOCK integrations, it is $integration.response.statuscode.
- For HTTP_PROXY and AWS_PROXY, the expression is not utilized, because you are requesting that the payload pass through to the caller.

WebSocket Selection Expression Summary

The following table summarizes the use cases for selection expressions in WebSocket APIs:
<table>
<thead>
<tr>
<th>Selection Expression</th>
<th>Evaluates to Key For</th>
<th>Notes</th>
<th>Example Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Api.RouteSelectionExpression</td>
<td>$default is supported as a catch-all route.</td>
<td>Route WebSocket messages based on the context of a client request.</td>
<td></td>
</tr>
<tr>
<td>Route.ModelSelectionExpression</td>
<td>Optional. If provided for non-proxy integration, model validation occurs.</td>
<td>Perform request validation dynamically within the same route.</td>
<td></td>
</tr>
<tr>
<td>Integration.TemplateSelectionExpression</td>
<td>Optional. May be provided for non-proxy integration to manipulate incoming payloads.</td>
<td>Manipulate the caller's request based on dynamic properties of the request.</td>
<td></td>
</tr>
<tr>
<td>Selection Expression</td>
<td>Evaluates to Key For</td>
<td>Notes</td>
<td>Example Use Case</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------</td>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>Integration.IntegrationResponseSelectionExpression</td>
<td>IntegrationResponse.IntegrationResponseKey</td>
<td>Optional. May be provided for non-proxy integrations.</td>
<td>Manipulate the response from the backend.</td>
</tr>
</tbody>
</table>

Acts as a pattern match for error messages (from Lambda) or status codes (from HTTP integrations). `$default` is required for non-proxy integrations to act as the catch-all for successful responses. Choose the action to occur based on the dynamic response of the backend (e.g., handling certain errors distinctly).
<table>
<thead>
<tr>
<th>Selection Expression</th>
<th>Evaluates to Key For</th>
<th>Notes</th>
<th>Example Use Case</th>
</tr>
</thead>
</table>
| IntegrationResponse.TemplateSelectionExpression | Key for IntegrationResponse.ResponseTemplates | Optional. May be provided for non-proxy integration. $default is supported. | In some cases, a dynamic property of the response may dictate different transformations within the same route and associated integration. 

${request.body.jsonPath}, ${integration.response.statuscode}, ${integration.response.header.headerName}, ${integration.response.multivalueheader.headerName} and static values are supported. $default is supported as a catch-all. |
### WebSocket Mapping Template Reference

This section summarizes the set of variables that are currently supported for WebSocket APIs in API Gateway.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$context.connectionId</td>
<td>A unique ID for the connection that can be used to make a callback to the client.</td>
</tr>
<tr>
<td>$context.connectedAt</td>
<td>The Epoch-formatted connection time.</td>
</tr>
<tr>
<td>$context.domainName</td>
<td>A domain name for the WebSocket API. This can be used to make a callback to the client (instead of a hard-coded value).</td>
</tr>
<tr>
<td>$context.eventType</td>
<td>The event type: CONNECT, MESSAGE, or DISCONNECT.</td>
</tr>
<tr>
<td>$context.messageId</td>
<td>A unique server-side ID for a message. Available only when the $context.eventType is MESSAGE.</td>
</tr>
<tr>
<td>$context.routeKey</td>
<td>The selected route key.</td>
</tr>
<tr>
<td>$context.requestId</td>
<td>Same as $context.extendedRequestId.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>$context.extendedRequestId</code></td>
<td>An automatically generated ID for the API call, which contains more useful information for debugging/troubleshooting.</td>
</tr>
<tr>
<td><code>$context.apiId</code></td>
<td>The identifier API Gateway assigns to your API.</td>
</tr>
<tr>
<td><code>$context.authorizer.principalId</code></td>
<td>The principal user identification associated with the token sent by the client and returned from an API Gateway Lambda authorizer (formerly known as a custom authorizer) Lambda function.</td>
</tr>
<tr>
<td><code>$context.authorizer.property</code></td>
<td>The stringified value of the specified key-value pair of the context map returned from an API Gateway Lambda authorizer function. For example, if the authorizer returns the following context map:</td>
</tr>
</tbody>
</table>
|           | ```
|           | "context" : {
|           | "key": "value",
|           | "numKey": 1,
|           | "boolKey": true
<p>|           | } |
|           | calling <code>$context.authorizer.key</code> returns the &quot;value&quot; string, calling <code>$context.authorizer.numKey</code> returns the &quot;1&quot; string, and calling <code>$context.authorizer.boolKey</code> returns the &quot;true&quot; string. |
| <code>$context.error.message</code> | A string containing an API Gateway error message. This variable can only be used in access logging. |
| <code>$context.error.messageString</code> | The quoted value of <code>$context.error.message</code>, namely &quot;$context.error.message&quot;. |
| <code>$context.error.responseType</code> | The error response type. This variable can only be used in access logging. |
| <code>$context.error.validationErrorString</code> | A string containing a detailed validation error message. |
| <code>$context.identity.accountId</code> | The AWS account ID associated with the request. |
| <code>$context.identity.apiKey</code> | The API owner key associated with key-enabled API request. |
| <code>$context.identity.apiKeyId</code> | The API key ID associated with the key-enabled API request. |
| <code>$context.identity.caller</code> | The principal identifier of the caller making the request. |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$context.identity.cognitoAuthenticationProvider</code></td>
<td>The Amazon Cognito authentication provider used by the caller making the request. Available only if the request was signed with Amazon Cognito credentials. For information related to this and the other Amazon Cognito <code>$context</code> variables, see Using Federated Identities in the Amazon Cognito Developer Guide.</td>
</tr>
<tr>
<td><code>$context.identity.sourceIp</code></td>
<td>The source IP address of the TCP connection making the request to API Gateway.</td>
</tr>
<tr>
<td><code>$context.identity.user</code></td>
<td>The principal identifier of the user making the request.</td>
</tr>
<tr>
<td><code>$context.identity.userAgent</code></td>
<td>The User Agent of the API caller.</td>
</tr>
<tr>
<td><code>$context.identity.userArn</code></td>
<td>The Amazon Resource Name (ARN) of the effective user identified after authentication.</td>
</tr>
<tr>
<td><code>$context.integrationLatency</code></td>
<td>The integration latency in ms, available for access logging only.</td>
</tr>
<tr>
<td><code>$context.requestTime</code></td>
<td>The CLF-formatted request time (dd/MMM/yyyy:HH:mm:ss +-hhmm).</td>
</tr>
<tr>
<td><code>$context.requestTimeEpoch</code></td>
<td>The Epoch-formatted request time.</td>
</tr>
<tr>
<td><code>$context.stage</code></td>
<td>The deployment stage of the API call (for example, Beta or Prod).</td>
</tr>
<tr>
<td><code>$input.body</code></td>
<td>Returns the raw payload as a string.</td>
</tr>
<tr>
<td><code>$input.json(x)</code></td>
<td>This function evaluates a JSONPath expression and returns the results as a JSON string. For example, <code>$input.json('$.pets')</code> will return a JSON string representing the pets structure. For more information about JSONPath, see JSONPath or JSONPath for Java.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| `$input.path(x)` | Takes a JSONPath expression string (x) and returns a JSON object representation of the result. This allows you to access and manipulate elements of the payload natively in Apache Velocity Template Language (VTL).

For example, if the expression `$input.path('$.pets')` returns an object like this:

```json
[
  {
    "id": 1,
    "type": "dog",
    "price": 249.99
  },
  {
    "id": 2,
    "type": "cat",
    "price": 124.99
  },
  {
    "id": 3,
    "type": "fish",
    "price": 0.99
  }
]
```

`$input.path('$.pets').count()` would return "3".

For more information about JSONPath, see [JSONPath](https://jsonpath.com) or [JSONPath for Java](https://www.jsonpath.org/).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$stageVariables.&lt;variable_name&gt;</code></td>
<td><code>&lt;variable_name&gt;</code> represents a stage variable name.</td>
</tr>
<tr>
<td><code>$stageVariables['&lt;variable_name&gt;']</code></td>
<td><code>&lt;variable_name&gt;</code> represents any stage variable name.</td>
</tr>
<tr>
<td><code>{{stageVariables['&lt;variable_name&gt;']}}</code></td>
<td><code>&lt;variable_name&gt;</code> represents any stage variable name.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>$util.escapeJavaScript()</code></td>
<td>Escapes the characters in a string using JavaScript string rules.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This function will turn any regular single quotes (') into escaped ones ('). However, the escaped single quotes are not valid in JSON. Thus, when the output from this function is used in a JSON property, you must turn any escaped single quotes (') back to regular single quotes ('). This is shown in the following example:</td>
</tr>
<tr>
<td></td>
<td><code>$util.escapeJavaScript(data).replaceAll(\&quot;\&quot;,\&quot;\&quot;)</code></td>
</tr>
<tr>
<td><code>$util.parseJson()</code></td>
<td>Takes &quot;stringified&quot; JSON and returns an object representation of the result. You can use the result from this function to access and manipulate elements of the payload natively in Apache Velocity Template Language (VTL). For example, if you have the following payload:</td>
</tr>
<tr>
<td></td>
<td><code>{&quot;errorMessage&quot;:{&quot;key1&quot;:&quot;var1&quot;,&quot;key2&quot;:{&quot;arr&quot;:[1,2,3]}}}</code></td>
</tr>
<tr>
<td></td>
<td>and use the following mapping template</td>
</tr>
<tr>
<td></td>
<td><code>#set ($errorMessageObj = $util.parseJson($input.path('$.errorMessage')))</code></td>
</tr>
<tr>
<td></td>
<td><code>{&quot;errorMessageObjKey2ArrVal&quot;: $errorMessageObj.key2.arr[0]}</code></td>
</tr>
<tr>
<td></td>
<td>You will get the following output:</td>
</tr>
<tr>
<td></td>
<td><code>{&quot;errorMessageObjKey2ArrVal&quot;: 1}</code></td>
</tr>
<tr>
<td><code>$util.urlEncode()</code></td>
<td>Converts a string into &quot;application/x-www-form-urlencoded&quot; format.</td>
</tr>
<tr>
<td><code>$util.urlDecode()</code></td>
<td>Decodes an &quot;application/x-www-form-urlencoded&quot; string.</td>
</tr>
<tr>
<td><code>$util.base64Encode()</code></td>
<td>Encodes the data into a base64-encoded string.</td>
</tr>
<tr>
<td><code>$util.base64Decode()</code></td>
<td>Decodes the data from a base64-encoded string.</td>
</tr>
</tbody>
</table>
Publishing Your API Gateway APIs

Once you’ve deployed your APIs, you can publish them by deploying a developer portal, and you can sell your APIs as a SaaS through the AWS Marketplace. You can also create a custom domain name for your API. You can export your API definitions to generate an SDK for your users to call the API using a supported programming language. And you can use a canary release for testing new changes.

Topics
- Use the Serverless Developer Portal to Catalog Your API Gateway APIs (p. 630)
- Sell Your API Gateway APIs through AWS Marketplace (p. 638)
- Set Up a Custom Domain Name for an API in API Gateway (p. 641)
- Export a REST API from API Gateway (p. 663)
- Set up an API Gateway Canary Release Deployment (p. 666)

Use the Serverless Developer Portal to Catalog Your API Gateway APIs

A developer portal is an application that you use to make your APIs available to your customers. The Serverless Developer Portal can be used to publish API Gateway-managed APIs directly from API Gateway. You can also use it to publish non-API Gateway-managed APIs by uploading OpenAPI definitions for them. When you publish APIs in a Serverless Developer Portal, your customers can easily:

- Discover which APIs are available.
- Browse your API documentation.
- Register for – and immediately receive – their own API key that can be used to build applications.
- Try out your APIs in the developer portal UI.
- Monitor their own API usage.

Amazon API Gateway publishes a regularly updated serverless developer portal in the AWS Serverless Application Repository and on GitHub. It is released under the Apache 2.0 license, letting you customize and incorporate it into your build and deployment tools. The front end is written in React and is designed to be fully customizable. See https://github.com/awslabs/aws-api-gateway-developer-portal/wiki/Customization.

For more information about the AWS Serverless Application Repository, see the AWS Serverless Application Repository Developer Guide.

Tip
If you’d like to try out an example serverless developer portal, see https://developer.exampleapigateway.com/.

Topics
- Create a developer portal (p. 631)
- Developer portal settings (p. 632)
- Create an Admin user for your developer portal (p. 634)
Create a developer portal

You can deploy the API Gateway developer portal as-is or customize it to fit your branding. There are two ways to deploy your developer portal:

- By using the AWS Serverless Application Repository. Just choose the Deploy button to launch the API Gateway Serverless developer portal AWS CloudFormation stack and enter a handful of stack parameters in the Lambda console.
- By downloading the API Gateway serverless developer portal from the AWS GitHub repository and launching the API Gateway Serverless developer portal AWS CloudFormation stack from the AWS SAM CLI.

To deploy the serverless developer portal using the AWS Serverless Application Repository

1. Go to the API Gateway serverless developer portal page in the AWS Serverless Application Repository.
2. Choose Deploy.
   
   Note
   You may be prompted to sign into the AWS Lambda console.
3. In the Lambda console, you’ll need to fill out the required developer portal stack parameters (p. 632) under Application settings.
   
   Note
   The S3 bucket names and the Amazon Cognito domain prefix are required; the other settings are optional.
4. If you wish to enable the Got an opinion? customer feedback button, you'll need to:
   - Enter an email address in the DevPortalAdminEmail box. When a customer submits feedback, email will be sent to this address.
     
     Note
     If you don’t supply an email address, the Got an opinion? will not appear in the developer portal.
   - You can optionally enter a table name in the DevPortalFeedbackTableName box. The default name is DevPortalFeedback. When a customer submits feedback, it will be stored in a DynamoDB table with this name.
5. Choose the checkbox next to I acknowledge that this app creates custom IAM roles.
6. Choose Deploy.
7. If you entered an email address in the AdminEmail stack parameter, an Amazon SNS subscription email is sent to that email address to confirm that you’d like to subscribe to the Amazon SNS topic that you specified in the MarketplaceSubscriptionTopicProductCode setting.

To download and deploy the serverless developer portal using AWS SAM

1. Ensure that you have the latest AWS CLI and AWS SAM CLI installed and configured.
2. Download or clone the API Gateway serverless developer portal repo to a local directory.

3. Ensure that you have a privately accessible Amazon S3 bucket to upload zipped Lambda functions into. If you don't have one, you can create one using the Amazon S3 console or CLI.

   In the SAM CLI, run the following command from the project root, replacing `your-lambda-artifacts-bucket-name` with the name of your Amazon S3 bucket:

   ```
   sam package --template-file ./cloudformation/template.yaml --output-template-file ./cloudformation/packaged.yaml --s3-bucket {your-lambda-artifacts-bucket-name}
   ```

4. For this step, see the section called "Developer portal settings" (p. 632) for more information about parameters (such as `CognitoDomainNameOrPrefix`) that follow `--parameter-override`.

   **Note**

   Ensure that you have a privately accessible Amazon S3 bucket to upload the SAM template into. (AWS CloudFormation will read the template from the bucket to deploy the developer portal.) This can be the same bucket that you specified in the previous step for uploading the zipped Lambda functions.

   Run the following command from the project root, replacing:

   - `{your-template-bucket-name}` with the name of your Amazon S3 bucket
   - `{custom-prefix}` with a prefix that is globally unique
   - `{cognito-domain-or-prefix}` with a unique string.

   ```
   sam deploy --template-file ./cloudformation/packaged.yaml --s3-bucket {your-template-bucket-name} --stack-name "{custom-prefix}-dev-portal" --capabilities CAPABILITY_NAMED_IAM --parameter-override CognitoDomainNameOrPrefix="{cognito-domain-or-prefix}" DevPortalSiteS3BucketName="{custom-prefix}-dev-portal-static-assets" ArtifactsS3BucketName="{custom-prefix}-dev-portal-artifacts"
   ```

Once your developer portal has been fully deployed, you can get its URL as follows.

**To get the URL for your newly created developer portal**

1. Open the AWS CloudFormation management console.
2. Choose the name of the stack (aws-serverless-repository-api-gateway-dev-portal is the default stack name).
3. Open the Outputs section. The URL for the developer portal is specified in the `WebSiteURL` property.

**Developer portal settings**

The following are settings you'll need to set during and after deployment of your developer portal:

**Note**

Many of the settings below can be changed after you've deployed your developer portal, by updating the AWS CloudFormation stack. For more information, see AWS CloudFormation Stack Updates.

**ArtifactsS3BucketName (REQUIRED)**

The deployment process will create a privately accessible Amazon S3 bucket where the catalog metadata will be stored. Specify a name to assign to the bucket. This name must be globally unique.
CognitoDomainNameOrPrefix (REQUIRED)

This string is used with the Amazon Cognito hosted UI for user sign-up and sign-in. Specify a unique domain name or prefix string.

CognitoIdentityPoolName

The deployment process will create a Amazon Cognito identity pool. The default name for the identity pool is DevPortalUserPool.

CustomDomainNameAcmCertArn

If you provided a domain name associated with an ACM certificate, then you must also specify here the ACM certificate's ARN. Leave this blank to create a developer portal without a custom domain name.

DevPortalAdminEmail

Specify an email address to enable the Got an opinion? customer feedback button. When a customer submits feedback, email will be sent to this address.

**Note**

If you don't supply an email address, the Got an opinion? button will not appear in the developer portal.

DevPortalFeedbackTableName

If you specify an email address for DevPortalAdminEmail, the deployment process will create a DynamoDB table to store feedback entered by customers. The default name is DevPortalFeedback. You can optionally specify your own table name.

DevPortalCustomersTableName

The deployment process will create a DynamoDB table where customer accounts will be stored. You can optionally specify a name to assign to this table. It must be unique within your account region. The default name of the table is DevPortalCustomers.

DevPortalSiteS3BucketName (REQUIRED)

The deployment process will create a privately accessible Amazon S3 bucket where the web application code will be stored. Specify a name to assign to this bucket. This name must be globally unique.

MarketplaceSubscriptionTopicProductCode

This is the Amazon SNS topic suffix for subscribe/unsubscribe events. Enter the desired value. The default value is DevPortalMarketplaceSubscriptionTopic. This setting is only relevant if you're using AWS Marketplace integration. For more information, see Configuring Your SaaS Product to Accept New Customers.

StaticAssetRebuildMode

By default, a static asset rebuild doesn't overwrite custom content. Specify overwrite-content to replace the custom content with your local version.

**Important**

If you specify overwrite-content, all custom changes in your Amazon S3 bucket will be lost. Don't do this unless you know what you're doing.

StaticAssetRebuildToken

Provide a token different from the last deployment's token to re-upload the developer portal site's static assets. You can provide a timestamp or GUID on each deployment to always re-upload the assets.
Create an Admin user for your developer portal

Once you've deployed your developer portal, you'll want to create at least one Admin user. You do that by creating a new user and adding that user to the administrator group for the Amazon Cognito user pool that AWS CloudFormation created when you deployed the developer portal.

