Tencent Cloud

API Gateway

Product Introduction

Product Documentation

Contents

Product Introduction
Overview

Last updated：2024-01-03 10:03:44

API Gateway implements full-lifecycle API management to help you easily manage APIs in different stages such as creation, maintenance, release, and monitoring. With the aid of API Gateway, you can encapsulate various backend businesses into APIs for service provision to users. In addition, API Gateway makes it easy for you to manage API documentation, test APIs, and generate SDKs.
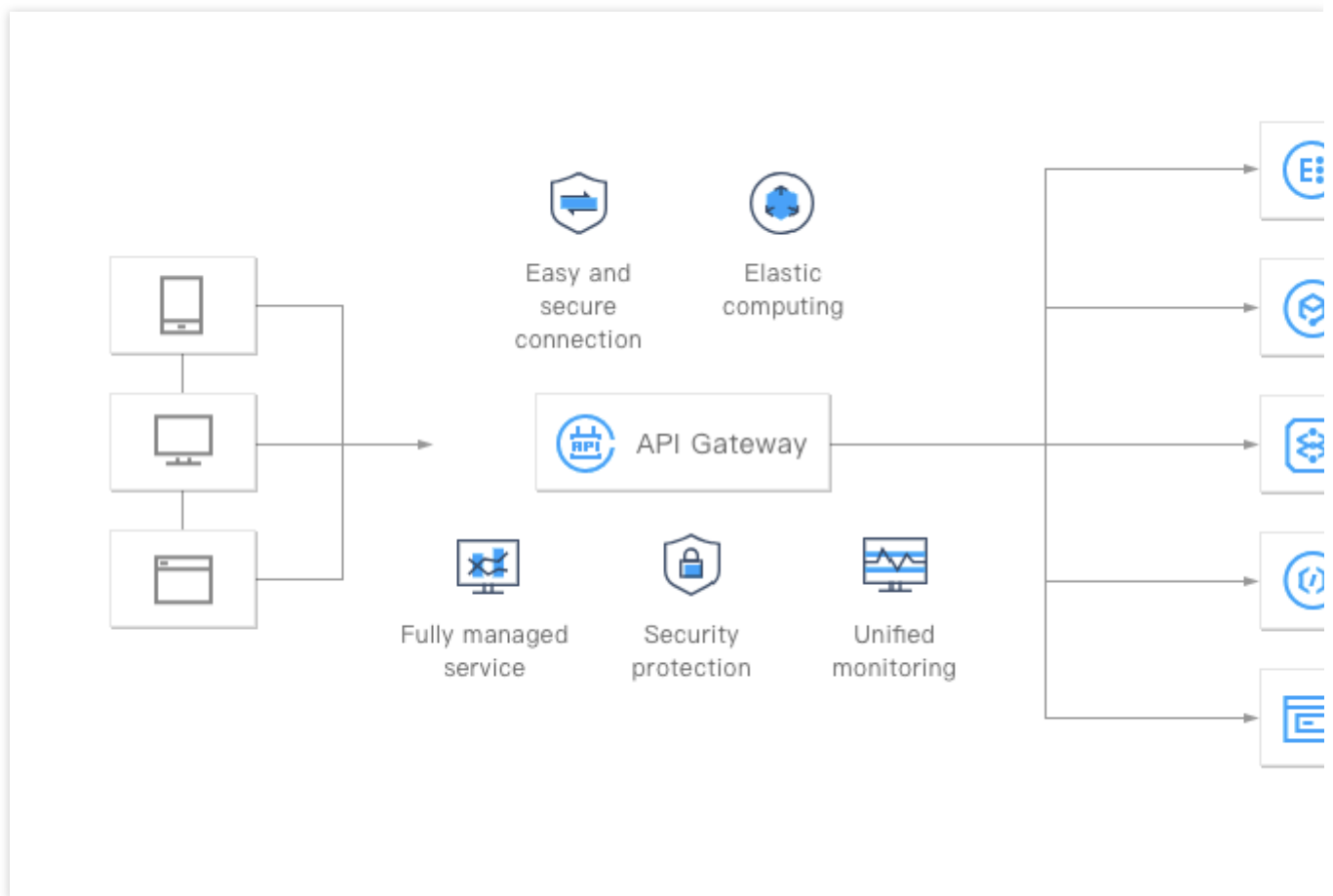
If a customer wants to use API gateway services or a provider wants to provide its business through Tencent Cloud Marketplace, they can use API Gateway. The provider can deploy its businesses on API Gateway, so that end users can directly call the API services with the corresponding domain names through mobile clients, web clients, IoT, or other applications.

Strengths

Last updated：2024-01-03 10:03:44

Simplified Management

You can perform all API management operations in the same place throughout the API lifecycle, including API creation, maintenance, and release. Through API Gateway, you can encapsulate and manage serverless functions from SCF, web services on CVM instances, and your own web services in a unified manner.

Pay-as-You-Go Billing

You only need to pay for the API calls and the outbound network traffic generated in API Gateway. API management, documentation maintenance, SDK generation, traffic control, and permission control are all free of charge.

