SOFAStack

API 网关

产品简介

产品版本：AntStack Plus 1.11.0

文档版本：20221013

蚂蚁集团
ANT GROUP

法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

商标声明

免责声明

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.API 网关

1.1. 什么是 API 网关

API 网关是金融分布式架构 SOFAStack 下的一个 API 管理平台，提供 API 托管服务，帮助企业开发者将内部系统的接口封装成 API 开放出去，供外部应用调用，为网络隔离的系统间提供高性能、高安全、高可靠的通信，同时保障内部系统的安全性。用于满足企业对外部合作伙伴开放业务，企业自身混合云互通、企业内网应用集成异构系统间通信的需求，帮助客户更好的进行场景和业务的创新。

API 网关支持的功能如下：

- 提供多种通信协议的 API 管理能力，同时也支持移动端和非移动端应用对 API 的订阅调用。
- 提供 API 的全生命周期管理，包括 API 的定义、测试、发布、版本管理等。
- 提供 API 的安全保障能力，包括身份认证、数据加密、流量控制、访问控制等安全措施。
- 提供 API 的可视化监控功能，帮助更好的运维和管理 API。

1.2. 产品优势

多种客户端接入支持

同一个 API 发布后，既支持 mPaaS 移动端 iOS，Android 的应用接入，也支持非移动端小程序、H5、Web、后端应用等应用接入。

多协议/多语言异构集成

支持不同语言，不同技术栈实现的业务系统之间进行无缝集成，支持协议转换，帮助用户对遗留系统兼容。

超强的安全能力

支持身份认证、数据加密方式、CORS，保障数据传输的安全性，也支持限流、访问控制等流量安全。

端到端全链路跟踪

支持从客户端发起的请求到后端服务所有节点的端到端的链路跟踪。

金融级容灾能力 LDC 单元化路由

支持 LDC 单元化金融级容灾架构场景下的路由转发能力，负责整体单元化架构横向流量的 LDC 路由转发。

灵活的插件自定义能力

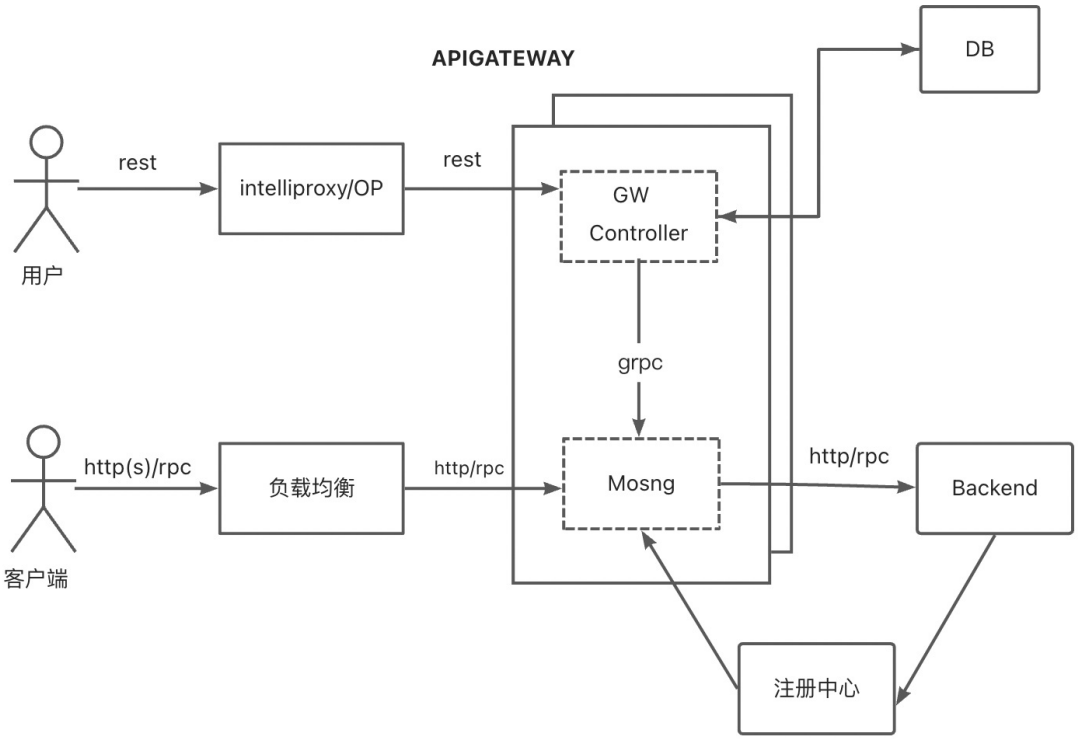
支持多种插件能力，包括参数映射、数据模型、外部授权 API 等多种自定义参数配置模型，满足不同业务场景的统一网关需求，可用于多部门协同时可通过网关实现统一规范场景。