Create an Admin user

1. In your developer portal, choose Register.
2. Enter an email address and password and choose Register.
3. In a separate browser tab, sign in to the Amazon Cognito console.
5. Choose the user pool for your developer portal that you set when you deployed the developer portal.
6. Choose the user to promote to administrator.
7. Choose Add to group.
8. From the dropdown menu, choose the \{stackname\}-dev-portalAdminsGroup, where \{stackname\} is the stack name from when you deployed the developer portal.
9. Choose Add to group.
10. In your developer portal, log out and log back in using the same credentials. You should now see an Admin Panel link in the upper right corner, next to My Dashboard.

Publish an API Gateway-managed API to your developer portal

The following steps outline how you, as the API owner, publish an API to your developer portal so that your customers can subscribe to it.

Step 1: Make an API Gateway-managed API available for publishing

1. If you have not already done so, deploy the API to a stage (p. 495).
2. If you have not already done so, create a usage plan (p. 432) and associate it with the API stage for the deployed API.

   Note
   You do not need to associate API keys with the usage plan. The developer portal will do this for you.

3. Sign in to the Developer Portal and go to the Admin Panel.
4. You should see the API in the Admin Panel API list. In the API list, APIs are grouped by usage plan. The Not Subscribable No Usage Plan group lists the APIs that aren't associated with a usage plan.

Step 2: Make the API Gateway-managed API visible in the developer portal

1. In the Admin Panel API list, check the Displayed value for your API. When it's first uploaded, this value will be set to False.
2. To make the API visible in the developer portal, choose the `False` button. Its value will change to `True`, indicating that the API is now visible.

   **Tip**
   To make all APIs in a usage plan visible, choose the `False` or `Partial` button in the header bar for the usage plan.

3. Navigate to the APIs panel to see the developer portal as your customers see it. You should see your API listed in the left navigation column.

   If the API is deployed to a stage that's associated with a usage plan, you'll see a `Subscribe` button for the API. This button causes the customer's API key to be associated with the usage plan that the API is associated with.

Now that the API Gateway-managed API is displayed, you can enable SDK generation so that your customers to download an SDK for it.

**Step 3: Enable SDK generation**

1. In the Admin Panel API list, choose the `Disabled` button. Its value will change to `Enabled`, indicating that SDK generation is now allowed.

2. Navigate to the APIs panel and choose your API in the left navigation column. You should now see a `Download SDK` button for it.

   If you choose the `Download SDK` button, you should see a list of SDK types that you can download.

**Update or delete an API Gateway-managed API**

If you make changes to your API in API Gateway after you've published it, you'll need to redeploy it.

**To update an API Gateway-managed API**

1. Make the desired changes to the API in the API Gateway console, AWS CLI, or an SDK.
2. Redeploy the API to the same stage as before.
3. In the developer portal, in the Admin Panel API list, choose Update. This updates the API that's displayed in the developer portal UI.

   **Note**
   The `Download SDK` button always gets the latest deployed version of your API, even if you don't update it in the developer portal.

4. Navigate to the APIs panel and choose your API in the left navigation column. You should see your changes.

To stop displaying an API in the developer portal API list (without revoking customers' access to it):

1. In the Admin Panel API list, check the `Displayed` value for your API. If the API is visible, this value will be set to `True`.
2. To make the API invisible, choose the `True` button. Its value will change to `False`, indicating that the API is now invisible.
3. Navigate to the APIs panel. You should no longer see your API listed in the left navigation column.

To revoke customers' access to an API without deleting it entirely, you must do one of the following in the API Gateway console (p. 438) or the API Gateway CLI or REST API (p. 443):

- Remove the API keys from the usage plan.
To remove a non-API Gateway-managed API

To stop displaying a non-API Gateway-managed API and remove customers' access to it, choose **Delete**. This won't delete the API, but it will delete its OpenAPI specification file from the developer portal.

Publish a non-API Gateway-managed API to your developer portal

The following steps outline how you publish non-API Gateway-managed (or "generic") APIs to your customers. You can upload OpenAPI 2.0 (Swagger) or 3.x definitions for the APIs in **JSON**, **YAML**, or **YML** files.

**To publish a non-API Gateway-managed API in your developer portal**

1. Sign in to the **Developer Portal** and go to the **Admin Panel**.
2. Under **Generic APIs**, choose **Add API**.
3. Browse to the directory where the OpenAPI files for your APIs reside and choose the files to upload.
4. Choose **Upload**.
   
   **Note**
   
   If any of the files can't be parsed or don't contain an API title, you'll get a warning, and those files won't be uploaded. All other files will be uploaded. You'll need to choose the x icon to dismiss the dialog.
5. You should now see your API listed under **Generic APIs**. If you don't, navigate away from the **Admin Panel** and back to it again to refresh the list.

How your customers use your developer portal

To build applications and test your APIs, your customers will need to create developer accounts by registering with your developer portal.

**To create a developer account and get an API key**

1. In the developer portal, choose **Register**.
2. Enter an email address and password and choose **Register**.
3. To locate the API key, choose **My Dashboard**.

A developer account gives your customer an API key, which is typically needed to use and test your APIs, and enables usage tracking for both you and your customers.

When a customer first registers, their new API key won't be tied to any of your APIs.

**To activate the API key for an API**

1. Choose **APIs**.
2. Choose the API from the API list and choose **Subscribe**.

   This causes the API key to be associated with the usage plan that the API is associated with.
The customer has now subscribed to the API, and they can make calls to methods on the API. Daily usage statistics for the API will be displayed in MyDashboard.

A customer can try out API methods in the developer portal UI without subscribing.

**Note**
If any of the API's methods require an API key, an Authorize button will appear above the method list. Methods that require an API key will have a black lock icon. To try out methods that require an API key, choose the Authorize button and enter a valid API key that's associated with the usage plan for the API stage.
You can safely ignore the Authorize button when it appears on APIs that you're already subscribed to.

**To try out an API without subscribing**
1. Navigate to the API in the API list.
2. Choose an API method to expand it.
3. Choose **Try it out**.
4. Choose **Execute**.

Your customers can submit customer feedback to you as follows:

**To submit feedback for an API**
1. Choose Got an opinion?.
2. In the popup window, enter comments.
3. Choose **Submit**.

The customer's feedback is stored in the DynamoDB table for the developer portal. The default name of this table is DevPortalFeedback. Also, email is sent to the email addresses that was specified in the DevPortalAdminEmail field. If no email address was specified when the developer portal was deployed, the Got an opinion? does not appear.

**Note**
If you change the name of this table, you must use a name that is unique within your account region.

If you've enabled SDK generation for the API in the Admin Panel, the customer can download an SDK for it.

**To download an SDK for an API**
1. Choose the Download SDK button for the desired API.
2. Choose the desired SDK platform or language as follows:
   - For **Android**:
     1. For **Group ID**, type the unique identifier for the corresponding project. This is used in the pom.xml file (for example, com.mycompany).
     2. For **Invoker package**, type the namespace for the generated client classes (for example, com.mycompany.clientsdk).
     3. For **Artifact ID**, type the name of the compiled .jar file without the version. This is used in the pom.xml file (for example, aws-apigateway-api-sdk).
     4. For **Artifact version**, type the artifact version number for the generated client. This is used in the pom.xml file and should follow a major.minor.patch pattern (for example, 1.0.0).
   - For **JavaScript**, the SDK is downloaded immediately.
• For **iOS (Objective-C)** or **iOS (Swift)**, Type a unique prefix in the **Prefix** box.

The effect of prefix is as follows: if you assign, for example, `SIMPLE_CALC` as the prefix for the SDK of the SimpleCalc (p. 527) API with Input, Output, and Result models, the generated SDK will contain the `SIMPLE_CALC`SimpleCalcClient class that encapsulates the API, including the method requests/responses. In addition, the generated SDK will contain the `SIMPLE_CALC`Input, `SIMPLE_CALC`Output, and `SIMPLE_CALC`Result classes to represent the input, output, and results, respectively, to represent the request input and response output. For more information, see Use iOS SDK Generated by API Gateway for a REST API in Objective-C or Swift (p. 548).

• For **Java**:

  1. For **Service Name**, specify the name of your SDK. For example, `SimpleCalcSdk`. This becomes the name of your SDK client class. The name corresponds to the `<name>` tag under `<project>` in the `pom.xml` file, which is in the SDK's project folder. Do not include hyphens.

  2. For **Java Package Name**, specify a package name for your SDK. For example, `examples.aws.apig.simpleCalc.sdk`. This package name is used as the namespace of your SDK library. Do not include hyphens.

• For **Ruby**, for **Service Name**, specify the name of your SDK. For example, `SimpleCalc`. This is used to generate the Ruby Gem namespace of your API. The name must be all letters, (a–zA–z), without any other special characters or numbers.

### Best Practices for Developer Portals

The following are suggested best practices to follow when deploying a developer portal.

• In most cases, you'll only want to deploy one developer portal for all of your APIs. In some cases, you may choose to have separate developer portals for development and production versions of your APIs. It is not recommended to use more than one developer portal for production APIs.

• When you create a usage plan and associate it with a stage, you don't need to associate any API keys with the usage plan. The developer portal will do this for you.

• Note that, if any APIs in a given usage plan are visible, **all** APIs in that usage plan are subscribable, even if you haven’t made them visible to your customers.

### Sell Your API Gateway APIs through AWS Marketplace

After you build, test, and deploy your APIs, you can package them in an API Gateway **usage plan** (p. 432) and sell the plan as a Software as a Service (SaaS) product through AWS Marketplace. API buyers subscribing to your product offering are billed by AWS Marketplace based on the number of requests made to the usage plan.

To sell your APIs on AWS Marketplace, you must set up the sales channel to integrate AWS Marketplace with API Gateway. Generally speaking, this involves listing your product on AWS Marketplace, setting up an IAM role with appropriate policies to allow API Gateway to send usage metrics to AWS Marketplace, associating an AWS Marketplace product with an API Gateway usage plan, and associating an AWS Marketplace buyer with an API Gateway API key. Details are discussed in the following sections.

To enable your customers to buy your product on AWS Marketplace, you must register your developer portal (an external application) with AWS Marketplace. The developer portal must handle the subscription requests that are redirected from the AWS Marketplace console.

For a sample developer portal application, see the [API Gateway Developer Portal](#).
For more information about selling your API as a SaaS product on AWS Marketplace, see the AWS Marketplace User Guide.

Topics
- Initialize AWS Marketplace Integration with API Gateway (p. 639)
- Handle Customer Subscription to Usage Plans (p. 640)

Initialize AWS Marketplace Integration with API Gateway

The following tasks are for one-time initialization of AWS Marketplace integration with API Gateway, which enables you to sell your APIs as a SaaS product.

List a Product on AWS Marketplace

To list your usage plan as a SaaS product, submit a product load form through AWS Marketplace. The product must contain a dimension named `apigateway` of the `requests` type. This dimension defines the price-per-request and is used by API Gateway to meter requests to your APIs.

Create the Metering Role

Create an IAM role named `ApiGatewayMarketplaceMeteringRole` with the following execution policy and trust policy. This role allows API Gateway to send usage metrics to AWS Marketplace on your behalf.

Execution Policy of the Metering Role

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-marketplace:BatchMeterUsage",
        "aws-marketplace:ResolveCustomer"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

Trusted Relationship Policy of the Metering Role

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "apigateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```
Associate Usage Plan with AWS Marketplace Product

When you list a product on AWS Marketplace, you receive an AWS Marketplace product code. To integrate API Gateway with AWS Marketplace, associate your usage plan with the AWS Marketplace product code. You enable the association by setting the API Gateway UsagePlan’s `productCode` field to your AWS Marketplace product code, using the API Gateway console, the API Gateway REST API, the AWS CLI for API Gateway, or AWS SDK for API Gateway. The following code example uses the API Gateway REST API:

```
PATCH /usageplans/USAGE_PLAN_ID
Host: apigateway.region.amazonaws.com
Authorization: ...;

{
    "patchOperations" : [
        {
            "path" : "/productCode",
            "value" : "MARKETPLACE_PRODUCT_CODE",
            "op" : "replace"
        }
    ]
}
```

Handle Customer Subscription to Usage Plans

The following tasks are handled by your developer portal application.

When a customer subscribes to your product through AWS Marketplace, AWS Marketplace forwards a POST request to the SaaS subscriptions URL that you registered when listing your product on AWS Marketplace. The POST request comes with an `x-amzn-marketplace-token` header parameter containing buyer information. Follow the instructions in Configuring Your SaaS Product to Accept New Customers to handle this redirect in your developer portal application.

Responding to a customer’s subscribing request, AWS Marketplace sends a `subscribe-success` notification to an Amazon SNS topic that you can subscribe to. (See Configuring Your SaaS Product to Accept New Customers). To accept the customer subscription request, you handle the `subscribe-success` notification by creating or retrieving an API Gateway API key for the customer, associating the customer’s AWS Marketplace-provisioned `customerId` with the API keys, and then adding the API key to your usage plan.

When the customer’s subscription request completes, the developer portal application should present the customer with the associated API key and inform the customer that the API key must be included in the `x-api-key` header in requests to the APIs.

When a customer cancels a subscription to a usage plan, AWS Marketplace sends an `unsubscribe-success` notification to the SNS topic. To complete the process of unsubscribing the customer, you handle the `unsubscribe-success` notification by removing the customer’s API keys from the usage plan.

Authorize a Customer to Access a Usage Plan

To authorize access to your usage plan for a given customer, use the API Gateway API to fetch or create an API key for the customer and add the API key to the usage plan.

The following example shows how to call the API Gateway REST API to create a new API key with a specific AWS Marketplace customerId value (`MARKETPLACE_CUSTOMER_ID`).

```
POST apikeys HTTP/1.1
Host: apigateway.region.amazonaws.com
Authorization: ...;

```
The following example shows how to get an API key with a specific AWS Marketplace `customerId` value (
\texttt{MARKETPLACE\_CUSTOMER\_ID}).

\begin{verbatim}
GET apikeys?customerId=MARKETPLACE\_CUSTOMER\_ID HTTP/1.1
Host: apigateway.region.amazonaws.com
Authorization: ...
\end{verbatim}

To add an API key to a usage plan, create a UsagePlanKey with the API key for the relevant usage plan. The following example shows how to accomplish this using the API Gateway REST API, where n371pt is the usage plan ID and q5ugs7qjjh is an example API keyId returned from the preceding examples.

\begin{verbatim}
POST /usageplans/n371pt/keys HTTP/1.1
Host: apigateway.region.amazonaws.com
Authorization: ...

{  
  "keyId": "q5ugs7qjjh",
  "keyType": "API\_KEY"
}
\end{verbatim}

### Associate a Customer with an API Key

You must update the ApiKey's customerId field to the AWS Marketplace customer ID of the customer. This associates the API key with the AWS Marketplace customer, which enables metering and billing for the buyer. The following code example calls the API Gateway REST API to do that.

\begin{verbatim}
PATCH /apikeys/q5ugs7qjjh
Host: apigateway.region.amazonaws.com
Authorization: ...

{  
  "patchOperations" : [{  
    "path": "/customerId",
    "value": "MARKETPLACE\_CUSTOMER\_ID",
    "op": "replace"
  }]  
}
\end{verbatim}

### Set Up a Custom Domain Name for an API in API Gateway

\textbf{Note}

It is now possible to choose a minimum TLS version that your API supports. For REST APIs, you can choose TLS 1.2 or TLS 1.0. For WebSocket APIs, you can only choose TLS 1.2.
After deploying your REST or WebSocket API, you (and your customers) can invoke the API using the default base URL of the following format:

https://api-id.execute-api.region.amazonaws.com/stage

where api-id is generated by API Gateway, region is specified by you when creating the API, and stage is specified by you when deploying the API.

**Note**

A custom domain can be associated with a REST API or a Websocket API, but not both. Custom domain names are not supported for private APIs (p. 194).

The host name portion of the URL (i.e., api-id.execute-api.region.amazonaws.com) refers to an API endpoint, which can be edge-optimized or regional. The default API endpoint can be difficult to recall and not user-friendly. To provide a simpler and more intuitive URL for your API users, you can set up a custom domain name (e.g., api.example.com) as the API's host name and choose a base path (e.g., myservice) to map the alternative URL to this API. The more user-friendly API base URL now becomes:

https://api.example.com/myservice

If you do not set any base mapping under a custom domain name, the resulting API's base URL is the same as the custom domain (e.g., https://api.example.com). In this case, the custom domain name cannot support more than one API.

When you deploy an edge-optimized API, API Gateway sets up an Amazon CloudFront distribution and a DNS record to map the API domain name to the CloudFront distribution domain name. Requests for the API are then routed to API Gateway through the mapped CloudFront distribution.

When you create a custom domain name for an edge-optimized API, API Gateway sets up a CloudFront distribution. But you must set up a DNS record to map the custom domain name to the CloudFront distribution domain name for API requests bound for the custom domain name to be routed to API Gateway through the mapped CloudFront distribution. You must also provide a certificate for the custom domain name.

When you create a custom domain name for a regional API, API Gateway creates a regional domain name for the API. You must set up a DNS record to map the custom domain name to the regional domain name for API requests bound for the custom domain name to be routed to API Gateway through the mapped regional API endpoint. You must also provide a certificate for the custom domain name.

**Note**

The CloudFront distribution created by API Gateway is owned by a region-specific account affiliated with API Gateway. When tracing operations to create and update such a CloudFront distribution in CloudWatch logs, you must use this API Gateway account ID. For more information, see Log Custom Domain Name Creation in CloudTrail (p. 652).

To set up an edge-optimized custom domain name or to update its certificate, you must have a permission to update CloudFront distributions. You can do so by attaching the following IAM policy statement to an IAM user, group or role in your account:

```json
{
   "Version": "2012-10-17",
   "Statement": [ 
      {
         "Sid": "AllowCloudFrontUpdateDistribution",
         "Effect": "Allow",
         "Action": [ "cloudfront:updateDistribution" ],
         "Resource": [ "*" ]
      }
   ]
}
```
API Gateway supports edge-optimized custom domain names by leveraging Server Name Indication (SNI) on the CloudFront distribution. For more information on using custom domain names on a CloudFront distribution, including the required certificate format and the maximum size of a certificate key length, see Using Alternate Domain Names and HTTPS in the Amazon CloudFront Developer Guide.

To set up a custom domain name as your API's host name, you, as the API owner, must provide an SSL/TLS certificate for the custom domain name.

To provide a certificate for an edge-optimized custom domain name, you can request AWS Certificate Manager (ACM) to generate a new certificate in ACM or to import into ACM one issued by a third-party certificate authority in the us-east-1 region (Northern Virginia).

To provide a certificate for a regional custom domain name in a region where ACM is supported, you must request a certificate from ACM. To provide a certificate for a regional custom domain name in a region where ACM is not supported, you must import a certificate to API Gateway in that region.

