Q: What is Amazon API Gateway?

Amazon API Gateway is a fully managed service that makes it easy for developers to publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as applications running on Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS) or AWS Elastic Beanstalk, code running on AWS Lambda, or any web application. Amazon API Gateway handles all of 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. Amazon API Gateway has no minimum fees or startup costs. You pay only for the API calls you receive and the amount of data transferred out.

Show less

Q: Why use Amazon API Gateway?

Amazon API Gateway provides developers with a simple, flexible, fully managed, pay-as-you-go service that handles all aspects of creating and operating robust APIs for application back ends. With Amazon API Gateway, you can launch new services faster and with reduced investment so you can focus on building your core business services. Amazon API Gateway was built to help you with several aspects of creating and managing APIs:

performance of your APIs and the latency your end users experience by caching the output of API calls to avoid calling your backend every time.

4) **Operations Monitoring**. After an API is published and in use, API Gateway provides you with a metrics dashboard to monitor calls to your services. The Amazon API Gateway dashboard, through integration with Amazon CloudWatch, provides you with backend performance metrics covering API calls, latency data and error rates. You can enable detailed metrics for each method in your APIs and also receive error, access or debug logs in CloudWatch Logs.

5) **Lifecycle Management**. After an API has been published, you often need to build and test new versions that enhance or add new functionality. Amazon API Gateway lets you operate multiple API versions and multiple stages for each version simultaneously so that existing applications can continue to call previous versions after new API versions are published.

6) **Designed for Developers**. Amazon API Gateway allows you to quickly create APIs and assign static content for their responses to reduce cross-team development effort and time-to-market for your applications. Teams who depend on your APIs can begin development while you build your backend processes.

Show less

Q: How do I get started with Amazon API Gateway?

7. Define how requests and responses are transformed using a mapping template, or accept the default settings to pass all of the request and response data through without applying any transformation.

8. Configure the method's security settings.

9. Deploy your new API to a stage.

10. From the Stage management page, set up caching and throttling.

11. On the Client Platforms tab in the Amazon API Gateway console, click the button to download the Android, iOS SDK, or JavaScript library that contains helper methods to call your sayHello operation. The SDK library makes calling your APIs similar to calling a local method. The client SDK automatically handles retries, informing the developer of network or other fault conditions. The SDK library includes the logic necessary to authenticate the client application to your APIs.

12. Integrate the downloaded SDK into your mobile application. Write the code to invoke your custom API. For example, to invoke the getCar(int carId) API in an iOS application:

–(void)getSampleCar

{

NSString *response = [MyServiceClient getCar:1323];

Show less

Q: What data types can I use with Amazon API Gateway ?

APIs built on Amazon API Gateway can accept any payloads sent over HTTP. Typical data formats include JSON, XML, query string parameters, and request headers. You can declare any content type for your API's responses, and then use the transform templates to change the back-end response into your desired format.

Show less

Q: With what backends can Amazon API Gateway communicate?

Amazon API Gateway can execute AWS Lambda functions in your account, start AWS Step Functions state machines, or call HTTP endpoints hosted on AWS Elastic Beanstalk, Amazon EC2, and also non-AWS hosted HTTP based operations that are accessible via the public Internet.API Gateway also allows you to specify a mapping template to generate static content to be returned, helping you mock your APIs before the backend is ready. You can also integrate API Gateway with other AWS services directly – for example, you could expose an API method in API Gateway that sends data directly to Amazon Kinesis.

Show less

Q: What can I manage through the Amazon API Gateway console?

Through the Amazon API Gateway console, you can define the REST API and its associated resources and methods, manage the API lifecycle, generate client SDKs and view API metrics. You can also use the API Gateway console to define your APIs' usage plans, manage developers' API keys, and configure throttling and quota limits. All of the same actions are available through the API Gateway APIs.

Show less

Q: What is a REST API?

In Amazon API Gateway, a REST API is a group of resources and methods, or endpoints. REST APIs can be deployed to different stages and cloned to new versions.

Show less

Q: What is a resource?