1.3. 产品架构

API 网关主要由 GW Controller 和 Mosng 两个组件构成，GW Controller 将数据推送给 Mosng 后，Mosng 开始对外提供服务。本文主要结合这两个组件介绍 API 网关架构。

API Gateway 系统主要由以下组件构成：

- GW Controller：网关控制台，负责提供页面操作。
- Mosng：核心业务系统，负责提供核心 RPC 能力。



API Gateway 的流量路径如下：

- 用户配置 API 信息
  i. 用户在 API 网关控制台页面配置 API 信息。
  ii. GW Controller 将配置信息入库，通过定时通知其他 APIGateway 容器。
  iii. GW Controller 把所有容器加载更新后的 API 信息通过 gRPC 推送到 Mosng 内存中。
- 应用调用 API 服务
  i. 应用通过 HTTP/SOFARPC/SOFAREST 等协议请求到网关。
  ii. Mosng 网关根据内存中的 API 信息校验应用的请求信息 （验签、解密、RPC 信息校验）。
    - 如果信息校验失败，则直接返回错误信息给应用。
    - 如果信息校验通过，则根据配置的协议（HTTP/SOFARPC/SOFAREST）将应用的请求转发到后端业务服务器。

1.4. 功能特性

功能总览

高性能
提供优化后的数据协议与通讯协议，提高网络通讯质量和效率；

高安全
提供高安全通信、权限管理功能、流量控制功能，确保服务安全可控；

高可靠
在环境恶劣的情况下也能最大程度地保证关键服务的 QoS；

高可用
提供 99.99% 以上的高可用性，确保在任何情况下整个系统始终连续运行不中断；

全生命周期
提供 API 的完整生命周期管理，及可视化的监控信息，简化维护；

API 全生命周期管理

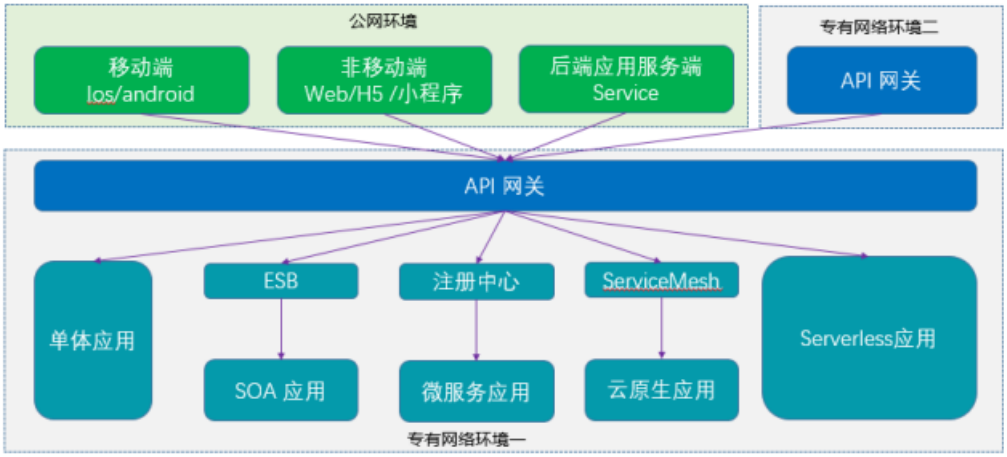
提供 API 的完整生命周期管理，快速构建、发布、订阅、管理 API，统一管理企业所有 API 接口，简化维护，提高效率。

多协议与协议转换

支持 HTTP、SOFARPC、DUBBO 协议。对于异构系统，也支持上述协议之间的两两互相转换。未来会支持更多的协议以及自定义协议。

异构集成

通过 API 网关，在不改变现有 IT 架构的情况下重塑 IT 架构，通过 API 打通不同的技术栈，连通不同的技术架构的各方系统，不同的终端调用，整合异构代码，快速构建新的产品和服务。对于微服务架构，网关支持使用注册中心寻址，对接多种注册中心，包含 SOFA Registry 和 Zookeeper 等。



流量治理

API 网关具有丰富的流量治理能力，网关可以对单个接口配置多种策略：

- 缓存策略：在指定的单位时间内，设置接口返回响应的缓存键值和缓存时间长度，这样在特定时间内，反复请求该接口，会返回固定的第一次的接口，避免多次反复请求打挂后端服务。
- 限流熔断策略：对单个接口到后端集群的 QPS 进行限制，在流量达到一定的阈值后，触发接口的限流熔断，返回指定好的异常结果。
- 多种路由方式：
  - 根据路径路由：HTTP 接口常规路由能力，要支持更换前后端路径的重定向能力。
  - 根据 Header 参数路由：根据请求头里的参数进行路由。
  - 根据权重路由：根据流量百分比的配置，将流量进行分流，按照百分比进行转发。
  - 根据 LDC 路由：网关要支持容灾架构，并且有多机房部署的实践经验，支持单元化路由，根据 UID 等参数进行路由。

参数映射

API 网关支持参数映射。参数映射是将请求或响应参数中的不规范或者不统一的参数，通过自定义脚本的方式，映射为符合客户端或者服务端规范的参数。该功能常用于多部门协同、实现参数统一规范，以及实现统一错误码等场景。 配置参数映射的脚本大致如下图所示：

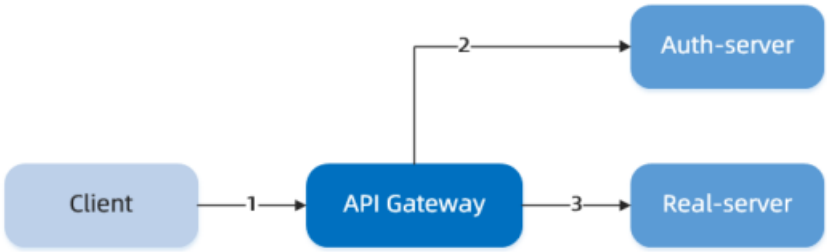
数据模型/API 文档

为了便于企业 API 进行批量管理，存量系统的 API 可以无缝导入新系统；在系统上线后， API 可以在不同的环境中导入，也可在在网络不通的环境互相导入。目前网关支持 Swagger 和 ProtoBuf 格式数据模型的导入，导入生成接口的数据模型后，在配置新的接口时，可以引入已经创建好的数据模型，对于接口复杂类型的录入（如 Object Map 等的多重嵌套）非常方便。

同时，对于已经创建完成的接口还可以生成并下载 Swagger 格式的文档，用于开发者的日常查看。

访问鉴权

网关需提供接入服务与接出服务的服务管控，对于 API 的订阅方进行鉴权。在 API 网关，开发者可以对指定接口进行授权对象的管理，可以指定应用（APPID）有权限调用特定的接口。同时，API 网关还提供了自定义外部授权接口（auth-api），将外部授权接口绑定到业务接口后，在发起请求时，客户端会先调用预先定义好的外部授权接口，通过后，才能调用真实的业务接口，外部授权 API 可以实现业内通用的 Oauth 2.0、JWT、Authentication 等鉴权能力。



批量授权与导入导出

当需要将单个 API 绑定给多个应用时，或单个应用需要绑定多个 API 时，支持通过批量授权方式统一绑定。API 管理过程中，也支持直接通过批量导入和导出的方式创建 API，大大提高配置效率。