High Performance and Reliability

By fully utilizing the powerful capabilities of TGW (Tencent Gateway), API Gateway provides high-performance and high-reliability services through multi-regional multi-server distributed clusters to sustain high numbers of large-traffic API calls

Security and Controllability

API Gateway ensures security of API calls in various authentication methods, prevents overload of your business through strict traffic control, and ensures high business availability with the aid of comprehensive monitoring and alarming mechanisms.

Note：

If you need to protect your websites or API services, you can purchase Tencent Cloud Web Application Firewall (WAF). It protects web security at the application layer against attacks made through web vulnerabilities, malicious crawlers, and CC attacks, helping defend your websites and web applications.

Features

Last updated：2024-01-03 10:03:44

API Full Lifecycle Management

Provides complete service (API grouping) and API lifecycle management.

Version management is supported. A version is generated automatically after the API is released. You can switch to any earlier version quickly.

Provides API calling logs and monitoring graphs. Users can view the traffic changes clearly.

API Plugins

Hot update is supported. After a plugin is bound to an API, it can take effect immediately.

Tencent Cloud provides multiple plugin templates to implement the capabilities such as custom CORS, advanced traffic throttling, cache and parameters routing.

Custom plugins are supported. You can write SCF code to modify the data stream.

API Security

Multiple authentication methods such as key pair and OAuth2.0 are supported.

Configuration of both IP blocklist and allowlist at the API level is supported.

API mapping and converting is supported, and the real backend is hidden.

Connection with Tencent Cloud security products such as WAF and BSP is supported.

Open APIs for Use by External Developers

Automatic documentation and SDK based on OpenAPI 3.0 Specification are supported.

APIs can be sold in Tencent Cloud market.

Use Limits

Last updated：2024-01-03 10:03:44

The use limits of API Gateway under a single tenant are as follows:

Category	Limit
Services under one tenant	50
APIs in one service	200
Custom domain names in one service	5
Usage plans under one tenant	200
Key pairs under one tenant	400
Keys bound to one usage plan	50
Usage plans bound to one key pair	10
Maximum QPS allowed in one usage plan	2,000
APIs bound to one usage plan	10,000
Maximum QPS supported by one service	5,000
Uploadable file size in one request	16 MB

Note：

In a shared API Gateway cluster, the maximum QPS a single service can support is 5,000, and this value cannot be increased.

If you need a higher QPS, you can activate the performance-optimized cluster service of API Gateway by submitting a ticket.

Use Cases

Last updated：2024-01-03 10:03:44

Microservice Development

If your system is developed under a microservice architecture, then:

There will be a lot of microservice modules.

Each module has its own APIs.

Each module has its own service address or CLB.

Certain API calls are contextual.

In certain cases, multiple APIs need to be called to get the final data.

The call specifications, naming conventions, and parameter designs of APIs may vary.

The APIs of each module require verification and authentication.

The API requests to certain modules may increase due to business surges.

In this case, it will become increasingly troublesome to manage and use APIs as microservice modules increase. API Gateway can be leveraged to address those issues by helping:

manage APIs in a unified manner, so that users can query and call APIs in the same place.

automatically generate the documentation and SDK and complete test calls, making it easy for users or developers to quickly get started with APIs.

set a request traffic limit, so that backend modules will not fail due to pressure surges.

unify the specifications, naming conventions, and parameter call methods of APIs.

implement unified API authentication.

Serverless Development

After you write a cloud function in Serverless Cloud Function (SCF), if you want to provide an API service for it so that apps, frontend webpages, or clients can access it, an access method will be required.

In this case, you can use API Gateway to configure an API for integration with the backend cloud function. Then, each request to the API will trigger the execution of the cloud function to implement the corresponding business feature. For serverless development, you only need to pay for actual requests and executions.

API Exposure of Traditional Applications

With API Gateway, traditional applications do not need to expose their existing APIs directly to the internet, thus avoiding server vulnerabilities and security issues.

Traffic control in API Gateway can help prevent excessive sudden requests from being passed to your application, ensuring high stability of your business.

When used in combination with Tencent Cloud CAM, API Gateway can grant different users or clients different permissions for the purpose of access control.

Regions and Availability Zones

Last updated：2024-01-03 10:03:44

A region is the physical location of an IDC. Availability zone (AZ) refers to the physical IDC of Tencent Cloud in the same region with independent power supplies and network resources. For more information, see CVM - Regions and AZs.

China

Region	Value
South China (Guangzhou)	ap-guangzhou
East China (Shanghai)	ap-shanghai
East China (Nanjing)	ap-nanjing
North China (Beijing)	ap-beijing
Southwest China (Chengdu)	ap-chengdu
Southwest China (Chongqing)	ap-chongqing
Hong Kong/Macao/Taiwan (Hong Kong, China)	ap-hongkong

Other countries and regions

Region	Value
Southeast Asia (Singapore)	ap-singapore
Northeast Asia (Seoul)	ap-seoul
Northeast Asia (Tokyo)	ap-tokyo
South Asia (Mumbai)	ap-mumbai
Southeast Asia (Bangkok)	ap-bangkok
North America (Toronto)	na-toronto
US West (Silicon Valley)	na-siliconvalley
Europe (Frankfurt)	eu-frankfurt