To import an SSL/TLS certificate, you must provide the PEM-formatted SSL/TLS certificate body, its private key, and the certificate chain for the custom domain name. Each certificate stored in ACM is identified by its ARN. To use an AWS-managed certificate for a domain name, you simply reference its ARN.

ACM makes it straightforward to set up and use a custom domain name for an API: create in or import into ACM a certificate for the given domain name, set up the domain name in API Gateway with the ARN of the certificate provided by ACM, and map a base path under the custom domain name to a deployed stage of the API. With certificates issued by ACM, you do not have to worry about exposing any sensitive certificate details, such as the private key.

You must have a registered Internet domain name in order to set up custom domain names for your APIs. If needed, you can register an Internet domain using Amazon Route 53 or using a third-party domain registrar of your choice. An API's custom domain name can be the name of a subdomain or the root domain (aka, zone apex) of a registered Internet domain.

After a custom domain name is created in API Gateway, you must create or update your domain name service (DNS) provider's resource record to map the edge-optimized custom domain name to its CloudFront distribution domain name or to map the regional custom domain name to its regional API endpoint. Without such a mapping, API requests bound for the custom domain name cannot reach API Gateway.

**Note**

An edge-optimized custom domain name is created in a specific region and owned by a specific AWS account. Moving such a custom domain name between regions or AWS accounts involves deleting the existing CloudFront distribution and creating a new one. The process may take approximately 30 minutes before the new custom domain name becomes available. For more information, see Updating CloudFront Distributions.

The following pages describe how to use ACM to create an SSL/TLS certificate for a custom domain name, to set up the custom domain name for an API, to associate a specific API with a base path under the custom domain name, and to renew (aka rotate) an expiring certificate that was imported into ACM for the custom domain name.

**Topics**

- Get Certificates Ready in AWS Certificate Manager (p. 644)
- Choose a Minimum TLS Version for a Custom Domain in API Gateway (p. 646)
- How to Create an Edge-Optimized Custom Domain Name (p. 649)
- Set Up a Custom Domain Name for a Regional REST API or WebSocket API in API Gateway (p. 655)
Get Certificates Ready in AWS Certificate Manager

Before setting up a custom domain name for an API, you must have an SSL/TLS certificate ready in AWS Certificate Manager. The following steps describe how to get this done. For more information, see the AWS Certificate Manager User Guide.

Note
To use an ACM Certificate with an API Gateway edge-optimized custom domain name, you must request or import the certificate in the US East (N. Virginia) (us-east-1) Region. For an API Gateway regional custom domain name, you must request or import the certificate in the same region as your API.

To get a certificate for a given domain name issued by or imported into ACM

1. Register your Internet domain; e.g., myDomain.com. You can use either Amazon Route 53 or a third-party accredited domain registrar. For a list of such registrars, see Accredited Registrar Directory at the ICANN website.
2. To create in or import into ACM an SSL/TLS certificate for a domain name, do one of the following:

   **To request a certificate provided by ACM for a domain name**
   1. Sign in to the AWS Certificate Manager console.
   2. Choose Request a certificate.
   3. Type a custom domain name for your API; e.g., api.example.com, in Domain name.
   4. Optionally, choose Add another name to this certificate.
   5. Choose Review and request.
   6. Choose Confirm and request.
   7. For a valid request, a registered owner of the Internet domain must consent to the request before ACM issues the certificate.

   **To import into ACM a certificate for a domain name**
   1. Get a PEM-encoded SSL/TLS certificate for your custom domain name from a certificate authority. For a partial list of such CAs, see the Mozilla Included CA List
      a. Generate a private key for the certificate and save the output to a file, using the OpenSSL toolkit at the OpenSSL website:

         openssl genrsa -out private-key-file 2048

      **Note**
      Amazon API Gateway leverages Amazon CloudFront to support certificates for custom domain names. As such, the requirements and constraints of a custom domain name SSL/TLS certificate are dictated by CloudFront. For example, the maximum size of the public key is 2048 and the private key size can be 1024, 2048, and 4096. The public key size is determined by the certificate authority you use. Ask your certificate authority to return keys of a size different from the default length. For more information, see Secure access to your objects and Create signed URLs and signed cookies.
      b. Generate a certificate signing request (CSR) with the previously generated private key, using OpenSSL:
openssl req -new -sha256 -key private-key-file -out CSR-file

c. Submit the CSR to the certificate authority and save the resulting certificate.
d. Download the certificate chain from the certificate authority.

**Note**
If you obtain the private key in another way and the key is encrypted, you can use the following command to decrypt the key before submitting it to API Gateway for setting up a custom domain name.

```
openssl pkcs8 -topk8 -inform pem -in MyEncryptedKey.pem -outform pem -nocrypt -out MyDecryptedKey.pem
```

2. Upload the certificate to AWS Certificate Manager:
   a. Sign in to the AWS Certificate Manager console.
   b. Choose *Import a certificate*.
   c. For **Certificate body**, type or paste the body of the PEM-formatted server certificate from your certificate authority. The following shows an abbreviated example of such a certificate.

```
-----BEGIN CERTIFICATE-----
EXAMPLECA+KgAwIBAgIQJ1XxJ8Pl++gOfQtj0IBoqDANBgkqhkiG9w0BAQUFADBB ...
az8Cg1aicxLBQ7EaWIhhgEXAMPLE
-----END CERTIFICATE-----
```

d. For **Certificate private key**, type or paste your PEM-formatted certificate's private key. The following shows an abbreviated example of such a key.

```
-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAKCAQEA2Qb3LDHD7StY7Wj6U2/opV6Xu37qUCckeDWhwp2MYJ9/nETO ...
1qGvJ3u04vdnzaYN5WoyN5LFckrlA71+CszD1CGSqbVDWEXAMPLE
-----END RSA PRIVATE KEY-----
```

e. For **Certificate chain**, type or paste the PEM-formatted intermediate certificates and, optionally, the root certificate, one after the other without any blank lines. If you include the root certificate, your certificate chain must start with intermediate certificates and end with the root certificate. Use the intermediate certificates provided by your certificate authority. Do not include any intermediaries that are not in the chain of trust path. The following shows an abbreviated example.

```
-----BEGIN CERTIFICATE-----
EXAMPLECA4ugAwIBAgIQWrYdrB5NogYUx1U9Pamy3DANBgkqhkiG9w0BAQUFADCB ...
8/if81IKse2e4/hEfcEejJx/arbxlBJCHBv1EFNsdw8EXAMPLE
-----END CERTIFICATE-----
```

Here is another example.

```
-----BEGIN CERTIFICATE-----
Intermediate certificate 2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate certificate 1
-----END CERTIFICATE-----
```
Choose a Minimum TLS Version for a Custom Domain in API Gateway

For greater security, you can choose a minimum Transport Layer Security (TLS) protocol version to be enforced for your Amazon API Gateway custom domain by setting a security policy in the API Gateway console, AWS CLI, or AWS SDKs.

A security policy is a predefined combination of minimum TLS version and cipher suite offered by Amazon API Gateway. You can choose either a TLS version 1.2 or TLS version 1.0 security policy. The TLS protocol addresses network security problems such as tampering and eavesdropping between a client and server. When your clients establish a TLS handshake to your API through the custom domain, the security policy enforces the TLS version and cipher suite options your clients can choose to use.

In custom domain settings, a security policy determines two settings:

- The minimum TLS version that API Gateway uses to communicate with API clients
- The cipher that API Gateway uses to encrypt the content that it returns to API clients

Topics
- How to Specify a Minimum TLS Protocol Version for Custom Domains in API Gateway (p. 646)
- Supported Security Policies, TLS Protocol Versions, and Ciphers for Edge-Optimized API Endpoints in API Gateway (p. 647)
- Supported SSL/TLS Protocols and Ciphers for Regional, Private, and WebSocket API Endpoints in API Gateway (p. 647)
- OpenSSL and RFC Cipher Names (p. 648)

How to Specify a Minimum TLS Protocol Version for Custom Domains in API Gateway

When you create a custom domain, you specify the security policy for it. For more information about security policies, see the tables in the following sections.

The following sections describe how to create a custom domain name, including specifying the minimum TLS version in the API Gateway console and CLI:

- the section called “How to Create an Edge-Optimized Custom Domain Name” (p. 649)
- the section called “Set Up a Regional Custom Domain Name for REST or WebSocket API” (p. 655)

You can change the security policy by updating the domain name settings. To change the minimum TLS version, use one of the following commands, specifying the new TLS version (TLS_1_0 or TLS_1_2) in the securityPolicy parameter. Allow up to 60 minutes for the update to be completed.

- domainname: update
- update-domain-name
Supported Security Policies, TLS Protocol Versions, and Ciphers for Edge-Optimized API Endpoints in API Gateway

The following table lists the protocols and ciphers that API Gateway can use for each security policy for edge-optimized APIs.

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>TLSv1.2</th>
<th>TLSv1.1</th>
<th>TLSv1</th>
<th>SSLv3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ciphers Supported</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA256</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA384</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES128-GCM-SHA256</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES256-GCM-SHA384</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES128-SHA256</td>
<td>♦</td>
<td>♦</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES256-SHA</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES128-SHA</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DES-CBC3-SHA</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RC4-MD5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Supported SSL/TLS Protocols and Ciphers for Regional, Private, and WebSocket API Endpoints in API Gateway

The following table describes the security policies that can be specified for regional, private, and WebSocket API endpoints.

**Note**
For private and WebSocket APIs, only TLS-1-2 can be specified.

<table>
<thead>
<tr>
<th>Security Policy</th>
<th>TLS-1-0</th>
<th>TLS-1-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS Protocols</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Choose a Minimum TLS Version for a Custom Domain

Security Policy | TLS-1-0 | TLS-1-2 |
--- | --- | --- |
Protocol-TLSv1 | ♦ | |
Protocol-TLSv1.1 | ♦ | |
Protocol-TLSv1.2 | ♦ | ♦

TLS Ciphers

<table>
<thead>
<tr>
<th>OpenSSL Cipher Name</th>
<th>RFC Cipher Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-ECDSA-AES128-GCM-SHA256</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td></td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES128-SHA256</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA256</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES128-SHA</td>
<td></td>
</tr>
<tr>
<td>ECDHE-RSA-AES128-SHA</td>
<td></td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-GCM-SHA384</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-GCM-SHA384</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-SHA384</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA384</td>
<td>♦</td>
</tr>
<tr>
<td>ECDHE-RSA-AES256-SHA</td>
<td></td>
</tr>
<tr>
<td>ECDHE-ECDSA-AES256-SHA</td>
<td></td>
</tr>
<tr>
<td>AES128-GCM-SHA256</td>
<td>♦</td>
</tr>
<tr>
<td>AES128-SHA256</td>
<td>♦</td>
</tr>
<tr>
<td>AES128-SHA</td>
<td></td>
</tr>
<tr>
<td>AES256-GCM-SHA384</td>
<td>♦</td>
</tr>
<tr>
<td>AES256-SHA256</td>
<td>♦</td>
</tr>
<tr>
<td>AES256-SHA</td>
<td></td>
</tr>
<tr>
<td>AES-CBC3-SHA</td>
<td></td>
</tr>
</tbody>
</table>

OpenSSL and RFC Cipher Names

OpenSSL and IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, use different names for the same ciphers. The following table maps the OpenSSL name to the RFC name for each cipher.

<table>
<thead>
<tr>
<th>OpenSSL Cipher Name</th>
<th>RFC Cipher Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDHE-RSA-AES128-GCM-SHA256</td>
<td>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</td>
</tr>
</tbody>
</table>
OpenSSL Cipher Name | RFC Cipher Name
---|---
ECDHE-RSA-AES128-SHA256 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ECDHE-RSA-AES128-SHA | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ECDHE-RSA-AES256-GCM-SHA384 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ECDHE-RSA-AES256-SHA384 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
ECDHE-RSA-AES256-SHA | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
AES128-GCM-SHA256 | TLS_RSA_WITH_AES_128_GCM_SHA256
AES256-GCM-SHA384 | TLS_RSA_WITH_AES_256_GCM_SHA384
AES128-SHA256 | TLS_RSA_WITH_AES_128_CBC_SHA256
AES256-SHA | TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA | TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA | TLS_RSA_WITH_3DES_EDE_CBC_SHA
RC4-MD5 | TLS_RSA_WITH_RC4_128_MD5

How to Create an Edge-Optimized Custom Domain Name

Topics

- Set Up an Edge-Optimized Custom Domain Name for an API Gateway API (p. 649)
- Log Custom Domain Name Creation in CloudTrail (p. 652)
- Configure Base Path Mapping of an API with a Custom Domain Name as its Host Name (p. 653)
- Rotate a Certificate Imported into ACM (p. 654)
- Call Your API with Custom Domain Names (p. 654)

Set Up an Edge-Optimized Custom Domain Name for an API Gateway API

The following procedure describes how to set up a custom domain name for an API using the API Gateway console.

To set up a custom domain name using the API Gateway console

2. Choose **Custom Domain Names** from the main navigation pane.
3. Choose **Create Custom Domain Name** next.
4. Under **New Custom Domain Name**:
   a. For the API protocol, choose **HTTP**.
   b. Under **Domain Name**, type a custom domain name, for example, `my-api.example.com`, in **Domain Name**.
      
      **Note**
      Do not use the wildcard character (i.e., `*`) for your custom domain names. API Gateway does not support it, even though the API Gateway console (or the AWS CLI) accepts it and can map it to a CloudFront distribution. However, you can use wildcard certificates.
   d. Under **Endpoint Configuration**, choose **Edge optimized**.
   e. Choose a certificate from the **ACM Certificate** list.
      
      **Note**
      To use an ACM certificate with an API Gateway edge-optimized custom domain name, you must request or import the certificate in the **us-east-1** region (Northern Virginia).
   f. Choose **Add mapping** under **Base Path Mappings** to set a base path (**Path**) for a deployed API in a given stage (selected from the **Destination** dropdown lists.) You can also set the base path mapping after the custom domain name is created. For more information, see **Configure Base Path Mapping of an API with a Custom Domain Name as its Host Name** (p. 653).
   g. Choose **Save**.
5. After the custom domain name is created, the console displays the associated CloudFront distribution domain name, in the form of `distribution-id.cloudfront.net`, along with the certificate ARN. Note the CloudFront distribution domain name shown in the output. You need it in the next step to set the custom domain's CNAME value or A-record alias target in your DNS.
   
   **Note**
   The newly created custom domain name takes about 40 minutes to be ready. In the meantime, you can configure the DNS record alias to map the custom domain name to the associated CloudFront distribution domain name and to set up the base path mapping for the custom domain name while the custom domain name is being initialized.

6. In this step, we use Amazon Route 53 as an example DNS provider to show how to set up an A-record alias for your Internet domain to map the custom domain name to the associated CloudFront distribution name. The instructions can be adapted to other DNS providers.
   a. Sign in to the Route 53 console.
   b. Create an **A-IPv4 address** record set for your custom domain (e.g., `api.example.com`). An A-record maps a custom domain name to an IP4 address.
   c. Choose **Yes** for **Alias**, type the CloudFront domain name (e.g., `d3boq9ikothtgw.cloudfront.net`) in **Alias Target**, and then choose **Create**. The A-record alias here maps your custom domain name to the specified CloudFront domain name that is itself mapped to an IP4 address.
**Tip**

The **Alias Hosted Zone ID** identifies the hosted zone of the specified **Alias Target**. The Route 53 console automatically fills in the value when you enter a valid domain name for **Alias Target**. To create an A-record alias without using the Route 53 console, such as when you use the AWS CLI, you must specified the required hosted zone Id. For any CloudFront
distribution domain name, the hosted zone Id value is always Z2FDTNDATAQYW2, as documented in AWS Regions and Endpoints for CloudFront.

For most DNS providers, a custom domain name is added to the hosted zone as a CNAME resource record set. The CNAME record name specifies the custom domain name you typed earlier in Domain Name (for example, api.example.com). The CNAME record value specifies the domain name for the CloudFront distribution. However, use of a CNAME record will not work if your custom domain is a zone apex (i.e., example.com instead of api.example.com). A zone apex is also commonly known as the root domain of your organization. For a zone apex you need to use an A-record alias, provided that is supported by your DNS provider.

With Route 53 you can create an A record alias for your custom domain name and specify the CloudFront distribution domain name as the alias target, as shown above. This means that Route 53 can route your custom domain name even if it is a zone apex. For more information, see Choosing Between Alias and Non-Alias Resource Record Sets in the Amazon Route 53 Developer Guide.

Use of A-record aliases also eliminates exposure of the underlying CloudFront distribution domain name because the domain name mapping takes place solely within Route 53. For these reasons, we recommend that you use Route 53 A-record alias whenever possible.

In addition to using the API Gateway console, you can use the API Gateway REST API, AWS CLI or one of the AWS SDKs to set up the custom domain name for your APIs. As an illustration, the following procedure outlines the steps to do so using the REST API calls.

**To set up a custom domain name using the API Gateway REST API**

1. Call `domainname:create`, specifying the custom domain name and the ARN of a certificate stored in AWS Certificate Manager.

   The successful API call returns a 201 Created response containing the certificate ARN as well as the associated CloudFront distribution name in its payload.

2. Note the CloudFront distribution domain name shown in the output. You need it in the next step to set the custom domain's CNAME value or A-record alias target in your DNS.

3. Follow Step 6 of the previous procedure to set up an A-record alias to map the custom domain name to its CloudFront distribution name.

For code examples of this REST API call, see `domainname:create`.

**Log Custom Domain Name Creation in CloudTrail**

When CloudTrail is enabled for logging API Gateway calls made by your account, API Gateway logs the associated CloudFront distribution updates when a custom domain name is created or updated for an API. Because these CloudFront distributions are owned by API Gateway, each of these reported CloudFront distributions is identified by one of the following region-specific API Gateway account IDs, instead of the API owner's account ID.

**Region-specific API Gateway account IDs of CloudFront distributions associated with a custom domain name**

<table>
<thead>
<tr>
<th>Region</th>
<th>Account ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td>392220576650</td>
</tr>
<tr>
<td>us-east-2</td>
<td>718770453195</td>
</tr>
<tr>
<td>us-west-1</td>
<td>968246515281</td>
</tr>
</tbody>
</table>
Region | Account ID
--- | ---
us-west-2 | 109351309407
eu-west-1 | 631144002099
eu-west-2 | 544388816663
eu-central-1 | 474240146802
ap-northeast-1 | 969236854626
ap-northeast-2 | 020402002396
ap-southeast-1 | 195145609632
ap-southeast-2 | 798376113853

### Configure Base Path Mapping of an API with a Custom Domain Name as its Host Name

You can use a single custom domain name as the host name of multiple APIs. You achieve this by configuring the base path mappings on the custom domain name. With the base path mappings, an API under the custom domain is accessible through the combination of the custom domain name and the associated base path.