A resource is a typed object that is part of your API's domain. Each resource may have associated a data model, relationships to other resources, and can respond to different methods.You can also define resources as variables to intercept requests to multiple child resources.

Usage plans help you declare plans for third-party developers that restrict access only to certain APIs, define throttling and request quota limits, and associate them with API keys. You can also extract utilization data on an per-API key basis to analyze API usage and generate billing documents. For example, you can create a basic, professional, and enterprise plans – you can configure the basic usage plan to only allow 1,000 requests per day and a maximum of 5 requests per second (RPS).

Show less

Q: What is the Amazon API Gateway API lifecycle?

With Amazon API Gateway, each REST API can have multiple stages. Stages are meant to help with the development lifecycle of an API -- for example, after you've built your APIs and you deploy them to a development stage, or when you are ready for production, you can deploy them to a production stage.

Show less

Q: What is a stage?

In Amazon API Gateway, stages are similar to tags. They define the path through which the deployment is accessible. For example, you can define a development stage and deploy your cars API to it. The resource will be accessible at https://www.myapi.com/dev/cars. You can also set up custom domain names to point directly to a stage, so that you don't have to use the additional

Show less

Q: What is a Resource Policy?

A Resource Policy is a JSON policy document 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 a Resource Policy 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.

Show less

Q: What if I mistakenly deployed to a stage?

Amazon API Gateway saves the history of your deployments. At any point, using the Amazon API Gateway APIs or the console, you can roll back a stage to a previous deployment.

Show less

Q: Can I run multiple versions of the same REST API?

Yes. Amazon API Gateway gives you the ability to clone an existing API. When you are ready to start working on the next major version of your API, you will be able to keep working on your version 1

You can monetize your APIs on API Gateway by publishing them as products in AWS Marketplace. You will first need to register as a seller in AWS Marketplace, and submit your usage plans on API Gateway as products. Read here to learn more about API Monetization.

Show less

Q: How do I document my API on Amazon API Gateway?

API Gateway offers the ability to create, update, and delete documentation associated with each portion of your API, such as methods and resources. You can access documentation-related APIs through the AWS SDKs, CLI, via RESTful calls, or by editing the documentation strings directly in the API Gateway console. Documentation can also be imported as a Swagger file, either as part of the API or separately, allowing you to add or update the documentation without disturbing the API definition. API Gateway conforms to the Open API specification for documentation imported from, or exported to, Swagger files.

Show less

Q: How can I avoid creating redundant copies of error messages and other documentation that recurs frequently in my API?

In addition to offering standards-conformant API documentation support, API Gateway additionally supports documentation inheritance, making it simple to define a documentation string once and then use it in multiple places. Inheritance simplifies the process of defining API

Security and Authorization

Q: How do I authorize access to my APIs?

With Amazon API Gateway, you can optionally set your API methods to require authorization. When setting up a method to require authorization you can leverage AWS Signature Version 4 or Lambda authorizers to support your own bearer token auth strategy.

Show less

Q: How does AWS Signature Version 4 work?

You can use AWS credentials - access and secret keys - to sign requests to your service and authorize access like other AWS services. The signing of an Amazon API Gateway API request is managed by the custom API Gateway SDK generated for your service. You can retrieve temporary credentials associated with a role in your AWS account using Amazon Cognito.

Show less

Q: What is a Lambda authorizer?

stage. However, we do not recommend you use API keys for authorization. You should use API keys to monitor usage by third-party developers and leverage a stronger mechanism for authorization, such as signed API calls or OAuth.

Show less

Q: How can I address or prevent API threats or abuse?

Amazon API Gateway supports throttling settings for each method in your APIs. You can set a standard rate limit and a burst rate limit per second for each method in your REST APIs. Further, Amazon API Gateway automatically protects your backend systems from distributed denial-of-service (DDoS) attacks, whether attacked with counterfeit requests (Layer 7) or SYN floods (Layer 3).

Show less

Q: Can I verify that it is API Gateway calling my backend?