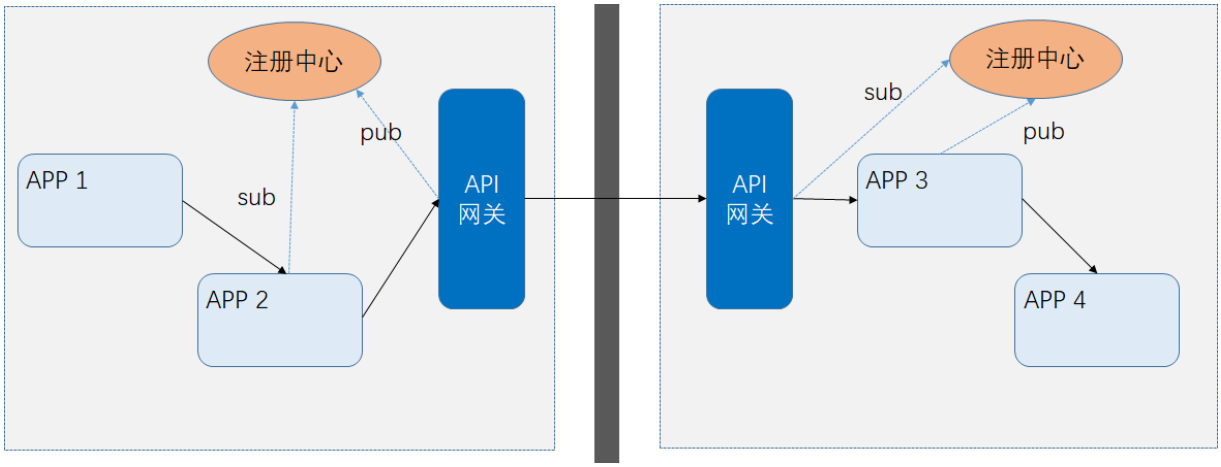
安全能力

在分布式架构下，API 网关保证了架构的安全、通信的安全、数据的安全：

- 系统架构方面，网关满足高可用架构和单元化能力并有成熟和经过实践验证的容灾部署方案，网关的节点可以无间断扩容，水平扩展节点，线性增加网关的 TPS 上限。
- 网络通信方面，网关满足通信安全的要求，具有以下能力：
  - 加验签能力，网关可以对单个接口使用 AK\SK 进行加签和验签，并且支持 **客户端-网关** 和 **网关-后端 server** 的双重加验签，即两段可以使用不同的 AK\SK。
  - IP 黑白名单能力，对单个接口进行 IP 黑白名单策略的绑定，可以指定特定的 IP 段或者 IP 地址的黑/白名单，允许或禁止特定的客户端访问指定的接口。
  - 浏览器跨域（CORS）能力，网关对单个接口配置 CORS 策略，允许指定或者全部来源的域名调用接口。
- 数据安全方面，网关在接口通信时能够通过密钥来进行加验签，同时对数据加密，目前网关支持主流的 ECC、RSA 和国密加密方式。

跨域互通

API 网关支持打通两个网络隔离的区域，并且支持 API 粒度的打通，如下图所示，可以配置一个 APP 3 对外开放的双网关 API，APP 2 作为调用端，可以在网络不通的另外一个环境发起调用，直接请求另一个区域中的 APP3。

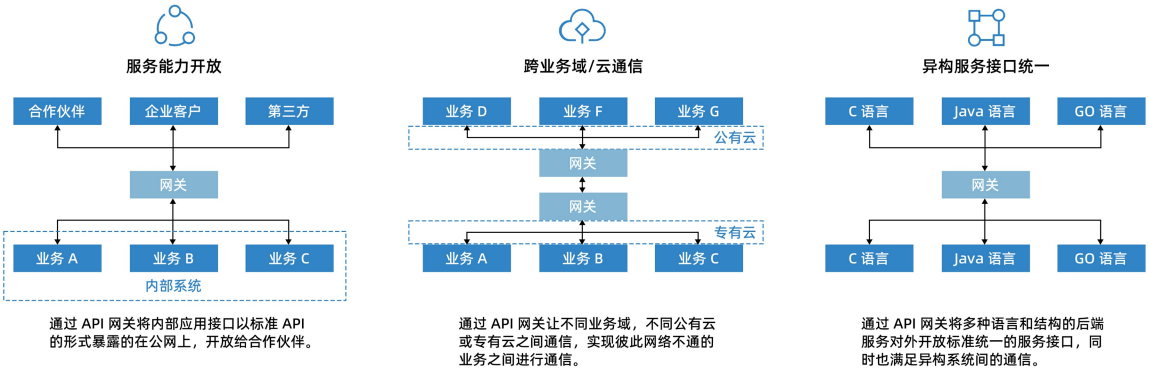


接口编排

在复杂的业务功能场景下，需要调用多个 API 接口才能够完成，此时可以使用网关接口编排功能，将多个接口按照业务顺序编排在一起，最终整合成一个结果返回给调用方。

1.5. 应用场景

本文主要介绍 API 网关在实际使用过程中有哪些应用场景，包括前后端分离场景、异构系统集成场景和混合云场景。



1.5.1. 前后端分离场景

- **统一接入标准**

  通过 API 网关向客户端提供统一协议的 API，允许 IT 团队选择最适合内部架构的技术栈。

- **后端异构集成**

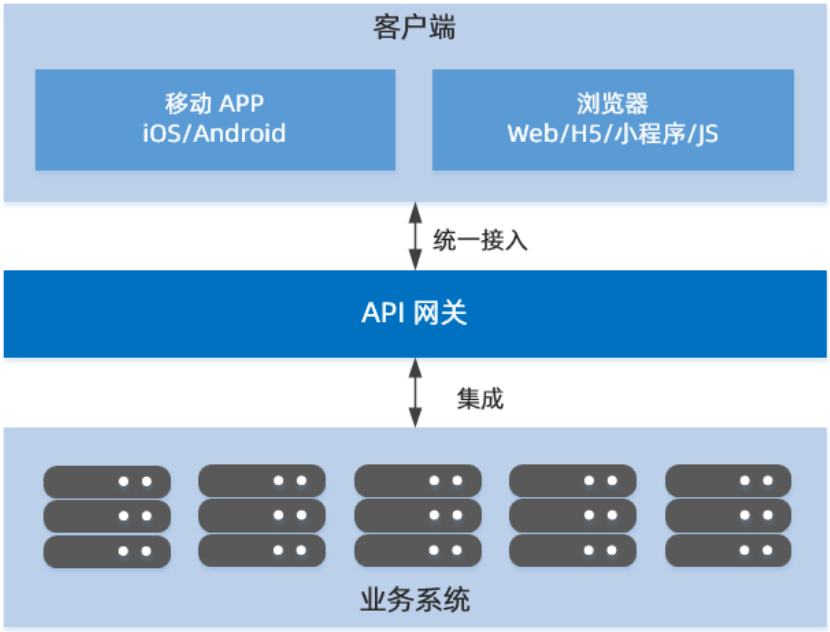
  屏蔽客户端与服务端差异，能够在不对外部绑定客户端产生负面影响的情况下重构服务。

- **降低业务代码复杂性**

  减少客户端与服务端的直接调用，流量控制、负载均衡等不需要每个服务都实现一遍。

- **提高研发效率**

  API 网关可以模拟或虚拟化服务，以验证设计要求或协助集成测试，提高研发效率。



1.5.2. 异构系统集成场景

- **统一集成**

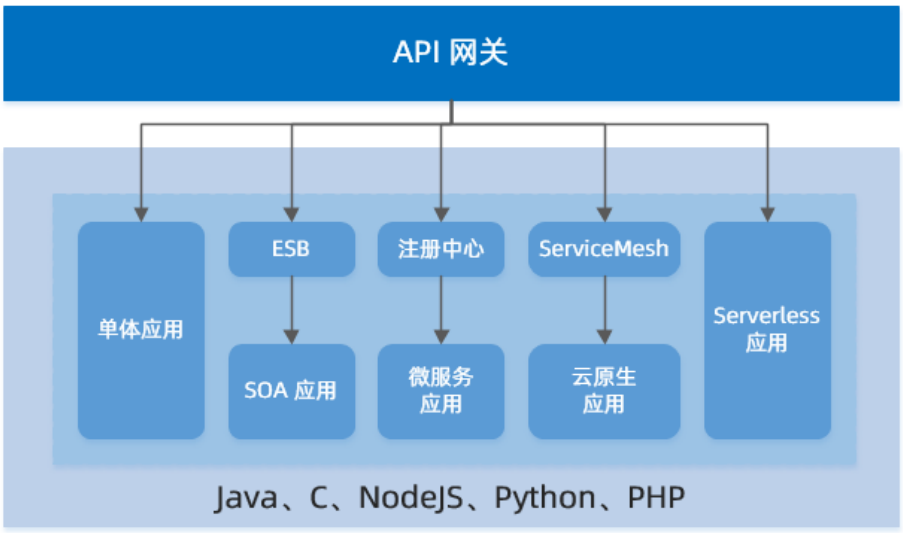
  降低企业内部系统集成的成本，无缝连接不同的软件应用程序。

- **遗留系统兼容**

  允许 IT 团队选择最适合技术栈，在转型过程中并且可以兼容遗留系统，加速企业转型升级。

- **集中管理**

  IT 团队可以从更集中的位置访问所有数据，提高研发效率。



1.5.3. 混合云场景

- **API 全生命周期管理**

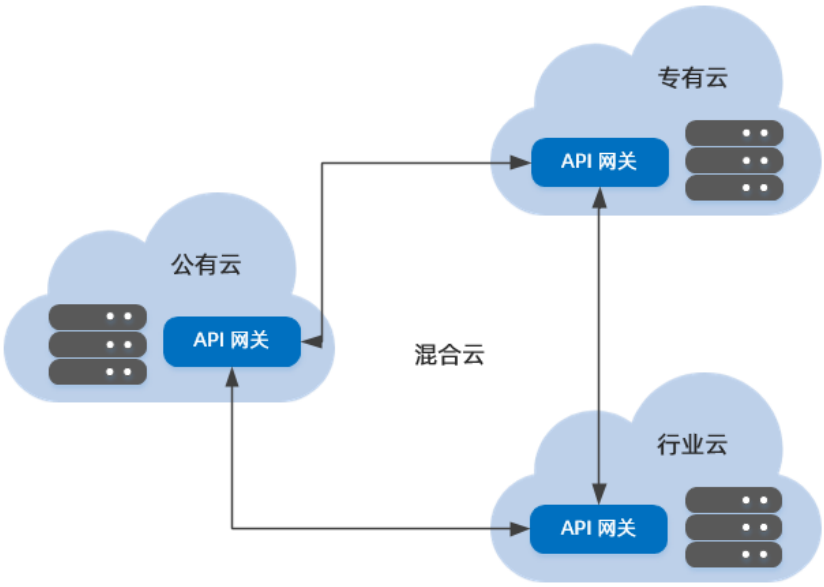
  云与云之间网络互通的基础上提供API全生命周期管理，避免所有 API 都对外暴露，提高 API 的安全性。

- **高性能跨云 RPC调用**

  支持跨云的场景下的 RPC 调用，使用方式同云内调用。

- **超强安全保障能力**

  提供多种安全能力确保访问的合法性以及数据安全性。



1.6. 基础术语

中文	释义
API	应用程序编程接口，是一些预先定义的函数，或指软件系统不同组成部分衔接的约定。
API 分组	用于将 API 进行逻辑的分组，分组下的 API 使用相同的分组标识做隔离。
分组标识	用于在网关上做全局的唯一标识，定位找访问的 API。
默认二级域名	客户端使用 HTTP 协议访问网关时使用，由分组标识+网关的二级域名组成。
SSL	安全套接字层，是一种标准协议，用于加密浏览器和服务器之间的通信。
前端协议类型	是指客户端请求到网关时使用的协议类型。

中文	释义
HTTP	超文本传输协议。
SOFARPC	蚂蚁集团自研的 RPC 调用框架。
请求路径	表示请求的资源的 URL，通过请求路径可以定位到要请求的资源。
绝对匹配	调用的请求路径固定为创建时填写的 API 请求 Path。
前缀匹配	只要请求路径前缀相同则都匹配到这个接口上，实现接口定义多个不同 Path。
HTTP 方法	表明要对给定的 HTTP 资源执行的操作。
请求参数	表示客户端向网关发起请求时要配置的参数。
header 参数	报文头包含若干个属性，格式为“属性名：属性值”，服务端据此获取客户端的信息。
query 参数	一般是指 URL 中 `?` 后面的参数。
请求 body 参数	指请求体中的数据。
响应参数	用于对响应内容进行解释。
响应 body 参数	用于解释响应体里的参数含义。
响应示例	用于示例响应的状态。
业务错误码	用于解释响应里的业务错误码代表的意思。
接口全名	RPC 接口的接口命名，就完成某些特定功能的类，是一个功能的集合。
RPC 方法	RPC 接口里的方法，表明要资源执行的具体操作。

中文	释义
OperationType	针对 mPaaS 移动应用设置的 API 服务标识，用于定位要访问的资源。
后端服务类型	表示网关接收到请求后转发给的后端服务类型。
后端协议类型	表示网关接收到请求后转发给的后端服务使用的通信协议类型。
报文类型	表示请求和响应中的媒体类型信息，告诉服务端如何处理请求的数据，以及告诉客户端（一般是浏览器）如何解析响应的数据。
报文编码	客户端接受什么字符集的文本内容。
MOCK	如果接口后端还没有提供，使用 Mock 用于模拟一个后端服务。
系统集群	表示网关接收到前端请求后转发到真实业务系统的集群。
地址配置方式	表示系统集群的地址来源。
集群地址	表示系统集群的地址，可以是 IP 地址，也可以是域名。
负载均衡	当后端地址大于 1 个时使用的负载均衡策略。
后端认证方式	表示网关向后端业务系统发送请求时是否要加签。
路由规则	表示当网关接收到语法后使用的路由策略。
应用	表示非 mPaaS 移动应用以外的应用。
mPaaS 移动应用	表示 mPaaS 移动应用，必须和 mPaaS 移动开发平台一起使用。