For example, if you created an API named PetStore and another API named PetShop and set up a custom domain name of api.example.com in API Gateway, you can set the PetStore API's URL as https://api.example.com or https://api.example.com/myPetStore. The PetStore API is associated with the base path of an empty string or myPetStore under the custom domain name of api.example.com. Similarly, you can assign a base path of yourPetShop for the PetShop API. The URL of https://api.example.com/yourPetShop is then the root URL of the PetShop API.

Before setting the base path for an API, complete the steps in Set Up an Edge-Optimized Custom Domain Name for an API Gateway API (p. 649).

**To set the base path for API mappings using the API Gateway console**

1. Choose a custom domain name from the list of available Custom Domain Names list under your account.
2. Choose Show Base Path Mappings or Edit.
3. Choose Add mapping.
4. (Optional) Type a base path name for Path, choose an API from Destination, and then choose a stage.

   **Note**
   The Destination list shows the deployed APIs under your account.
5. Choose Save to finish setting up the base path mapping for the API.

   **Note**
   To delete a mapping after you create it, next to the mapping that you want to delete, choose the trash icon.

In addition, you can call the API Gateway REST API, AWS CLI, or one of the AWS SDKs to set up the base path mapping of an API with a custom domain name as its host name. As an illustration, the following procedure outlines the steps to do so using the REST API calls.
To set up the base path mapping of an API using the API Gateway REST API

- Call `bapathmapping:create` on a specific custom domain name, specifying the `basePath`, `restApiId`, and a deployment stage property in the request payload.

The successful API call returns a 201 Created response.

For code examples of the REST API call, see `bapathmapping:create`.

Rotate a Certificate Imported into ACM

ACM automatically handles renewal of certificates it issues. You do not need to rotate any ACM-issued certificates for your custom domain names. CloudFront handles it on your behalf.

However, if you import a certificate into ACM and use it for a custom domain name, you must rotate the certificate before it expires. This involves importing a new third-party certificate for the domain name and rotate the existing certificate to the new one. You need to repeat the process when the newly imported certificate expires. Alternatively, you can request ACM to issue a new certificate for the domain name and rotate the existing one to the new ACM-issued certificate. After that, you can leave ACM and CloudFront to handle the certificate rotation for you automatically. To create or import a new ACM Certificate, follow the steps to request or import a new ACM Certificate (p. 644) for the specified domain name.

To rotate a certificate for a domain name, you can use the API Gateway console, the API Gateway REST API, AWS CLI, or one of the AWS SDKs.

**To rotate an expiring certificate imported into ACM using the API Gateway console**

1. Request or import a certificate in ACM.
2. Go back to the API Gateway console.
3. Choose **Custom Domain Names** from the API Gateway console main navigation pane.
4. Select the custom domain name of your choice, under the **Custom Domain Names** pane.
5. Choose **Edit**.
6. Choose the desired certificate from the **ACM Certificate** dropdown list.
7. Choose **Save** to begin rotating the certificate for the custom domain name.

**Note**

It takes about 40 minutes for the process to finish. After the rotation is done, you can choose the two-way arrow icon next to **ACM Certificate** to roll back to the original certificate.

To illustrate how to programmatically rotate an imported certificate for a custom domain name, we outline the steps using the API Gateway REST API.

**Rotate an imported certificate using the API Gateway REST API**

- Call `domainname:update` action, specifying the ARN of the new ACM Certificate for the specified domain name.

**Call Your API with Custom Domain Names**

Calling an API with a custom domain name is the same as calling the API with its default domain name, provided that the correct URL is used.
The following examples compare and contrast a set of default URLs and corresponding custom URLs of two APIs (udxjef and qf3duz) in a specified region (us-east-1), and of a given custom domain name (api.example.com).

### Root URLs of APIs with default and custom domain names

<table>
<thead>
<tr>
<th>API ID</th>
<th>Stage</th>
<th>Default URL</th>
<th>Base path</th>
<th>Custom URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>udxjef</td>
<td>pro</td>
<td><a href="https://udxjef.execute-api.us-east-1.amazonaws.com/pro">https://udxjef.execute-api.us-east-1.amazonaws.com/pro</a></td>
<td>/petstore</td>
<td><a href="https://api.example.com/petstore">https://api.example.com/petstore</a></td>
</tr>
<tr>
<td>qf3duz</td>
<td>dev</td>
<td><a href="https://qf3duz.execute-api.us-east-1.amazonaws.com/dev">https://qf3duz.execute-api.us-east-1.amazonaws.com/dev</a></td>
<td>/bookstore</td>
<td><a href="https://api.example.com/bookstore">https://api.example.com/bookstore</a></td>
</tr>
<tr>
<td>qf3duz</td>
<td>tst</td>
<td><a href="https://qf3duz.execute-api.us-east-1.amazonaws.com/tst">https://qf3duz.execute-api.us-east-1.amazonaws.com/tst</a></td>
<td>/bookstand</td>
<td><a href="https://api.example.com/bookstand">https://api.example.com/bookstand</a></td>
</tr>
</tbody>
</table>

API Gateway supports custom domain names for an API by using Server Name Indication (SNI). You can invoke the API with a custom domain name using a browser or a client library that supports SNI.

API Gateway enforces SNI on the CloudFront distribution. For information on how CloudFront uses custom domain names, see Amazon CloudFront Custom SSL.

### Set Up a Custom Domain Name for a Regional REST API or WebSocket API in API Gateway

As with an edge-optimized API endpoint, you can create a custom domain name for a regional API endpoint. To support a regional custom domain name, you must provide a certificate. If an AWS Certificate Manager (ACM) Certificate is used, this certificate must be region-specific. If ACM is available in the region, you must provide an ACM Certificate specific to that region. If ACM is not supported in the region, you must upload a certificate to API Gateway in that region when creating the regional custom domain name. For more information about creating or uploading a custom domain name certificate, see Get Certificates Ready in AWS Certificate Manager (p. 644).

**Important**

For an API Gateway regional custom domain name, you must request or import the certificate in the same region as your API.

When you create a regional custom domain name (or migrate one) with an ACM Certificate, API Gateway creates a service-linked role in your account, if the role does not exist already. The service-linked role is required to attach your ACM Certificate to your regional endpoint. The role is named
Set Up a Regional Custom Domain Name for REST or WebSocket API

AWSServiceRoleForAPIGateway and will have the APIGatewayServiceRolePolicy managed policy attached to. For more information about use of the service-linked role, see Using Service-Linked Roles.

Important
You must create a DNS record to point the custom domain name to the regional domain name. This enables the traffic that is bound to the custom domain name to be routed to the API's regional host name. The DNS record can be of the CNAME or A type.

Topics
• Set Up a Regional Custom Domain Name With ACM Certificate Using the API Gateway Console (p. 656)
• Set Up a Regional Custom Domain Name With ACM Certificate Using AWS CLI (p. 656)
• Set Up a Regional Custom Domain Name Certificate Without ACM Using AWS CLI (p. 658)

Set Up a Regional Custom Domain Name With ACM Certificate Using the API Gateway Console

To use the API Gateway console to set up a regional custom domain name, use the following procedure.

To set up a regional custom domain name using the API Gateway console

1. Sign in to the API Gateway console and choose Custom Domain Names in the primary navigation pane.
2. Choose +Create New Custom Domain Name above the Custom Domain Names table.
3. Under New Custom Domain Name:
   a. Choose the API protocol: HTTP or WebSocket.
   b. Under Domain Name, type a custom domain name, for example, my-api.example.com, in Domain Name.
5. Under Endpoint Configuration, choose Regional.
6. Choose a certificate from the ACM Certificate drop-down list. The certificate must be from the same region where the API is deployed.
7. If you have created and deployed an API to use this custom domain name, choose Add mapping, type a base path under the custom domain name in Path, choose an API from the API drop-down list under Destination, and choose a stage from the Stage drop-down list. To add another base path mapping, repeat the step. You can also set the base path mapping after the custom domain name is created. For more information, see Configure Base Path Mapping of an API with a Custom Domain Name as its Host Name (p. 653).
8. Choose Save.
9. Follow the Route 53 documentation on configuring Route 53 to route traffic to API Gateway.

Set Up a Regional Custom Domain Name With ACM Certificate Using AWS CLI

To use the AWS CLI to set up a custom domain name for a regional API, use the following procedure.

1. Call create-domain-name, specifying a custom domain name of the REGIONAL type and the ARN of a regional certificate.

   ```bash
   aws apigateway create-domain-name \
   ```
Set Up a Regional Custom Domain Name for REST or WebSocket API

```
--domain-name 'regional.example.com' \ 
--endpoint-configuration types=REGIONAL \ 
--regional-certificate-arn 'arn:aws:acm:us-west-2:123456789012:certificate/c19332f0-3be6-457f-a244-e03a423084e6'
```

Note that the specified certificate is from the us-west-2 region and for this example, we assume that the underlying API is from the same region.

If successful, the call returns a result similar to the following:

```
{
  "certificateUploadDate": "2017-10-13T23:02:54Z",
  "domainName": "regional.example.com",
  "endpointConfiguration": {
    "types": "REGIONAL"
  },
  "regionalCertificateArn": "arn:aws:acm:us-west-2:123456789012:certificate/c19332f0-3be6-457f-a244-e03a423084e6",
  "regionalDomainName": "d-numh1z56v6.execute-api.us-west-2.amazonaws.com"
}
```

The regionalDomainName property value returns the regional API's host name. You must create a DNS record to point your custom domain name to this regional domain name. This enables the traffic that is bound to the custom domain name to be routed to this regional API's host name.

2. Create a DNS record to associate the custom domain name and the regional domain name. This enables requests that are bound to the custom domain name to be routed to the API's regional host name.

3. Add a base path mapping to expose the specified API (for example, 0qzs2sy7bh) in a deployment stage (for example, test) under the specified custom domain name (for example, regional.example.com).

```
aws apigateway create-base-path-mapping \
--domain-name 'regional.example.com' \ 
--base-path 'RegionalApiTest' \ 
--rest-api-id 0qzs2sy7bh \ 
--stage 'test'
```

As a result, the base URL using the custom domain name for the API that is deployed in the stage becomes https://regional.example.com/RegionalApiTest.

4. Configure your DNS records to map the regional custom domain name to its host name of the given hosted zone ID. First create a JSON file that contains the configuration for setting up a DNS record for the regional domain name. The following example shows how to create a DNS A record to map a regional custom domain name (regional.example.com) to its regional host name (d-numh1z56v6.execute-api.us-west-2.amazonaws.com) provisioned as part of the custom domain name creation. The DNSName and HostedZoneId properties of AliasTarget can take the regionalDomainName and regionalHostedZoneId values, respectively, of the custom domain name. You can also get the regional Route 53 Hosted Zone IDs in API Gateway Regions and Endpoints.

```
{
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "regional.example.com",
        "Type": "A",
        "AliasTarget": {
          "DNSName": "d-numh1z56v6.execute-api.us-west-2.amazonaws.com",
          "HostedZoneId": "Z2VJ58B8YI37JH"
        }
      }
    }
  ]
}
```
Set Up a Regional Custom Domain Name Certificate Without ACM Using AWS CLI

To use the AWS CLI to set up a custom domain name for a regional API in regions where ACM is not available, you'll need to upload the certificate directly to API Gateway by using the following procedure.

To upload a server certificate to API Gateway, you must provide the certificate and its matching private key. When the certificate is not self-signed, you must also provide a certificate chain. (You don't need a certificate chain when uploading a self-signed certificate.) Before you upload a certificate, ensure that you have all these items and that they meet the following criteria:

- The certificate must be valid at the time of upload. You cannot upload a certificate before its validity period begins (the certificate's `NotBefore` date) or after it expires (the certificate's `NotAfter` date).
- The private key must be unencrypted. You cannot upload a private key that is protected by a password or passphrase. For help decrypting an encrypted private key, see Troubleshooting.
- The certificate, private key, and certificate chain must all be PEM-encoded. For help converting these items to PEM format, see Troubleshooting.

1. Create the following PEM files. If you use different filenames, you'll need to change the filenames in the `create-domain-name` command to match.

   - Store the PEM-encoded certificate in a file named `Certificate.pem`.
   - Store the PEM-encoded certificate chain in a file named `CertificateChain.pem`.
   - Store the PEM-encoded, unencrypted private key in a file named `PrivateKey.pem`.

2. To use the following example command, replace these file names with your own and replace `regional.example.com cert` with a name for your uploaded certificate. Type the command on one continuous line. The following example includes line breaks and extra spaces to make it easier to read.

   ```bash
   aws apigateway create-domain-name --domain-name 'regional.example.com'
   --regional-certificate-name 'regional.example.com cert'
   --certificate-body file://Certificate.pem
   --certificate-private-key file://PrivateKey.pem
   --certificate-chain file://CertificateChain.pem
   --endpoint-configuration types=REGIONAL
   ```

If successful, the call returns a result similar to the following:
The `regionalDomainName` property value returns the regional API's host name. You must create a DNS record to point your custom domain name to this regional domain name. This enables the traffic that is bound to the custom domain name to be routed to this regional API's host name.

3. Add a base path mapping to expose the specified API (for example, `0qzs2sy7bh`) in a deployment stage (for example, `test`) under the specified custom domain name (for example, `regional.example.com`).

   ```bash
   aws apigateway create-base-path-mapping \
   --domain-name 'regional.example.com' \
   --base-path 'RegionalApiTest' \
   --rest-api-id 0qzs2sy7bh \
   --stage 'test'
   ```

   As a result, the base URL using the custom domain name for the API that is deployed in the stage becomes `https://regional.example.com/RegionalApiTest`.

4. **Note**

   This step assumes that your domain is hosted in Route 53.

   Configure your DNS records to map the regional custom domain name to the target domain name. First create a JSON file that contains the configuration for setting up a DNS record for the regional domain name. The following example shows how to create a DNS A record to map a regional custom domain name (`regional.example.com`) to its regional host name (`d-numh1z56v6.execute-api.us-west-2.amazonaws.com`) provisioned as part of the custom domain name creation. The `DNSName` and `HostedZoneId` properties of `AliasTarget` can take the target domain name and hosted zone ID values, respectively, of the custom domain name that you see in the API Gateway console. You can also get the regional Route 53 Hosted Zone IDs in API Gateway Regions and Endpoints.

   ```json
   { 
   "Changes": [ 
   { 
   "Action": "CREATE", 
   "ResourceRecordSet": { 
   "Name": "regional.example.com", 
   "Type": "A", 
   "AliasTarget": { 
   "DNSName": "d-numh1z56v6.execute-api.us-west-2.amazonaws.com", 
   "HostedZoneId": "Z2OJLYMUO9EFXC", 
   "EvaluateTargetHealth": false 
   } 
   } 
   ]
   }
   ```

5. Run the following CLI command:
aws route53 change-resource-record-sets \
   --hosted-zone-id {your-hosted-zone-id} \
   --change-batch file://path/to/your/setup-dns-record.json

where {your-hosted-zone-id} is the Route 53 Hosted Zone ID of the DNS record set in your account. The change-batch parameter value points to a JSON file (setup-dns-record.json) in a folder (path/to/your).

Migrate a Custom Domain Name to a Different API Endpoint

You can migrate your custom domain name between edge-optimized and regional endpoints. You first add the new endpoint configuration type to the existing endpointConfiguration.types list for the custom domain name. Next, you set up a DNS record to point the custom domain name to the newly provisioned endpoint. An optional last step is to remove the obsolete custom domain name configuration data.

When planning the migration, remember that for an edge-optimized API's custom domain name, the required certificate provided by ACM must be from the US East (N. Virginia) Region (us-east-1). This certificate is distributed to all the geographic locations. However, for a regional API, the ACM Certificate for the regional domain name must be from the same region hosting the API. You can migrate an edge-optimized custom domain name that is not in the us-east-1 region to a regional custom domain name by first requesting a new ACM Certificate from the region that is local to the API.

It may take up to 60 seconds to complete a migration between an edge-optimized custom domain name and a regional custom domain name in API Gateway. For the newly created endpoint to become ready to accept traffic, the migration time also depends on when you update your DNS records.

Topics
• Migrate Regional and Edge-Optimized Domain Names Using the API Gateway Console (p. 660)
• Migrate Custom Domain Names Using the AWS CLI (p. 661)

Migrate Regional and Edge-Optimized Domain Names Using the API Gateway Console

To use the API Gateway console to migrate a regional custom domain name to an edge-optimized custom domain name and vice versa, use the following procedure.

To migrate a regional or edge-optimized custom domain name using the API Gateway console

1. Sign in to the API Gateway console and choose Custom Domain Names in the primary navigation pane.
2. Choose an existing domain name from Custom Domain Names, and then choose Edit.
3. Depending on the existing endpoint type, do the following:
   a. For an edge-optimized domain name, choose Add Regional Configuration.
   b. For a regional domain name, choose Add Edge Configuration.
4. Choose a certificate from the drop-down list.
5. Choose Save.
6. Choose Proceed to confirm adding the new endpoint.
7. Update the DNS records to point the new domain name to the newly provisioned target domain name.

**Migrate Custom Domain Names Using the AWS CLI**

To use the AWS CLI to migrate a custom domain name from an edge-optimized endpoint to a regional endpoint or vice versa, call the `update-domain-name` command to add the new endpoint type and, optionally, call the `update-domain-name` command to remove the old endpoint type.

**Topics**
- Migrate an Edge-Optimized Custom Domain Name to Regional (p. 661)
- Migrate a Regional Custom Domain Name to Edge-Optimized (p. 662)

**Migrate an Edge-Optimized Custom Domain Name to Regional**

To migrate an edge-optimized custom domain name to a regional custom domain name, call the `update-domain-name` command, as follows:

```bash
aws apigateway update-domain-name \
  --domain-name 'api.example.com' \
  --patch-operations [ \
    { op:'add', path: '/endpointConfiguration/types', value: 'REGIONAL' }, \
  ]
```

The regional certificate must be of the same region as the regional API.

The success response has a 200 OK status code and a body similar to the following:

```json
{
  "certificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/34a95aa1-77fa-427c-aa07-3a88b9d9f3c0a",
  "certificateName": "edge-cert",
  "certificateUploadDate": "2017-10-16T23:22:57Z",
  "distributionDomainName": "d1frvgze7y1bf.cloudfront.net",
  "domainName": "api.example.com",
  "endpointConfiguration": {
    "types": [
      "EDGE",
      "REGIONAL"
    ]
  },
  "regionalDomainName": "d-fdisjghyn6.execute-api.us-west-2.amazonaws.com"
}
```

For the migrated regional custom domain name, the resulting `regionalDomainName` property returns the regional API host name. You must set up a DNS record to point the regional custom domain name to this regional host name. This enables the traffic that is bound to the custom domain name to be routed to the regional host.

After the DNS record is set, you can remove the edge-optimized custom domain name by calling the `update-domain-name` command of AWS CLI:

```bash
aws apigateway update-domain-name \
```
Migrate a Regional Custom Domain Name to Edge-Optimized

To migrate a regional custom domain name to an edge-optimized custom domain name, call the `update-domain-name` command of the AWS CLI, as follows:

```bash
aws apigateway update-domain-name
--domain-name 'api.example.com'
--patch-operations [ \
    { op: 'add', path: '/endpointConfiguration/types', value: 'EDGE' }, \
    { op: 'add', path: '/certificateName', value: 'edge-cert' }, \
    { op: 'add', path: '/certificateArn', value: 'arn:aws:acm:us-east-1:123456789012:certificate/34a95aa1-77fa-427c-aa07-3a88bd9f3c0a' } \
]
```

The edge-optimized domain certificate must be created in the `us-east-1` region.

The success response has a 200 OK status code and a body similar to the following:

```json
{
    "certificateArn": "arn:aws:acm:us-east-1:738575810317:certificate/34a95aa1-77fa-427c-aa07-3a88bd9f3c0a",
    "certificateName": "edge-cert",
    "certificateUploadDate": "2017-10-16T23:22:57Z",
    "distributionDomainName": "d1frvgze7vylbf.cloudfront.net",
    "domainName": "api.example.com",
    "endpointConfiguration": {
        "types": ["EDGE", "REGIONAL"],
    },
    "regionalDomainName": "d-cgkq2qwgzf.execute-api.us-east-1.amazonaws.com"
}
```

For the specified custom domain name, API Gateway returns the edge-optimized API host name as the `distributionDomainName` property value. You must set a DNS record to point the edge-optimized custom domain name to this distribution domain name. This enables traffic that is bound to the edge-optimized custom domain name to be routed to the edge-optimized API host name.

After the DNS record is set, you can remove the `REGION` endpoint type of the custom domain name:

```bash
aws apigateway update-domain-name
--domain-name api.example.com
--patch-operations [ \
    { op: 'remove', path: '/endpointConfiguration/types', value: 'REGIONAL' }, \
    { op: 'remove', path: 'regionalCertificateArn' } \
]
```

The result of this command is similar to the following output, with only edge-optimized domain name configuration data:
Export a REST API from API Gateway

Once you created and configured a REST API in API Gateway, using the API Gateway console or otherwise, you can export it to an OpenAPI file using the API Gateway Export API, which is part of the Amazon API Gateway Control Service. You have options to include the API Gateway integration extensions, as well as the Postman extensions, in the exported OpenAPI definition file.

**Note**
When exporting the API using the AWS CLI, be sure to include the extensions parameter as shown in the following example, to ensure that the x-amazon-apigateway-request-validator extension is included:

```bash
aws apigateway get-export --parameters extensions='apigateway' --rest-api-id abcdedfg123 --stage-name dev --export-type swagger latestswagger2.json
```

You cannot export an API if its payloads are not of the application/json type. If you try, you will get an error response stating that JSON body models are not found.

### Request to Export a REST API

With the Export API, you export an existing REST API by submitting a GET request, specifying the to-be-exported API as part of URL paths. The request URL is of the following format:

**OpenAPI 3.0**

```
https://<host>/restapis/<restapi_id>/stages/<stage_name>/exports/oas30
```

**OpenAPI 2.0**

```
https://<host>/restapis/<restapi_id>/stages/<stage_name>/exports/swagger
```

You can append the extensions query string to specify whether to include API Gateway extensions (with the integration value) or Postman extensions (with the postman value).

In addition, you can set the Accept header to application/json or application/yaml to receive the API definition output in JSON or YAML format, respectively.
For more information about submitting GET requests using the API Gateway Export API, see Making HTTP Requests.

**Note**  
If you define models in your API, they must be for the content type of "application/json" for API Gateway to export the model. Otherwise, API Gateway throws an exception with the "Only found non-JSON body models for ..." error message. Models must contain properties or be defined as a particular JSONSchema type.

### Download REST API OpenAPI Definition in JSON

To export and download a REST API in OpenAPI definitions in JSON format:

**OpenAPI 3.0**

```plaintext
GET /restapis/<restapi_id>/stages/<stage_name>/exports/oas30
Host: apigateway.<region>.amazonaws.com
Accept: application/json
```

**OpenAPI 2.0**

```plaintext
GET /restapis/<restapi_id>/stages/<stage_name>/exports/swagger
Host: apigateway.<region>.amazonaws.com
Accept: application/json
```

Here, `<region>` could be, for example, `us-east-1`. For all the regions where API Gateway is available, see Regions and Endpoints.

### Download REST API OpenAPI Definition in YAML

To export and download a REST API in OpenAPI definitions in YAML format:

**OpenAPI 3.0**

```plaintext
GET /restapis/<restapi_id>/stages/<stage_name>/exports/oas30
Host: apigateway.<region>.amazonaws.com
Accept: application/yaml
```

**OpenAPI 2.0**

```plaintext
GET /restapis/<restapi_id>/stages/<stage_name>/exports/swagger
Host: apigateway.<region>.amazonaws.com
Accept: application/yaml
```
Download REST API OpenAPI Definition with Postman Extensions in JSON

To export and download a REST API in OpenAPI definitions with Postman in JSON format:

OpenAPI 3.0

GET /restapis/<restapi_id>/stages/<stage_name>/exports/oas30?extensions=postman
Host: apigateway.<region>.amazonaws.com
Accept: application/json

OpenAPI 2.0

GET /restapis/<restapi_id>/stages/<stage_name>/exports/swagger?extensions=postman
Host: apigateway.<region>.amazonaws.com
Accept: application/json

Download REST API OpenAPI Definition with API Gateway Integration in YAML

To export and download a REST API in OpenAPI definitions with API Gateway integration in YAML format:

OpenAPI 3.0

GET /restapis/<restapi_id>/stages/<stage_name>/exports/oas30?extensions=integrations
Host: apigateway.<region>.amazonaws.com
Accept: application/yaml

OpenAPI 2.0

GET /restapis/<restapi_id>/stages/<stage_name>/exports/swagger?extensions=integrations
Host: apigateway.<region>.amazonaws.com
Accept: application/yaml

Export REST API Using the API Gateway Console

After deploying your REST API to a stage (p. 495), you can proceed to export the API in the stage to an OpenAPI file using the API Gateway console.
From the *stage configuration* page in the API Gateway console, choose the *Export* tab and then one of the available options (Export as OpenAPI, Export as OpenAPI + API Gateway Integrations and Export as Postman) to download your API's OpenAPI definition.

### Set up an API Gateway Canary Release Deployment

**Canary release** is a software development strategy in which a new version of an API (as well as other software) is deployed as a canary release for testing purposes, and the base version remains deployed as a production release for normal operations on the same stage. For purposes of discussion, we refer to the base version as a production release in this documentation. Although this is reasonable, you are free to apply canary release on any non-production version for testing.

In a canary release deployment, total API traffic is separated at random into a production release and a canary release with a pre-configured ratio. Typically, the canary release receives a small percentage of API traffic and the production release takes up the rest. The updated API features are only visible to API traffic through the canary. You can adjust the canary traffic percentage to optimize test coverage or performance.

By keeping canary traffic small and the selection random, most users are not adversely affected at any time by potential bugs in the new version, and no single user is adversely affected all the time.

After the test metrics pass your requirements, you can promote the canary release to the production release and disable the canary from the deployment. This makes the new features available in the production stage.

**Topics**

- Canary Release Deployment in API Gateway (p. 666)
- Create a Canary Release Deployment (p. 667)
- Update a Canary Release (p. 671)
- Promote a Canary Release (p. 673)
- Disable a Canary Release (p. 675)

### Canary Release Deployment in API Gateway

In API Gateway, a canary release deployment uses the deployment stage for the production release of the base version of an API, and attaches to the stage a canary release for the new versions, relative to the base version, of the API. The stage is associated with the initial deployment and the canary with subsequent deployments. At the beginning, both the stage and the canary point to the same API version.
We use stage and production release interchangeably and use canary and canary release interchangeably throughout this section.

To deploy an API with a canary release, you create a canary release deployment by adding canary settings to the stage of a regular deployment. The canary settings describe the underlying canary release and the stage represents the production release of the API within this deployment. To add canary settings, set canarySettings on the deployment stage and specify the following:

- A deployment ID, initially identical to the ID of the base version deployment set on the stage.
- A percentage of API traffic, between 0.0 and 100.0 inclusive, for the canary release.
- Stage variables for the canary release that can override production release stage variables.
- The use of the stage cache for canary requests, if the useStageCache is set and API caching is enabled on the stage.

After a canary release is enabled, the deployment stage cannot be associated with another non-canary release deployment until the canary release is disabled and the canary settings removed from the stage.

When you enable API execution logging, the canary release has its own logs and metrics generated for all canary requests. They are reported to a production stage CloudWatch Logs log group as well as a canary-specific CloudWatch Logs log group. The same applies to access logging. The separate canary-specific logs are helpful to validate new API changes and decide whether to accept the changes and promote the canary release to the production stage, or to discard the changes and revert the canary release from the production stage.

The production stage execution log group is named API-Gateway-Execution-Logs/{rest-api-id}/{stage-name} and the canary release execution log group is named API-Gateway-Execution-Logs/{rest-api-id}/{stage-name}/Canary. For access logging, you must create a new log group or choose an existing one. The canary release access log group name has the /Canary suffix appended to the selected log group name.

A canary release can use the stage cache, if enabled, to store responses and use cached entries to return results to the next canary requests, within a pre-configured time-to-live (TTL) period.

In a canary release deployment, the production release and canary release of the API can be associated with the same version or with different versions. When they are associated with different versions, responses for production and canary requests are cached separately and the stage cache returns corresponding results for production and canary requests. When the production release and canary release are associated with the same deployment, the stage cache uses a single cache key for both types of requests and returns the same response for the same requests from the production release and canary release.

Create a Canary Release Deployment

You create a canary release deployment when deploying the API with canary settings as an additional input to the deployment creation operation.

You can also create a canary release deployment from an existing non-canary deployment by making a stage:update request to add the canary settings on the stage.

When creating a non-canary release deployment, you can specify a non-existing stage name. API Gateway creates one if the specified stage does not exist. However, you cannot specify any non-existing stage name when creating a canary release deployment. You will get an error and API Gateway will not create any canary release deployment.

You can create a canary release deployment in API Gateway using the API Gateway console, the AWS CLI, or an AWS SDK.
Create a Canary Deployment Using the API Gateway Console

To use the API Gateway console to create a canary release deployment, follow the instructions below:

**To create the initial canary release deployment**
1. Sign in to the API Gateway console.
2. Choose an existing API or create a new API.
3. Change the API, if necessary, or set up desired API methods and integrations.
4. Choose **Deploy API** from the **Actions** drop-down menu. Follow the on-screen instructions in **Deploy API** to deploy the API to a new stage.

So far, you have deployed the API to a production release stage. Next, you configure canary settings on the stage and, if needed, also enable caching, set stage variables, or configure API execution or access logs.

5. To enable API caching, choose the **Settings** tab in **Stage Editor** and follow the on-screen instructions. For more information, see the section called “Enable API Caching” (p. 500).
6. To set stage variables, choose the **Stage Variables** tab in **Stage Editor** and follow the on-screen instructions to add or modify stage variables. For more information, see the section called “Set up Stage Variables for a REST API” (p. 514).
7. To configure execution or access logging, choose the **Logs** tab in **Stage Editor** and follow the on-screen instructions. For more information, see Set Up CloudWatch API Logging in API Gateway (p. 510).
8. In **Stage Editor**, choose the **Canary** tab and then choose **Create Canary**.
9. Under the **Stage’s Request Distribution** section, choose the pencil icon next to **Percentage of requests to Canary** and type a number (for example, \(0.5\)) in the input text field. Choose the check mark icon to save the setting.
10. To associate an AWS WAF web ACL with the stage, choose a web ACL from the **Web ACL** dropdown list.

    **Note**
    If needed, choose **Create Web ACL** to open the AWS WAF console in a new browser tab, create the web ACL, and return to the API Gateway console to associate the web ACL with the stage.
11. If desired, choose **Block API Request if WebACL cannot be evaluated (Fail- Close)**.
12. If needed, choose **Add Stage Variables** to add them under the **Canary Stage Variables** section to override existing stage variables or add new stage variables for the canary release.
13. If desired, choose **Enable use of stage cache** to enable caching for the canary release and save your choice. The cache is not available for the canary release until API caching is enabled.

After the canary release is initialized on the deployment stage, you change the API and want to test the changes. You can redeploy the API to the same stage so that both the updated version and the base version are accessible through the same stage. The following steps describe how to do that.

**To deploy the latest API version to a canary**
1. With each update of the API, choose **Deploy API** from the **Actions** drop-down menu next to the **Resources** list.
2. In **Deploy API**, choose the now canary-enabled stage from the **Deployment stage** drop-down list.
3. Optionally, type a description in **Deployment description**.
4. Choose Deploy to push the latest API version to the canary release.
5. If desired, reconfigure the stage settings, logs, or canary settings, as describe in To create the initial canary release deployment (p. 668).

As a result, the canary release points to the latest version while the production release still points to the initial version of the API. The **canarySettings** now has a new **deploymentId** value, whereas the stage still has the initial **deploymentId** value. Behind the scenes, the console calls **stage:update**.

### Create a Canary Deployment Using the AWS CLI

First create a baseline deployment with two stage variables, but without any canary:

```bash
aws apigateway create-deployment
  --variables sv0=val0,sv1=val1
  --rest-api-id 4wk1k4onj3
  --stage-name prod
```

The command returns a representation of the resulting **Deployment**, similar to the following:

```json
{
  "id": "du4ot1",
  "createdDate": 1511379050
}
```

The resulting deployment **id** identifies a snapshot (or version) of the API.

Now create a canary deployment on the **prod** stage:

```bash
aws apigateway create-deployment
  --canary-settings '{
    "percentTraffic":10.5,
    "useStageCache":false,
    "stageVariableOverrides":{
      "sv1":"val2",
      "sv2":"val3"
    }
  }
  --rest-api-id 4wk1k4onj3
  --stage-name prod
```

If the specified stage (**prod**) does not exist, the preceding command returns an error. Otherwise, it returns the newly created **deployment** resource representation similar to the following:

```json
{
  "id": "a6rox0",
  "createdDate": 1511379433
}
```

The resulting deployment **id** identifies the test version of the API for the canary release. As a result, the associated stage is canary-enabled. You can view this stage representation by calling the **get-stage** command, similar to the following:

```bash
aws apigateway get-stage --rest-api-id 4wk1k4onj3 --stage-name prod
```
The following shows a representation of the Stage as the output of the command:

```json
{
    "stageName": "prod",
    "variables": {
        "sv0": "val0",
        "sv1": "val1"
    },
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "du4ot1",
    "lastUpdatedDate": 1511379433,
    "createdDate": 1511379050,
    "canarySettings": {
        "percentTraffic": 10.5,
        "deploymentId": "a6rox0",
        "useStageCache": false,
        "stageVariableOverrides": {
            "sv2": "val3",
            "sv1": "val2"
        }
    },
    "methodSettings": {}
}
```

In this example, the base version of the API will use the stage variables of \{"sv0":val0", "sv1":val1\"}, while the test version uses the stage variables of \{"sv1":val2", "sv2":val3\"}. Both the production release and canary release use the same stage variable of \sv1\ but with different values, val1 and val2, respectively. The stage variable of \sv0\ is used solely in the production release and the stage variable of \sv2\ is used in the canary release only.

You can create a canary release deployment from an existing regular deployment by updating the stage to enable a canary. To demonstrate this, create a regular deployment first:

```bash
aws apigateway create-deployment \
  --variables sv0=val0,sv1=val1 \
  --rest-api-id 4wk1k4onj3 \
  --stage-name beta
```

The command returns a representation of the base version deployment:

```json
{
    "id": "cifeiw",
    "createdDate": 1511380879
}
```

The associated beta stage does not have any canary settings:

```json
{
    "stageName": "beta",
    "variables": {
        "sv0": "val0",
        "sv1": "val1"
    },
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "cifeiw",
    "lastUpdatedDate": 1511380879,
    "createdDate": 1511380879,
    "methodSettings": {}
Now, create a new canary release deployment by attaching a canary on the stage:

```bash
aws apigateway update-stage \
  --patch-operations '[[ \
    "op":"replace", \
    "path":"/canarySettings/percentTraffic", \n    "value":"10.5" \n  ],[ \
    "op":"replace", \
    "path":"/canarySettings/useStageCache", \n    "value":"false" \n  ],[ \
    "op":"replace", \n    "path":"/canarySettings/stageVariableOverrides/sv1", \n    "value":"val2" \n  ],[ \
    "op":"replace", \n    "path":"/canarySettings/stageVariableOverrides/sv2", \n    "value":"val3" \n  ]}' \
  --rest-api-id 4wk1k4onj3  \
  --stage-name beta
```

A representation of the updated stage looks like this:

```json
{
    "stageName": "beta",
    "variables": {
        "sv0": "val0",
        "sv1": "val1"
    },
    "cacheClusterEnabled": false,
    "cacheClusterStatus": "NOT_AVAILABLE",
    "deploymentId": "cifeiw",
    "lastUpdatedDate": 1511381930,
    "createdDate": 1511380879,
    "canarySettings": {
        "percentTraffic": 10.5,
        "deploymentId": "cifeiw",
        "useStageCache": false,
        "stageVariableOverrides": {
            "sv2": "val3",
            "sv1": "val2"
        }
    },
    "methodSettings": {}
}
```

Because we just enabled a canary on an existing version of the API, both the production release (Stage) and canary release (canarySettings) point to the same deployment, i.e., the same version (deploymentId) of the API. After you change the API and deploy it to this stage again, the new version will be in the canary release, while the base version remains in the production release. This is manifested in the stage evolution when the deploymentId in the canary release is updated to the new deployment id and the deploymentId in the production release remains unchanged.

**Update a Canary Release**

After a canary release is deployed, you may want to adjust the percentage of the canary traffic or enable or disable the use of a stage cache to optimize the test performance. You can also modify stage variables...
used in the canary release when the execution context is updated. To make such updates, call the `stage:update` operation with new values on `canarySettings`.

You can update a canary release using the API Gateway console, the AWS CLI `update-stage` command or an AWS SDK.

**Topics**
- Update a Canary Release Using the API Gateway Console (p. 672)
- Update a Canary Release Using the AWS CLI (p. 672)

## Update a Canary Release Using the API Gateway Console

To use the API Gateway console to update existing canary settings on a stage, do the following:

1. Sign in to the API Gateway console and choose an existing API in the primary navigation pane.
2. Choose **Stages** under the API and then choose an existing stage under the **Stages** list to open the **Stage Editor**.
3. Choose the **Canary** tab in the **Stage Editor**.
4. Update **Percentage of requests directed to Canary** by increasing or decreasing the percentage number between 0.0 and 100.0, inclusive.
5. Update **Canary Stage Variables**, including adding, removing, or modifying a desired stage variable.
6. Update the **Enable use of stage cache** option by selecting or clearing the check box.
7. Save the changes.

## Update a Canary Release Using the AWS CLI

To use the AWS CLI to update a canary, call the `update-stage` command.

To enable or disable the use of a stage cache for the canary, call the `update-stage` command as follows:

```
aws apigateway update-stage          
  --rest-api-id {rest-api-id}      
  --stage-name '{stage-name}'      
  --patch-operations op=replace,path=/canarySettings/useStageCache,value=true
```

To adjust the canary traffic percentage, call `update-stage` to replace the `/canarySettings/percentTraffic` value on the **stage**.

```
aws apigateway update-stage          
  --rest-api-id {rest-api-id}      
  --stage-name '{stage-name}'      
  --patch-operations op=replace,path=/canarySettings/percentTraffic,value=25.0
```

To update canary stage variables, including adding, replacing, or removing a canary stage variable:

```
aws apigateway update-stage          
  --rest-api-id {rest-api-id}      
  --stage-name '{stage-name}'      
  --patch-operations '{[  
    "op": "replace",  
    "path": "/canarySettings/stageVariableOverides/newVar"  
    "value": "newVal",
    ],}'}
```
You can update all of the above by combining the operations into a single `patch-operations` value:

```bash
aws apigateway update-stage
  --rest-api-id {rest-api-id}
  --stage-name '{stage-name}'
  --patch-operations '[
    "op": "replace",
    "path": "/canarySettings/stageVariableOverides/var2",
    "value": "val4",
  ],
    "op": "remove",
    "path": "/canarySettings/stageVariableOverides/var1",
  ]'
```

### Promote a Canary Release

To promote a canary release makes it available in the production stage the API version under testing. The operation involves the following tasks:

- Reset the deployment ID of the stage with the deployment ID settings of the canary. This updates the API snapshot of the stage with the snapshot of the canary, making the test version the production release as well.

- Update stage variables with canary stage variables, if any. This updates the API execution context of the stage with that of the canary. Without this update, the new API version may produce unexpected results if the test version uses different stage variables or different values of existing stage variables.

- Set the percentage of canary traffic to 0.0%.

Promoting a canary release does not disable the canary on the stage. To disable a canary, you must remove the canary settings on the stage.

#### Topics

- Promote a Canary Release Using the API Gateway Console (p. 673)
- Promote a Canary Release Using the AWS CLI (p. 674)

### Promote a Canary Release Using the API Gateway Console

To use the API Gateway console to promote a canary release deployment, do the following:
1. Sign in to the API Gateway console and choose an existing API in the primary navigation pane.
2. Choose Stages under the API and then choose an existing stage under the Stages list to open the Stage Editor.
3. Choose the Canary tab in the Stage Editor.
5. Confirm changes to be made and choose Update.

After the promotion, the production release references the same API version (deploymentId) as the canary release. You can verify this using the AWS CLI. For example, see the section called “Promote a Canary Release Using the AWS CLI” (p. 674).

Promote a Canary Release Using the AWS CLI

To promote a canary release to the production release using the AWS CLI commands, call the update-stage command to copy the canary-associated deploymentId to the stage-associated deploymentId, to reset the canary traffic percentage to zero (0.0), and, to copy any canary-bound stage variables to the corresponding stage-bound ones.

Suppose we have a canary release deployment, described by a stage similar to the following:

```json
{
   "_links": {
      ...
   },
   "accessLogSettings": {
      ...
   },
   "cacheClusterEnabled": false,
   "cacheClusterStatus": "NOTAVAILABLE",
   "canarySettings": {
      "deploymentId": "eh1sby",
      "useStageCache": false,
      "stageVariableOverrides": {
         "sv2": "val3",
         "sv1": "val2"
      },
      "percentTraffic": 10.5
   },
   "createdDate": "2017-11-20T04:42:19Z",
   "deploymentId": "nfcn0x",
   "lastUpdatedDate": "2017-11-22T00:54:28Z",
   "methodSettings": {
      ...
   },
   "stageName": "prod",
   "variables": {
      "sv1": "val1"
   }
}
```

We call the following update-stage request to promote it:

```bash
aws apigateway update-stage
   --rest-api-id {rest-api-id} \
   --stage-name '{stage-name}' \
   --patch-operations '{
      "op": "replace",
      "value": "0.0"
   }
```

674
After the promotion, the stage now looks like this:

```json
{
  "_links": {
    ...
  },
  "accessLogSettings": {
    ...
  },
  "cacheClusterEnabled": false,
  "cacheClusterStatus": "NOT_AVAILABLE",
  "canarySettings": {
    "deploymentId": "eh1sby",
    "useStageCache": false,
    "stageVariableOverrides": {
      "sv2": "val3",
      "sv1": "val2"
    },
    "percentTraffic": 0
  },
  "createdDate": "2017-11-20T04:42:19Z",
  "deploymentId": "eh1sby",
  "lastUpdatedDate": "2017-11-22T05:29:47Z",
  "methodSettings": {
    ...
  },
  "stageName": "prod",
  "variables": {
    "sv2": "val3",
    "sv1": "val2"
  }
}
```

As you can see, promoting a canary release to the stage does not disable the canary and the deployment remains to be a canary release deployment. To make it a regular production release deployment, you must disable the canary settings. For more information about how to disable a canary release deployment, see the section called “Disable a Canary Release” (p. 675).

## Disable a Canary Release

To disable a canary release deployment is to set the **canarySettings** to null to remove it from the stage.

You can disable a canary release deployment using the API Gateway console, the AWS CLI, or an AWS SDK.

**Topics**
- Disable a Canary Release Using the API Gateway Console (p. 676)
- Disable a Canary Release Using the AWS CLI (p. 676)
Disable a Canary Release Using the API Gateway Console

To use the API Gateway console to disable a canary release deployment, use the following steps:

1. Sign in to the API Gateway console and choose an existing API in the primary navigation pane.
2. Choose Stages under the API and then choose an existing stage under the Stages list to open the Stage Editor.
3. Choose the Canary tab in the Stage Editor.
4. Choose Delete Canary.
5. Confirm you want to delete the canary by choosing Delete.

As a result, the canarySettings property becomes null and is removed from the deployment stage. You can verify this using the AWS CLI. For example, see the section called “Disable a Canary Release Using the AWS CLI” (p. 676).

Disable a Canary Release Using the AWS CLI

To use the AWS CLI to disable a canary release deployment, call the update-stage command as follows:

```bash
aws apigateway update-stage \
  --rest-api-id 4wk1k4onj3 \
  --stage-name canary \
  --patch-operations '"op":"remove", "path":"/canarySettings"'
```

A successful response returns a payload similar to the following:

```json
{
  "StageName": "prod",
  "accessLogSettings": {
    ...
  },
  "cacheClusterEnabled": false,
  "cacheClusterStatus": "NOT_AVAILABLE",
  "deploymentId": "nfcn0x",
  "lastUpdatedDate": 1511309280,
  "createdDate": 1511152939,
  "methodSettings": {
    ...
  }
}
```

As shown in the output, the canarySettings property is no longer present in the stage of a canary-disabled deployment.
You can use AWS Config to record configuration changes made to your API Gateway API resources and send notifications based on resource changes. Maintaining a configuration change history for API Gateway resources is useful for operational troubleshooting, audit, and compliance use cases.

AWS Config can track changes to:

- **API stage configuration**, such as:
  - cache cluster settings
  - throttle settings
  - access log settings
  - the active deployment set on the stage
- **API configuration**, such as:
  - endpoint configuration
  - version
  - protocol
  - tags

In addition, the AWS Config Rules feature enables you to define configuration rules and automatically detect, track, and alert violations to these rules. By tracking changes to these resource configuration properties, you can also author change-triggered AWS Config rules for your API Gateway resources, and test your resource configurations against best practices.

You can enable AWS Config in your account by using the AWS Config console or the AWS CLI. Select the resource types for which you want to track changes. If you previously configured AWS Config to record all resource types, then these API Gateway resources will be automatically recorded in your account.

Support for Amazon API Gateway in AWS Config is available in all AWS public regions and AWS GovCloud (US). For the full list of supported Regions, see Regions and Endpoints in the AWS General Reference.

**Topics**
- Supported Resource Types (p. 677)
- Setting up AWS Config (p. 678)
- Configuring AWS Config to Record API Gateway Resources (p. 678)
- Viewing API Gateway Configuration Details in the AWS Config Console (p. 678)
- Evaluating API Gateway Resources Using AWS Config Rules (p. 679)

**Supported Resource Types**

The following API Gateway resource types are integrated with AWS Config and are documented in AWS Config Supported AWS Resource Types and Resource Relationships:

- `AWS::ApiGatewayV2::Api` (WebSocket API)
- `AWS::ApiGateway::RestApi` (REST API)
• AWS::ApiGatewayV2::Stage (WebSocket API stage)
• AWS::ApiGateway::Stage (REST API stage)

For more information about AWS Config, see the AWS Config Developer Guide. For pricing information, see the AWS Config pricing information page.

Important
If you change any of the following API properties after the API is deployed, you must redeploy (p. 494) the API to propagate the changes. Otherwise, you'll see the attribute changes in the AWS Config console, but the previous property settings will still be in effect; the API's runtime behavior will be unchanged.

• AWS::ApiGateway::RestApi – binaryMediaTypes, minimumCompressionSize, apiKeySource
• AWS::ApiGatewayV2::Api – apiKeySelectionExpression

Setting up AWS Config

To initially set up AWS Config, see the following topics in the AWS Config Developer Guide.

• Setting Up AWS Config with the Console
• Setting Up AWS Config with the AWS CLI

Configuring AWS Config to Record API Gateway Resources

By default, AWS Config records configuration changes for all supported types of regional resources that it discovers in the region in which your environment is running. You can customize AWS Config to record changes only for specific resource types, or changes to global resources.

To learn about regional vs. global resources and learn how to customize your AWS Config configuration, see Selecting which Resources AWS Config Records.

Viewing API Gateway Configuration Details in the AWS Config Console

You can use the AWS Config console to look for API Gateway resources and get current and historical details about their configurations. The following procedure shows how to find information about an API Gateway API.

To find an API Gateway resource in the AWS Config console

1. Open the AWS Config console.
2. Choose Resources.
3. On the Resource inventory page, choose Resources.
4. Open the Resource type menu, scroll to APIGateway or APIGatewayV2, and then choose one or more of the API Gateway resource types.
5. Choose Look up.
6. Choose a resource ID in the list of resources that AWS Config displays. AWS Config displays configuration details and other information about the resource you selected.
7. To see the full details of the recorded configuration, choose View Details.

To learn more ways to find a resource and view information on this page, see Viewing AWS Resource Configurations and History in the AWS Config Developer Guide.

Evaluating API Gateway Resources Using AWS Config Rules

You can create AWS Config rules, which represent the ideal configuration settings for your API Gateway resources. You can use predefined AWS Config Managed Rules, or define custom rules. AWS Config continuously tracks changes to the configuration of your resources to determine whether those changes violate any of the conditions in your rules. The AWS Config console shows the compliance status of your rules and resources.

If a resource violates a rule and is flagged as noncompliant, AWS Config can alert you using an Amazon Simple Notification Service Developer Guide (Amazon SNS) topic. To programmatically consume the data in these AWS Config alerts, use an Amazon Simple Queue Service (Amazon SQS) queue as the notification endpoint for the Amazon SNS topic.

To learn more about setting up and using rules, see Evaluating Resources with Rules in the AWS Config Developer Guide.
Tagging Your API Gateway Resources

A *tag* is a metadata label that you assign or that AWS assigns to an AWS resource. Each tag has two parts:

- A *tag key* (for example, `CostCenter`, `Environment`, or `Project`). Tag keys are case sensitive.
- An optional field known as a *tag value* (for example, `111122223333` or `Production`). Omitting the tag value is the same as using an empty string. Like tag keys, tag values are case-sensitive.

Tags help you do the following:

- Control access to your resources based on the tags that are assigned to them. You control access by specifying tag keys and values in the conditions for an AWS Identity and Access Management (IAM) policy. For more information about tag-based access control, see Controlling Access Using Tags in the IAM User Guide.
- Track your AWS costs. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Use Cost Allocation Tags in the AWS Billing and Cost Management User Guide.
- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related. For example, you could assign the same tag to an API Gateway stage that you assign to a CloudWatch Events rule.

For tips on using tags, see the AWS Tagging Strategies post on the AWS Answers blog.

The following sections provide more information about tags for Amazon API Gateway.

**Topics**

- API Gateway Resources That Can Be Tagged (p. 680)
- Using Tags to Control Access to API Gateway Resources (p. 682)

**API Gateway Resources That Can Be Tagged**

Tags can be set on the following WebSocket API resources in the Amazon API Gateway V2 API:

- Api
- DomainName
- Stage

In addition, tags can be set on the following REST API resources in the Amazon API Gateway V1 API:

- ApiKey
- ClientCertificate
- DomainName
- RestApi
- Stage
Tag Inheritance in the Amazon API Gateway V1 API

Previously it was only possible to set tags on stages. Now that you can also set them on other resources, a Stage can receive a tag two ways:

• The tag can be set directly on the Stage.
• The stage can inherit the tag from its parent RestApi.

If a stage receives a tag both ways, the tag that was set directly on the stage takes precedence. For example, suppose a stage inherits the following tags from its parent REST API:

```json
{
  'foo': 'bar',
  'x':'y'
}
```

Suppose it also has the following tags set on it directly:

```json
{
  'foo': 'bar2',
  'hello': 'world'
}
```

The net effect would be for the stage to have the following tags, with the following values:

```json
{
  'foo': 'bar2',
  'hello': 'world'
}
```
Tag Restrictions and Usage Conventions

The following restrictions and usage conventions apply to using tags with API Gateway resources:

- Each resource can have a maximum of 50 tags.
- For each resource, each tag key must be unique, and each tag key can have only one value.
- The maximum tag key length is 128 Unicode characters in UTF-8.
- The maximum tag value length is 256 Unicode characters in UTF-8.
- Allowed characters for keys and values are letters, numbers, spaces representable in UTF-8, and the following characters: -, ., @, =, +. Amazon EC2 resources allow any characters.
- Tag keys and values are case-sensitive. As a best practice, decide on a strategy for capitalizing tags, and consistently implement that strategy across all resource types. For example, decide whether to use Costcenter, costcenter, or CostCenter, and use the same convention for all tags. Avoid using similar tags with inconsistent case treatment.
- The `aws:` prefix is prohibited for tags; it's reserved for AWS use. You can't edit or delete tag keys or values with this prefix. Tags with this prefix do not count against your tags per resource limit.

Using Tags to Control Access to API Gateway Resources

Conditions in AWS Identity and Access Management policies are part of the syntax that you use to specify permissions to API Gateway resources. For details about specifying IAM policies, see the section called "Use IAM Permissions" (p. 362). In API Gateway, resources can have tags, and some actions can include tags. When you create an IAM policy, you can use tag condition keys to control:

- Which users can perform actions on an API Gateway resource, based on tags that the resource already has.
- What tags can be passed in an action's request.
- Whether specific tag keys can be used in a request.

Using tag-based access control can allow for finer control than API-level control as well as more dynamic control than resource-based access control. IAM policies can be created that allow or disallow an operation based on tags provided in the request (request tags) or tags on the resource that is being operated on (resource tags). In general, resource tags are for resources that already exist. Request tags are for when you're creating new resources.

For the complete syntax and semantics of tag condition keys, see Controlling Access Using Tags in the IAM User Guide.

The following examples demonstrate how to specify tag conditions in policies for API Gateway users.

Example 1: Limit actions based on resource tags

The following example policy grants users permission to perform GET actions on all resources. In addition, if a resource has a tag named `iamrole` with a value of `readWrite`, the policy grants users permission to perform all actions on the resource.
Example 2: Limit actions based on tags in the request

The following example policy specifies that:

- When the user creates a new stage, the request to create the stage must contain a tag named `stage`
- The value of the `stage` tag must be `beta`, `gamma`, or `prod`. Otherwise, the request to create the stage is denied.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["apigateway:*"],
            "Resource": ["*"]
        },
        {
            "Effect": "Deny",
            "Action": "apigateway:POST",
            "Resource": "arn:aws:apigateway:*::/restapis/*/stages",
            "Condition": {
                "Null": {
                    "aws:RequestTag/stage": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "apigateway:POST",
            "Resource": "arn:aws:apigateway:*::/restapis/*/stages",
            "Condition": {
                "ForAnyValue:StringNotEquals": [
                    "aws:RequestTag/stage": ["beta", "gamma", "prod"]
                ]
            }
        }
    ]
}
```
Example 3: Deny actions based on resource tags

The following example policy allows users to perform all actions on API Gateway resources by default. If a resource has a tag named `stage` with a value of `prod`, users are denied permission to perform modifications (PATCH, PUT, POST, DELETE) on the resource.

```json
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "apigateway:*",
        "Resource": "*"
      },
      {
        "Effect": "Deny",
        "Action": [
          "apigateway:PATCH",
          "apigateway:PUT",
          "apigateway:POST",
          "apigateway:DELETE"
        ],
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/stage": "prod"
          }
        }
      }
    ]
}
```

Example 4: Allow actions based on resource tags

This example policy allows users to perform all actions on all API Gateway resources by default. If a resource has a tag named `environment` whose value is `prod`, users are not allowed to perform any operations on the resource.

```json
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": "apigateway:*",
        "Resource": "*"
      },
      {
        "Effect": "Deny",
        "Action": [
          "apigateway:*
        ],
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/environment": "prod"
          }
        }
      }
    ]
}
```
"StringEquals": {
  "aws:ResourceTag/environment": "prod"
}
]
}
Amazon API Gateway provides APIs for creating and deploying your own HTTP and WebSocket APIs. In addition, API Gateway APIs are available in standard AWS SDKs.

If you are using a language for which an AWS SDK exists, you may prefer to use the SDK rather than using the API Gateway REST APIs directly. The SDKs make authentication simpler, integrate easily with your development environment, and provide easy access to API Gateway commands.

Here's where to find the AWS SDKs and API Gateway REST API reference documentation:

- [Tools for Amazon Web Services](#) (for developer tools, SDKs, and IDE toolkits)
- [Amazon API Gateway Version 1 API Reference](#) (for creating and deploying HTTP APIs)
- [Amazon API Gateway Version 2 API Reference](#) (for creating and deploying WebSocket APIs)
Amazon API Gateway Limits and Important Notes

**Topics**
- API Gateway Limits (p. 687)
- Amazon API Gateway Important Notes (p. 692)

**API Gateway Limits**

Unless noted otherwise, the limits can be increased upon request. To request a limit increase, contact the AWS Support Center.

When authorization is enabled on a method, the maximum length of the method's ARN (e.g., `arn:aws:execute-api:{region-id}:{account-id}:{api-id}/{stage-id}/{method}/ {resource}/{path}`) is 1600 bytes. The path parameter values, the size of which are determined at run time, can cause the ARN length to exceed the limit. When this happens, the API client will receive a 414 Request URI too long response.

**Note**
This limits URI length when resource policies are used. In the case of private APIs where a resource policy is required, this limits the URI length of all private APIs.

**API Gateway Account-Level Limits**

The following limits apply at the account level in Amazon API Gateway.

<table>
<thead>
<tr>
<th>Resource or Operation</th>
<th>Default Limit</th>
<th>Can Be Increased</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throttle limit per region across REST APIs, WebSocket APIs, and WebSocket callback APIs</td>
<td>10,000 requests per second (RPS) with an additional burst capacity provided by the token bucket algorithm, using a maximum bucket capacity of 5,000 requests.</td>
<td>Yes</td>
</tr>
<tr>
<td>Regional APIs</td>
<td>600</td>
<td>No</td>
</tr>
<tr>
<td>Edge-Optimized APIs</td>
<td>120</td>
<td>No</td>
</tr>
</tbody>
</table>

**API Gateway Limits for Configuring and Running a WebSocket API**

The following limits apply to configuring and running a WebSocket API in Amazon API Gateway.
### API Gateway Limits for Configuring and Running a REST API

The following limits apply to configuring and running a REST API in Amazon API Gateway.

<table>
<thead>
<tr>
<th>Resource or Operation</th>
<th>Default Limit</th>
<th>Can Be Increased</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom domain names per account per region</td>
<td>120</td>
<td>Yes</td>
</tr>
<tr>
<td>Length, in characters, of the URL for an edge-optimized API</td>
<td>8192</td>
<td>No</td>
</tr>
</tbody>
</table>

### API Gateway Limits for Configuring and Running a REST API

The following limits apply to configuring and running a REST API in Amazon API Gateway.

<table>
<thead>
<tr>
<th>Resource or Operation</th>
<th>Default Limit</th>
<th>Can Be Increased</th>
</tr>
</thead>
<tbody>
<tr>
<td>New connections per second per account (across all WebSocket APIs) per region</td>
<td>500</td>
<td>No</td>
</tr>
<tr>
<td>AWS Lambda authorizers per API</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>AWS Lambda authorizer result size</td>
<td>8 KB</td>
<td>No</td>
</tr>
<tr>
<td>Routes per API</td>
<td>300</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrations per API</td>
<td>300</td>
<td>Yes</td>
</tr>
<tr>
<td>Stages per API</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>WebSocket frame size</td>
<td>32 KB</td>
<td>No</td>
</tr>
<tr>
<td>Message payload size</td>
<td>128 KB</td>
<td>No</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Because of the WebSocket frame-size limit of 32 KB, a message larger than 32 KB must be split into multiple frames, each 32 KB or smaller. If a larger message (or larger frame size) is received, the connection is closed with code 1009.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connection duration for WebSocket API</td>
<td>2 hours</td>
<td>No</td>
</tr>
<tr>
<td>Idle Connection Timeout</td>
<td>10 minutes</td>
<td>No</td>
</tr>
<tr>
<td>Resource or Operation</td>
<td>Default Limit</td>
<td>Can Be Increased</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Length, in characters, of the URL for a regional API</td>
<td>10240</td>
<td>No</td>
</tr>
<tr>
<td>Private APIs per account per region</td>
<td>600</td>
<td>No</td>
</tr>
<tr>
<td>Length, in characters, of API Gateway resource policy</td>
<td>8192</td>
<td>Yes</td>
</tr>
<tr>
<td>API keys per account per region</td>
<td>500</td>
<td>Yes</td>
</tr>
<tr>
<td>Client certificates per account per region</td>
<td>60</td>
<td>Yes</td>
</tr>
<tr>
<td>Authorizers per API (AWS Lambda and Amazon Cognito)</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Documentation parts per API</td>
<td>2000</td>
<td>Yes</td>
</tr>
<tr>
<td>Resources per API</td>
<td>300</td>
<td>Yes</td>
</tr>
<tr>
<td>Stages per API</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Stage variables per stage</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>Length, in characters, of the key in a stage variable</td>
<td>64</td>
<td>Yes</td>
</tr>
<tr>
<td>Length, in characters, of the value in a stage variable</td>
<td>512</td>
<td>Yes</td>
</tr>
<tr>
<td>Usage plans per account per region</td>
<td>300</td>
<td>Yes</td>
</tr>
<tr>
<td>Usage plans per API key</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Per-method throttling limit settings per API stage</td>
<td>20</td>
<td>Yes</td>
</tr>
<tr>
<td>VPC links per account per region</td>
<td>20</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource or Operation</td>
<td>Default Limit</td>
<td>Can Be Increased</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>API caching TTL</td>
<td>300 seconds by default and configurable between 0 and 3600 by an API owner.</td>
<td>Not for the upper bound (3600)</td>
</tr>
<tr>
<td>Cached response size</td>
<td>1048576 Bytes. Cache data encryption may increase the size of the item that is being cached.</td>
<td>No</td>
</tr>
<tr>
<td>Integration timeout</td>
<td>50 milliseconds - 29 seconds for all integration types, including Lambda, Lambda proxy, HTTP, HTTP proxy, and AWS integrations.</td>
<td>Not for the lower or upper bounds.</td>
</tr>
<tr>
<td>Total combined size of all header values</td>
<td>10240 Bytes</td>
<td>No</td>
</tr>
<tr>
<td>Payload size</td>
<td>10 MB</td>
<td>No</td>
</tr>
<tr>
<td>Tags per stage</td>
<td>50</td>
<td>No</td>
</tr>
<tr>
<td>Number of iterations in a <code>#foreach ... #end</code> loop in mapping templates</td>
<td>1000</td>
<td>No</td>
</tr>
<tr>
<td>ARN length of a method with authorization</td>
<td>1600 bytes</td>
<td>No</td>
</tr>
</tbody>
</table>

For `restapi:import` or `restapi:put`, the maximum size of the API definition file is 2 MB.

All of the per-API limits can only be increased on specific APIs.

**API Gateway Limits for Creating, Deploying and Managing an API**

The following fixed limits apply to creating, deploying, and managing an API in API Gateway, using the AWS CLI, the API Gateway console, or the API Gateway REST API and its SDKs. These limits cannot be increased.

<table>
<thead>
<tr>
<th>Action</th>
<th>Default Limit</th>
<th>Can Be Increased</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateApiKey</td>
<td>5 requests per second per account</td>
<td>No</td>
</tr>
<tr>
<td>CreateDeployment</td>
<td>1 request every 5 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>CreateDocumentationVersion</td>
<td>1 request every 20 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>Action</td>
<td>Default Limit</td>
<td>Can Be Increased</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>CreateDomainName</td>
<td>1 request every 30 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>CreateResource</td>
<td>5 requests per second per account</td>
<td>No</td>
</tr>
<tr>
<td>CreateRestApi</td>
<td><strong>Regional or Private API</strong></td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 request every 3 seconds per account</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Edge-Optimized API</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 request every 30 seconds per account</td>
<td></td>
</tr>
<tr>
<td>DeleteApiKey</td>
<td>5 requests per second per account</td>
<td>No</td>
</tr>
<tr>
<td>DeleteDomainName</td>
<td>1 request every 30 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>DeleteResource</td>
<td>5 requests per second per account</td>
<td>No</td>
</tr>
<tr>
<td>DeleteRestApi</td>
<td>1 request every 30 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>GetResources</td>
<td>5 requests every 2 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>ImportDocumentationParts</td>
<td>1 request every 30 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>ImportRestApi</td>
<td><strong>Regional or Private API</strong></td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• 1 request every 3 seconds per account</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Edge-Optimized API</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 1 request every 30 seconds per account</td>
<td></td>
</tr>
<tr>
<td>PutRestApi</td>
<td>1 request per second per account</td>
<td>No</td>
</tr>
<tr>
<td>UpdateAccount</td>
<td>1 request every 20 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>UpdateDomainName</td>
<td>1 request every 30 seconds per account</td>
<td>No</td>
</tr>
<tr>
<td>UpdateUsagePlan</td>
<td>1 request every 20 seconds per account</td>
<td>No</td>
</tr>
</tbody>
</table>
### Amazon API Gateway Important Notes

#### Topics
- Amazon API Gateway Important Notes for REST and WebSocket APIs (p. 692)
- Amazon API Gateway Important Notes for WebSocket APIs (p. 692)
- Amazon API Gateway Important Notes for REST APIs (p. 692)

#### Amazon API Gateway Important Notes for REST and WebSocket APIs

- API Gateway does not support wildcard subdomain names (of the `*.domain` form). However, it does support wildcard certificates (certificates for wildcard subdomain names).
- API Gateway does not support sharing a custom domain name across REST and WebSocket APIs.
- Stage names can only contain alphanumeric characters, hyphens, and underscores. Maximum length is 128 characters.
- The `/ping` and `/sping` paths are reserved for the service health check. Use of these for API root-level resources with custom domains will fail to produce the expected result.
- API Gateway currently limits log events to 1024 bytes. Log events larger than 1024 bytes, such as request and response bodies, will be truncated by API Gateway before submission to CloudWatch Logs.
- CloudWatch Metrics currently limits dimension names and values to 255 valid XML characters. (For more information, see the CloudWatch User Guide.) Dimension values are a function of user-defined names, including API name, label (stage) name, and resource name. When choosing these names, be careful not to exceed CloudWatch Metrics limits.
- The maximum size of a mapping template is 300 KB.

#### Amazon API Gateway Important Notes for WebSocket APIs

- API Gateway supports message payloads up to 128 KB with a maximum frame size of 32 KB. If a message exceeds 32 KB, you must split it into multiple frames, each 32 KB or smaller. If a larger message is received, the connection is closed with code 1009.

#### Amazon API Gateway Important Notes for REST APIs

- The plain text pipe character (|) is not supported for any request URL query string and must be URL-encoded.

---

<table>
<thead>
<tr>
<th>Action</th>
<th>Default Limit</th>
<th>Can Be Increased</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other operations</td>
<td>No limit up to the total account limit.</td>
<td>No</td>
</tr>
<tr>
<td>Total operations</td>
<td>10 requests per second with a burst limit of 40 requests per second.</td>
<td>No</td>
</tr>
</tbody>
</table>
• The semicolon character (;) is not supported for any request URL query string and results in the data being split.

• When using the API Gateway console to test an API, you may get an "unknown endpoint errors" response if a self-signed certificate is presented to the backend, the intermediate certificate is missing from the certificate chain, or any other recognizable certificate-related exceptions thrown by the backend.

• For an API Resource or Method entity with a private integration, you should delete it after removing any hard-coded reference of a VpcLink. Otherwise, you have a dangling integration and receive an error stating that the VPC link is still in use even when the Resource or Method entity is deleted. This behavior does not apply when the private integration references VpcLink through a stage variable.

• The following backends may not support SSL client authentication in a way that's compatible with API Gateway:
  • NGINX
  • Heroku

API Gateway supports most of the OpenAPI 2.0 specification and the OpenAPI 3.0 specification, with the following exceptions:

• Path segments can only contain alphanumeric characters, hyphens, periods, commas, and curly braces. Path parameters must be separate path segments. For example, "resource/{path_parameter_name}" is valid; "resource(path_parameter_name)" is not.

• Model names can only contain alphanumeric characters.

• For input parameters, only the following attributes are supported: name, in, required, type, description. Other attributes are ignored.

• The securitySchemes type, if used, must be apiKey. However, OAuth 2 and HTTP Basic authentication are supported via Lambda authorizers (p. 380); the OpenAPI configuration is achieved via vendor extensions (p. 578).

• The deprecated field is not supported and is dropped in exported APIs.

• API Gateway models are defined using JSON schema draft 4, instead of the JSON schema used by OpenAPI.

• The additionalProperties and anyOf fields are not supported in Models.

• The discriminator parameter is not supported in any schema object.

• The example tag is not supported.

• exclusiveMinimum is not supported by API Gateway.

• The maxItems and minItems tags are not included in simple request validation. To work around this, update the model after import before doing validation.

• oneOf is not supported by API Gateway.

• The readOnly field is not supported.

• Response definitions of the "500": {"$ref": "/responses/UnexpectedError"} form is not supported in the OpenAPI document root. To work around this, replace the reference by the inline schema.

• Numbers of the Int32 or Int64 type are not supported. An example is shown as follows:

```
"elementId": {
    "description": "Working Element Id",
    "format": "int32",
    "type": "number"
}
```

• Decimal number format type ("format": "decimal") is not supported in a schema definition.

• In method responses, schema definition must be of an object type and cannot be of primitive types. For example, "schema": { "type": "string"} is not supported. However, you can work around this using the following object type:
• API Gateway doesn’t use root level security defined in the OpenAPI specification. Hence security
needs to be defined at an operation level to be appropriately applied.

• API Gateway enacts the following restrictions and limitations when handling methods with either
Lambda integration or HTTP integration.

• Header names and query parameters are processed in a case-sensitive way.

• The following table lists the headers that may be dropped, remapped, or otherwise modified when
sent to your integration endpoint or sent back by your integration endpoint. In this table:

  • Remapped means that the header name is changed from `<string>` to `X-Amzn-Remapped-<string>`.

  • Remapped Overwritten means that the header name is changed from `<string>` to `X-Amzn-Remapped-<string>` and the value is overwritten.

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Request (http/http_proxy/lambda)</th>
<th>Response (http/http_proxy/lambda)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Accept</td>
<td>Passthrough</td>
<td>Dropped/Passthrough/Passthrough</td>
</tr>
<tr>
<td>Accept-Charset</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Accept-Encoding</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Authorization</td>
<td>Passthrough</td>
<td>Remapped</td>
</tr>
<tr>
<td>Connection</td>
<td>Passthrough/Passthrough/Dropped</td>
<td>Remapped</td>
</tr>
<tr>
<td>Content-Encoding</td>
<td>Passthrough/Dropped/Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Content-Length</td>
<td>Passthrough (generated based on body)</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Content-MD5</td>
<td>Dropped</td>
<td>Remapped</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Date</td>
<td>Passthrough</td>
<td>Remapped Overwritten</td>
</tr>
<tr>
<td>Expect</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>Host</td>
<td>5XX/5XX/Overwritten by Lambda</td>
<td>Dropped</td>
</tr>
</tbody>
</table>
### Important Notes for REST APIs

<table>
<thead>
<tr>
<th>Header Name</th>
<th>Request (http/http_proxy/lambda)</th>
<th>Response (http/http_proxy/lambda)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max-Forwards</td>
<td>Dropped</td>
<td>Remapped</td>
</tr>
<tr>
<td>Pragma</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Proxy-Authorize</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>Range</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Referer</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>Server</td>
<td>Dropped</td>
<td>Remapped Overwritten</td>
</tr>
<tr>
<td>TE</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>Transfer-Encoding</td>
<td>Dropped/Dropped/Exception</td>
<td>Dropped</td>
</tr>
<tr>
<td>Trailer</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>Upgrade</td>
<td>Dropped</td>
<td>Dropped</td>
</tr>
<tr>
<td>User-Agent</td>
<td>Passthrough</td>
<td>Remapped</td>
</tr>
<tr>
<td>Via</td>
<td>Dropped/Dropped/Passthrough</td>
<td>Passthrough/Passthrough/Dropped</td>
</tr>
<tr>
<td>Warn</td>
<td>Passthrough</td>
<td>Passthrough</td>
</tr>
<tr>
<td>WWW-Authorize</td>
<td>Dropped</td>
<td>Remapped</td>
</tr>
</tbody>
</table>

- The Android SDK of an API generated by API Gateway uses the java.net.HttpURLConnection class. This class will throw an unhandled exception, on devices running Android 4.4 and earlier, for a 401 response resulted from remapping of the WWW-Authorize header to X-Amzn-Remapped-WWW-Authorize.
- Unlike API Gateway-generated Java, Android and iOS SDKs of an API, the JavaScript SDK of an API generated by API Gateway does not support retries for 500-level errors.
- The test invocation of a method uses the default content type of application/json and ignores specifications of any other content types.
- When sending requests to an API by passing the X-HTTP-Method-Override header, API Gateway overrides the method. So in order to pass the header to the backend, the header needs to be added to the integration request.
- When a request contains multiple media types in its Accept header, API Gateway only honors the first Accept media type. In the situation where you cannot control the order of the Accept media types and the media type of your binary content is not the first in the list, you can add the first Accept media type in the binaryMediaTypes list of your API, API Gateway will return your content as binary. For example, to send a JPEG file using an <img> element in a browser, the browser might send Accept:image/webp, image/*,*/*;q=0.8 in a request. By adding image/webp to the binaryMediaTypes list, the endpoint will receive the JPEG file as binary.

---

695
Document History

The following table describes the important changes to the documentation since the last release of Amazon API Gateway. For notification about updates to this documentation, you can subscribe to an RSS feed by choosing the RSS button in the top menu panel.

- **Latest documentation update:** June 27, 2019

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag-Based Access Control for WebSocket APIs (p. 696)</td>
<td>Added support for tag-based access control for WebSocket APIs. For more information, see API Gateway Resources That Can Be Tagged.</td>
<td>June 27, 2019</td>
</tr>
<tr>
<td>TLS version selection for custom domains (p. 696)</td>
<td>Added support for Transport Layer Security (TLS) version selection for APIs that are deployed to custom domains. See the note in Choose a Minimum TLS Version for a Custom Domain in API Gateway.</td>
<td>June 20, 2019</td>
</tr>
<tr>
<td>VPC endpoint policies for private APIs (p. 696)</td>
<td>Added support for improving the security of private APIs by attaching endpoint policies to interface VPC endpoints. For more information, see Use VPC Endpoint Policies for Private APIs in API Gateway.</td>
<td>June 4, 2019</td>
</tr>
<tr>
<td>Documentation updated (p. 696)</td>
<td>Rewrote Getting Started with Amazon API Gateway. Moved tutorials to Amazon API Gateway Tutorials.</td>
<td>May 29, 2019</td>
</tr>
<tr>
<td>Tag-Based Access Control for REST APIs (p. 696)</td>
<td>Added support for tag-based access control for REST APIs. For more information, see Using Tags with IAM Policies to Control Access to API Gateway Resources.</td>
<td>May 23, 2019</td>
</tr>
<tr>
<td>Documentation updated (p. 696)</td>
<td>Rewrote 6 topics: What Is Amazon API Gateway?, TUTORIAL: Build an API with HTTP Proxy Integration, TUTORIAL: Create a Calc REST API with Three Non-Proxy Integrations, API Gateway Mapping Template and Access Logging Variable Reference, Use API Gateway Lambda Authorizers, and Enable CORS</td>
<td>April 5, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Serverless developer portal improvements (p. 696)</td>
<td>Added administrator panel and other improvements to make it easier to publish APIs in the Amazon API Gateway developer portal. For more information, see Use a Developer Portal to Catalog Your APIs.</td>
<td>March 28, 2019</td>
</tr>
<tr>
<td>Support for AWS Config (p. 696)</td>
<td>Added support for AWS Config. For more information, see Monitoring API Gateway API Configuration with AWS Config.</td>
<td>March 20, 2019</td>
</tr>
<tr>
<td>Support for AWS CloudFormation (p. 696)</td>
<td>Added API Gateway V2 API to the AWS CloudFormation template reference. For more information, see Amazon API Gateway V2 Resource Types Reference.</td>
<td>February 7, 2019</td>
</tr>
<tr>
<td>Support for WebSocket APIs (p. 696)</td>
<td>Added support for WebSocket APIs. For more information, see Creating a WebSocket API in Amazon API Gateway.</td>
<td>December 18, 2018</td>
</tr>
<tr>
<td>Serverless developer portal available through AWS Serverless Application Repository (p. 696)</td>
<td>The Amazon API Gateway developer portal serverless application is now available from the AWS Serverless Application Repository (in addition to GitHub). For more information, see Use a Developer Portal to Catalog Your API Gateway APIs.</td>
<td>November 16, 2018</td>
</tr>
<tr>
<td>Support for AWS WAF (p. 696)</td>
<td>Added support for AWS WAF (Web Application Firewall). For more information, see Control Access to an API Using AWS WAF.</td>
<td>November 5, 2018</td>
</tr>
<tr>
<td>Serverless developer portal (p. 696)</td>
<td>Amazon API Gateway now provides a fully customizable developer portal as a serverless application that you can deploy for publishing your API Gateway APIs. For more information, see Use a Developer Portal to Catalog Your API Gateway APIs.</td>
<td>October 29, 2018</td>
</tr>
<tr>
<td>Support for multi-value headers and query string parameters (p. 696)</td>
<td>Amazon API Gateway now supports multiple headers and query string parameters that have the same name. For more information, see Support for Multi-Value Headers and Query String Parameters.</td>
<td>October 4, 2018</td>
</tr>
<tr>
<td>Change Description</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>OpenAPI support (p. 696)</td>
<td>Amazon API Gateway now supports OpenAPI 3.0 as well as OpenAPI (Swagger) 2.0.</td>
<td>September 27, 2018</td>
</tr>
<tr>
<td>Documentation updated (p. 696)</td>
<td>Added a new topic: How Amazon API Gateway Resource Policies Affect Authorization Workflow.</td>
<td>September 27, 2018</td>
</tr>
<tr>
<td>Active AWS X-Ray integration (p. 696)</td>
<td>You can now use AWS X-Ray to trace and analyze latencies in user requests as they travel through your APIs to the underlying services. For more information, see Trace API Gateway API Execution with AWS X-Ray.</td>
<td>September 6, 2018</td>
</tr>
<tr>
<td>Caching improvements (p. 696)</td>
<td>Only GET methods will have caching enabled by default when you enable caching for an API stage. This helps to ensure the safety of your API. You can enable caching for other methods by overriding method settings. For more information, see Enable API Caching to Enhance Responsiveness.</td>
<td>August 20, 2018</td>
</tr>
<tr>
<td>Service limits revised (p. 696)</td>
<td>Several limits have been revised: Increased number of APIs per account. Increased API rate limits for Create/Import/Deploy APIs. Corrected some rates from per minute to per second. For more information, see Limits.</td>
<td>July 13, 2018</td>
</tr>
<tr>
<td>Overriding API request and response parameters and headers (p. 696)</td>
<td>Added support for overriding request headers, query strings, and paths, as well as response headers and status codes. For more information, see Use a Mapping Template to Override an API's Request and Response Parameters and Headers.</td>
<td>July 12, 2018</td>
</tr>
<tr>
<td>Method-level throttling for usage plans (p. 696)</td>
<td>Added support for setting default per-method throttling limits, as well as setting throttling limits for individual API methods in usage plan settings. These settings are in addition to the existing account-level throttling and default method-level throttling limits that you can set in stage settings. For more information, see Throttle API Requests for Better Throughput.</td>
<td>July 11, 2018</td>
</tr>
</tbody>
</table>
Earlier Updates

The following table describes important changes in each release of the API Gateway Developer Guide before June 27, 2018.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private APIs</td>
<td>Added support for private APIs (p. 194), which you expose via interface VPC endpoints. Traffic to your private APIs does not leave the Amazon network; it is isolated from the public internet.</td>
<td>June 14, 2018</td>
</tr>
<tr>
<td>Cross-Account Lambda Authorizers and Integrations and Cross-Account Amazon Cognito User Pool Authorizers</td>
<td>Use an AWS Lambda function from a different AWS account as a Lambda authorizer function or as an API integration backend. Or use an Amazon Cognito user pool as an authorizer. The other account can be in any region where Amazon API Gateway is available. For more information, see the section called “Configure a Cross-Account Lambda Authorizer” (p. 395), the section called “TUTORIAL: Build an API with Cross-Account Lambda Proxy Integration” (p. 31), and the section called “Configure Cross-Account Amazon Cognito Authorizer for a REST API” (p. 404).</td>
<td>April 2, 2018</td>
</tr>
<tr>
<td>Resource Policies for APIs</td>
<td>Use API Gateway resource policies to enable users from a different AWS account to securely access your API or to allow the API to be invoked only from specified source IP address ranges or CIDR blocks. For more information, see the section called “Use API Gateway Resource Policies” (p. 347).</td>
<td>April 2, 2018</td>
</tr>
<tr>
<td>Tagging for API Gateway resources</td>
<td>Tag an API stage with up to 50 tags for cost allocation of API requests and caching in API Gateway. For more information see the section called “Set Up Tags” (p. 508).</td>
<td>December 19, 2017</td>
</tr>
<tr>
<td>Payload compression and decompression</td>
<td>Enable calling your API with compressed payloads using one of the supported content codings. The compressed payloads are subject to mapping if a body-mapping template is specified. For more information, see the section called “Enable Payload Compression” (p. 325).</td>
<td>December 19, 2017</td>
</tr>
<tr>
<td>API key sourced from a custom authorizer</td>
<td>Return an API key from a custom authorizer to API Gateway to apply a usage plan for API methods that require the key.</td>
<td>December 19, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Authorization with OAuth 2 scopes</td>
<td>Enable authorization of method invocation by using OAuth 2 scopes with the COGNITO_USER_POOLS authorizer. For more information, see the section called “Use Cognito User Pool as Authorizer for a REST API” (p. 397).</td>
<td>December 14, 2017</td>
</tr>
<tr>
<td>Private Integration and VPC Link</td>
<td>Create an API with the API Gateway private integration to provide clients with access to HTTP/HTTPS resources in an Amazon VPC from outside of the VPC through a VpcLink resource. For more information, see the section called “TUTORIAL: Build an API with Private Integration” (p. 85) and the section called “Set up Private Integrations” (p. 244).</td>
<td>November 30, 2017</td>
</tr>
<tr>
<td>Deploy a Canary for API testing</td>
<td>Add a canary release to an existing API deployment to test a newer version of the API while keeping the current version in operation on the same stage. You can set a percentage of stage traffic for the canary release and enable canary-specific execution and access logged in separate CloudWatch Logs logs. For more information, see the section called “Set up a Canary Release Deployment” (p. 666).</td>
<td>November 28, 2017</td>
</tr>
<tr>
<td>Access Logging</td>
<td>Log client access to your API with data derived from $context variables (p. 293) in a format of your choosing. For more information, see the section called “Set Up CloudWatch API Logging” (p. 510).</td>
<td>November 21, 2017</td>
</tr>
<tr>
<td>Ruby SDK of an API</td>
<td>Generate a Ruby SDK for your API and use it to invoke your API methods. For more information, see the section called “Generate the Ruby SDK of an API” (p. 523) and the section called “Use a Ruby SDK Generated by API Gateway for a REST API” (p. 545).</td>
<td>November 20, 2017</td>
</tr>
<tr>
<td>Regional API endpoint</td>
<td>Specify a regional API endpoint to create an API for non-mobile clients. A non-mobile client, such as an EC2 instance, runs in the same AWS Region where the API is deployed. As with an edge-optimized API, you can create a custom domain name for a regional API. For more information, see the section called “Set up a Regional API” (p. 192) and the section called “Set Up a Regional Custom Domain Name for REST or WebSocket API” (p. 655).</td>
<td>November 2, 2017</td>
</tr>
<tr>
<td>Custom request authorizer</td>
<td>Use custom request authorizer to supply user-authenticating information in request parameters to authorize API method calls. The request parameters include headers and query string parameters as well as stage and context variables. For more information, see Use API Gateway Lambda Authorizers (p. 380).</td>
<td>September 15, 2017</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Customizing gateway responses</td>
<td>Customize API Gateway-generated gateway responses to API requests that failed to reach the integration backend. A customized gateway message can provide the caller with API-specific custom error messages, including returning needed CORS headers, or can transform the gateway response data to a format of an external exchange. For more information, see Set up Gateway Responses to Customize Error Responses (p. 252).</td>
<td>June 6, 2017</td>
</tr>
<tr>
<td>Mapping Lambda custom error properties to method response headers</td>
<td>Map individual custom error properties returned from Lambda to the method response header parameters using the integration.response.body parameter, relying API Gateway to deserialize the stringified custom error object at run time. For more information, see Handle Custom Lambda Errors in API Gateway (p. 237).</td>
<td>June 6, 2017</td>
</tr>
<tr>
<td>Throttling limits increase</td>
<td>Increase the account-level steady-state request rate limit to 10,000 requests per second (rps) and the burst limit to 5000 concurrent requests. For more information, see Throttle API Requests for Better Throughput (p. 505).</td>
<td>June 6, 2017</td>
</tr>
<tr>
<td>Validating method requests</td>
<td>Configure basic request validators on the API level or method levels so that API Gateway can validate incoming requests. API Gateway verifies that required parameters are set and not blank, and verifies that the format of applicable payloads conforms to the configured model. For more information, see Enable Request Validation in API Gateway (p. 329).</td>
<td>April 11, 2017</td>
</tr>
<tr>
<td>Integrating with ACM</td>
<td>Use ACM Certificates for your API's custom domain names. You can create a certificate in AWS Certificate Manager or import an existing PEM-formatted certificate into ACM. You then refer to the certificate's ARN when setting a custom domain name for your APIs. For more information, see Set Up a Custom Domain Name for an API in API Gateway (p. 641).</td>
<td>March 9, 2017</td>
</tr>
<tr>
<td>Generating and calling a Java SDK of an API</td>
<td>Let API Gateway generate the Java SDK for your API and use the SDK to call the API in your Java client. For more information, see Use a Java SDK Generated by API Gateway for a REST API (p. 538).</td>
<td>January 13, 2017</td>
</tr>
<tr>
<td>Integrating with AWS Marketplace</td>
<td>Sell your API in a usage plan as a SaaS product through AWS Marketplace. Use AWS Marketplace to extend the reach of your API. Rely on AWS Marketplace for customer billing on your behalf. Let API Gateway handle user authorization and usage metering. For more information, see Sell Your APIs as SaaS (p. 638).</td>
<td>December 1, 2016</td>
</tr>
<tr>
<td>Enabling Documentation Support for your API</td>
<td>Add documentation for API entities in DocumentationPart resources in API Gateway. Associate a snapshot of the collection DocumentationPart instances with an API stage to create a DocumentationVersion. Publish API documentation by exporting a documentation version to an external file, such as a Swagger file. For more information, see Documenting a REST API in API Gateway (p. 446).</td>
<td>December 1, 2016</td>
</tr>
</tbody>
</table>
## Earlier Updates

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated custom authorizer</td>
<td>A customer authorizer Lambda function now returns the caller’s principal identifier. The function also can return other information as key-value pairs of the context map and an IAM policy. For more information, see Output from an Amazon API Gateway Lambda Authorizer (p. 391).</td>
<td>December 1, 2016</td>
</tr>
<tr>
<td>Supporting binary payloads</td>
<td>Set binaryMediaTypes on your API to support binary payloads of a request or response. Set the contentHandling property on an Integration or IntegrationResponse to specify whether to handle a binary payload as the native binary blob, as a Base64-encoded string, or as a passthrough without modifications. For more information, see Support Binary Payloads in API Gateway (p. 303).</td>
<td>November 17, 2016</td>
</tr>
<tr>
<td>Enabling a proxy integration with an HTTP or Lambda backend through a proxy resource of an API.</td>
<td>Create a proxy resource with a greedy path parameter of the form <code>{proxy+}</code> and the catch-all ANY method. The proxy resource is integrated with an HTTP or Lambda backend using the HTTP or Lambda proxy integration, respectively. For more information, see Set up a Proxy Integration with a Proxy Resource (p. 215).</td>
<td>September 20, 2016</td>
</tr>
<tr>
<td>Extending selected APIs in API Gateway as product offerings for your customers by providing one or more usage plans.</td>
<td>Create a usage plan in API Gateway to enable selected API clients to access specified API stages at agreed-upon request rates and quotas. For more information, see Create and Use Usage Plans with API Keys (p. 432).</td>
<td>August 11, 2016</td>
</tr>
<tr>
<td>Enabling method-level authorization with a user pool in Amazon Cognito</td>
<td>Create a user pool in Amazon Cognito and use it as your own identity provider. You can configure the user pool as a method-level authorizer to grant access for users who are registered with the user pool. For more information, see Control Access to a REST API Using Amazon Cognito User Pools as Authorizer (p. 397).</td>
<td>July 28, 2016</td>
</tr>
<tr>
<td>Enabling Amazon CloudWatch metrics and dimensions under the AWS/ApiGateway namespace.</td>
<td>The API Gateway metrics are now standardized under the CloudWatch namespace of AWS/ApiGateway. You can view them in both the API Gateway console and the Amazon CloudWatch console. For more information, see Amazon API Gateway Dimensions and Metrics (p. 570).</td>
<td>July 28, 2016</td>
</tr>
<tr>
<td>Enabling certificate rotation for a custom domain name</td>
<td>Certificate rotation allows you to upload and renew an expiring certificate for a custom domain name. For more information, see Rotate a Certificate Imported into ACM (p. 654).</td>
<td>April 27, 2016</td>
</tr>
<tr>
<td>Documenting changes for the updated Amazon API Gateway console.</td>
<td>Learn how to create and set up an API using the updated API Gateway console. For more information, see TUTORIAL: Create a REST API by Importing an Example (p. 42) and TUTORIAL: Build an API with HTTP Non-Proxy Integration (p. 56).</td>
<td>April 5, 2016</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Enabling the Import API feature to create a new or update an existing API from external API definitions.</td>
<td>With the Import API features, you can create a new API or update an existing one by uploading an external API definition expressed in Swagger 2.0 with the API Gateway extensions. For more information about the Import API, see Import a REST API into API Gateway (p. 341).</td>
<td>April 5, 2016</td>
</tr>
<tr>
<td>Exposing the $input.body variable to access the raw payload as string and the $util.parseJson() function to turn a JSON string into a JSON object in a mapping template.</td>
<td>For more information about $input.body and $util.parseJson(), see API Gateway Mapping Template and Access Logging Variable Reference (p. 293).</td>
<td>April 5, 2016</td>
</tr>
<tr>
<td>Enabling client requests with method-level cache invalidation, and improving request throttling management.</td>
<td>Flush API stage-level cache and invalidate individual cache entry. For more information, see Flush the API Stage Cache in API Gateway (p. 503) and Invalidate an API Gateway Cache Entry (p. 503). Improve the console experience for managing API request throttling. For more information, see Throttle API Requests for Better Throughput (p. 505).</td>
<td>March 25, 2016</td>
</tr>
<tr>
<td>Enabling and calling API Gateway API using custom authorization</td>
<td>Create and configure an AWS Lambda function to implement custom authorization. The function returns an IAM policy document that grants the Allow or Deny permissions to client requests of an API Gateway API. For more information, see Use API Gateway Lambda Authorizers (p. 380).</td>
<td>February 11, 2016</td>
</tr>
<tr>
<td>Importing and exporting API Gateway API using a Swagger definition file and extensions</td>
<td>Create and update your API Gateway API using the Swagger specification with the API Gateway extensions. Import the Swagger definitions using the API Gateway Importer. Export an API Gateway API to a Swagger definition file using the API Gateway console or API Gateway Export API. For more information, see Import a REST API into API Gateway (p. 341) and Export a REST API (p. 663).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>Mapping request or response body or body's JSON fields to request or response parameters.</td>
<td>Map method request body or its JSON fields into integration request's path, query string, or headers. Map integration response body or its JSON fields into request response's headers. For more information, see Amazon API Gateway API Request and Response Data Mapping Reference (p. 289).</td>
<td>December 18, 2015</td>
</tr>
<tr>
<td>Working with Stage Variables in Amazon API Gateway</td>
<td>Learn how to associate configuration attributes with a deployment stage of an API in Amazon API Gateway. For more information, see Set up Stage Variables for a REST API Deployment (p. 514).</td>
<td>November 5, 2015</td>
</tr>
<tr>
<td>How to: Enable CORS for a Method</td>
<td>It is now easier to enable cross-origin resource sharing (CORS) for methods in Amazon API Gateway. For more information, see Enable CORS for a REST API Resource (p. 405).</td>
<td>November 3, 2015</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Date Changed</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>How to: Use Client Side SSL</td>
<td>Authentication Use Amazon API Gateway to generate SSL certificates that you can use to authenticate calls to your HTTP backend. For more information, see Generate and Configure an SSL Certificate for Backend Authentication (p. 411).</td>
<td>September 22, 2015</td>
</tr>
<tr>
<td>Mock integration of methods</td>
<td>Learn how to mock-integrate an API with Amazon API Gateway (p. 250). This feature enables developers to generate API responses from API Gateway directly without the need for a final integration backend beforehand.</td>
<td>September 1, 2015</td>
</tr>
<tr>
<td>Amazon Cognito Identity support</td>
<td>Amazon API Gateway has expanded the scope of the $context variable so that it now returns information about Amazon Cognito Identity when requests are signed with Amazon Cognito credentials. In addition, we have added a $util variable for escaping characters in JavaScript and encoding URLs and strings. For more information, see API Gateway Mapping Template and Access Logging Variable Reference (p. 293).</td>
<td>August 28, 2015</td>
</tr>
<tr>
<td>Swagger integration</td>
<td>Use the Swagger import tool on GitHub to import Swagger API definitions into Amazon API Gateway. Learn more about API Gateway Extensions to OpenAPI (p. 575) to create and deploy APIs and methods using the import tool. With the Swagger importer tool you can also update existing APIs.</td>
<td>July 21, 2015</td>
</tr>
<tr>
<td>Initial public release</td>
<td>This is the initial public release of the API Gateway Developer Guide.</td>
<td>July 9, 2015</td>
</tr>
</tbody>
</table>
AWS Glossary

For the latest AWS terminology, see the AWS Glossary in the AWS General Reference.