Yes. Amazon API Gateway can generate a client-side SSL certificate and make the public key of that certificate available to you. Calls to your backend can be made with the generated certificate, and you can verify calls originating from Amazon API Gateway using the public key of the certificate.

Show less

Endpoints.

Show less

Q: Can I restrict access to private APIs to a specific Amazon VPC or VPC endpoint?

Yes, you can apply a Resource Policy to an API to restrict access to a specific Amazon VPC or VPC endpoint. You can also give an Amazon VPC or VPC endpoint from a different account access to the Private API using a Resource Policy.

Show less

Q: Can I configure my APIs in Amazon API Gateway to use TLS 1.1 or higher ?

Yes, you can set up a CloudFront distribution with custom SSL certificate in your account and use it with Regional APIs in API Gateway. You can then configure the Security Policy for the CloudFront distribution with TLS 1.1 or higher based on your security and compliance requirements.

Show less

back to top >>

Yes, Amazon API Gateway sends logging information and metrics to Amazon CloudWatch. You can utilize the Amazon CloudWatch console to set up custom alarms.

Show less

Q: How can I set up metrics for Amazon API Gateway?

By default, Amazon API Gateway monitors traffic at a REST API level. Optionally, you can enable detailed metrics for each method in your REST API from the deployment configuration APIs or console screen. Detailed metrics are also logged to Amazon CloudWatch and will be charged at the CloudWatch rates.

Show less

Q: Can I determine which version of the API my customers are using?

Yes. Metric details are specified by REST API and stage. Additionally, you can enable metrics for each method in your REST API.

Show less

Q: Does Amazon API Gateway provide logging support?

Throttling and Caching

Q: How can I protect my backend systems and applications from traffic spikes?

Amazon API Gateway provides throttling at multiple levels including global and by service call. Throttling limits can be set for standard rates and bursts. For example, API owners can set a rate limit of 1,000 requests per second for a specific method in their REST APIs, and also configure Amazon API Gateway to handle a burst of 2,000 requests per second for a few seconds. Amazon API Gateway tracks the number of requests per second. Any requests over the limit will receive a 429 HTTP response. The client SDKs generated by Amazon API Gateway retry calls automatically when met with this response.

Show less

Q: Can I throttle individual developers calling my APIs?

Yes. With usage plans you can set throttling limits for individual API keys.

Show less

Q: How does throttling help me?

First. API Gateway checks against your AWS account limit. If the traffic is below the set account limit, API Gateway checks the limit you have set on a stage or method. If the traffic is below the stage limit, then API Gateway applies the usage plans limits you set on a per-API key basis.

Show less

Q: Does Amazon API Gateway provide API result caching?

Yes. You can add caching to API calls by provisioning an Amazon API Gateway cache and specifying its size in gigabytes. The cache is provisioned for a specific stage of your APIs. This improves performance and reduces the traffic sent to your back end. Cache settings allow you to control the way the cache key is built and the time-to-live (TTL) of the data stored for each method. Amazon API Gateway also exposes management APIs that help you invalidate the cache for each stage.

Show less

Q: What happens if a large number of end users try to invoke my API simultaneously?

If caching is not enabled and throttling limits have not been applied, then all requests will pass through to your backend service until the account level throttling limits are reached. If throttling limits are in place, then Amazon API Gateway will shed the necessary amount of requests and send only the defined limit to your back-end service. If a cache is configured, then Amazon API Gateway will return a cached response for duplicate requests for a customizable time, but only if under configured throttling limits. This balance between the backend and client ensures optimal

back to top >>

Billing

Q: How am I charged for using Amazon API Gateway?

Amazon API Gateway rates are $3.50 per million API calls, plus the cost of data transfer out, in gigabytes. If you choose to provision a cache for your API, hourly rates apply. Please see the API Gateway Pricing pages for details on data transfer and caching costs.

Show less

Q: Who pays for Amazon API Gateway API calls generated by third-party developers?

The API owner is charged for the calls to their APIs on API Gateway.

Show less

Ready to get started?

Sign up

Have more questions?

Contact us

DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Oil & Gas
Automotive
Blockchain
Manufacturing

Resources & Training

Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS