SOFAStack

API 网关

技术白皮书

产品版本：AntStack Plus 1.11.0

文档版本：20220928

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

1.什么是 API 网关

产品背景

API 网关的前身是 SOFAGW 和 mPaaSGW，SOFAGW 是 SOFAStack 中的核心组件，mPaaSGW 是 mPaaS 中的核心组件，二者皆提供网关服务。区别是 SOFAGW 面向的是 Web 应用和跨云的场景，而 mPaaSGW 专注于移动端。随着产品的不断迭代，二者功能的重合度越来越高。用户使用时也越来越困惑：为什么会存在两个网关？ 于是蚂蚁集团决定将 SOFAGW 和 mPaaSGW 融合为一个统一的、通用的，并且适用于各种场景的网关，也就是新一代的 API 网关。

产品简介

API 网关是蚂蚁技术上云的重要组件之一，是内部系统与外部应用通信的桥梁：

- 内部系统通过 API 网关将内部服务开放。
- 外部应用通过 API 网关访问内部系统。

内部系统指的是通常意义上的后端集群，外部应用指的是 Android、iOS 客户端，或者 Web 应用等。外部应用与内部系统之间的通信往往需要鉴权、验签、限流等，内部系统可能使用的不是 HTTP 协议，不能很方便的对外部应用提供服务，需要一个协议转换层来实现这个逻辑。网关可以很好地实现上述两种需求：对请求进行过滤和对协议进行转换。

不仅仅是外部应用，在实际业务中，内部系统之间也存在很多异构系统的通信问题，例如：Java、Nodejs、Go、Python 应用之间如何进行调用？对于这种场景，API 网关的协议转换能力就是一个很好的解决方案。对于更复杂的网络不通场景，比如跨云、跨 VPC 等，API 网关也提出了一系列的解决方案。总而言之，API 网关可以提供全场景的代理服务。

2.产品优势

API 网关致力于打造为一个通用的、全场景的 API 管理平台，提供包括但不限于以下能力。

多协议转换

提供多种协议互相转换的能力，包括 HTTP、SOFARPC、SOFAREST、Dubbo 等。可以帮助服务端将某种协议的 API 通过网关以另一种协议的方式暴露给客户端调用。为异构服务的接入、迁移、改造提供最大程度的便利。

多种 SDK 支持

为了方便调用方快速接入，API 网关提供了 Java、JS、Go 等多种 SDK，还支持代码生成功能，一键生成调用代码，提升用户使用效率。

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。

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。

丰富的 API 治理能力

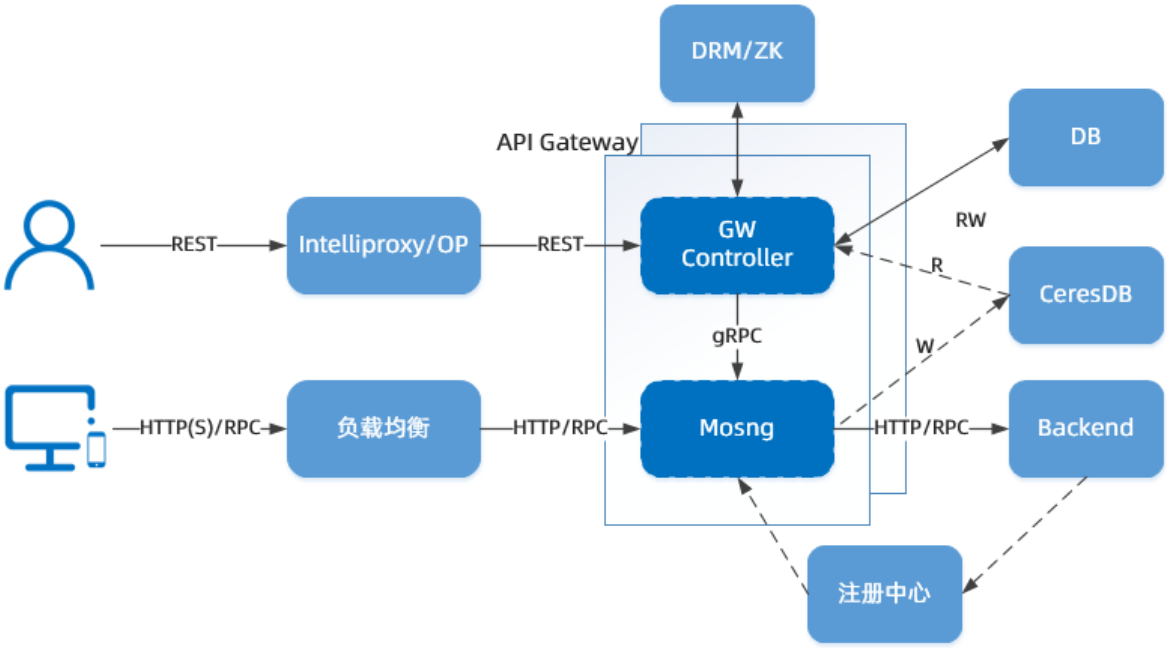
API 网关支持接口级别限流、系统集群级别限流、请求参数签名校验、响应缓存、CORS、数据模型转换、自定义外部授权能力等丰富的 API 治理能力，为后端服务提供自主可控的、高安全性的、高可用的 API 托管服务。

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。

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，并使用 ZK/DRM 通知其他 API Gateway 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。

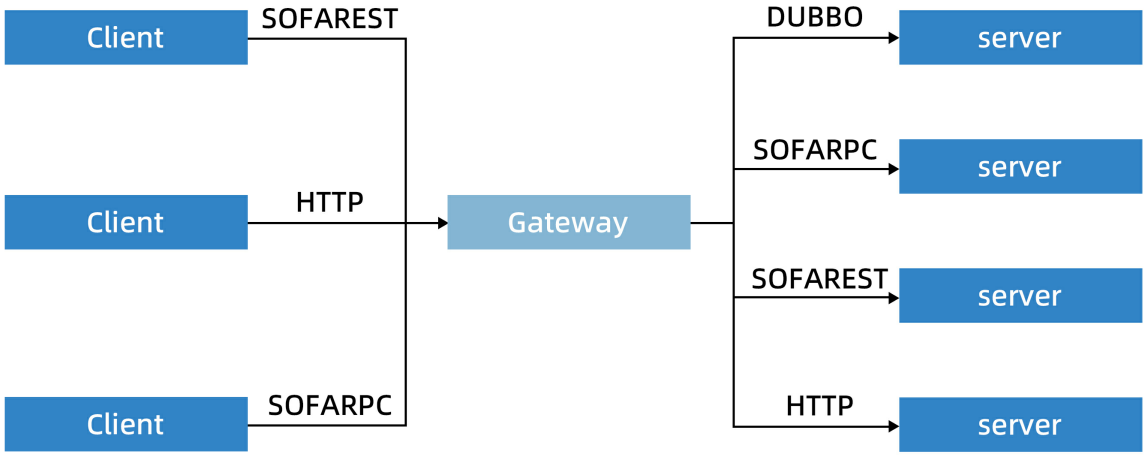
4.性能指标

场景	QPS	RT	CPU
纯转发	20000	400 ms	330
开启验签	17000	110 ms	300
验签+日志	15000	50 ms	310

5.功能特性

协议转换

API 网关当前支持 HTTP、SOFARPC、SOFAREST、DUBBO 协议。同时针对异构系统，网关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。



验签功能

为了验证客户端请求的合法性以及保证数据在传输过程中不被篡改，API 网关提供了签名校验的机制。默认所有的 API 都需要加签验签才可工作，可以在 API 级别下选择是否打开上下游加签验签逻辑。其中加签逻辑遵循的是 HTTP Signature 标准。

加签验签的流程如下：

限流功能

为了保障后端服务不被大流量打垮，API 网关提供了限流的能力。当前网关支持 API 级别的限流，也支持令牌桶级别的限流。限流算法默认是令牌桶算法，也支持漏桶、滑动窗口的限流算法。未来还会支持分布式限流、自适应限流等高级限流算法。

跨域资源共享

针对 HTTP 的跨域请求，API 网关支持 API 级别的跨域配置以及 workspace 级别的跨域配置。支持设置标准 CORS 的规则，包括：

- Access-Control-Allow-Origin：允许跨域的 Origin 列表。
- Access-Control-Allow-Methods：允许跨域的方法列表。

- Access-Control-Allow-Headers：允许跨域的 Header 列表。
- Access-Control-Expose-Headers：允许暴露的 Header 列表。
- Access-Control-Max-Age：最大的浏览器缓存时间。
- Access-Control-Allow-Credentials：是否允许发送 Cookie。

缓存功能

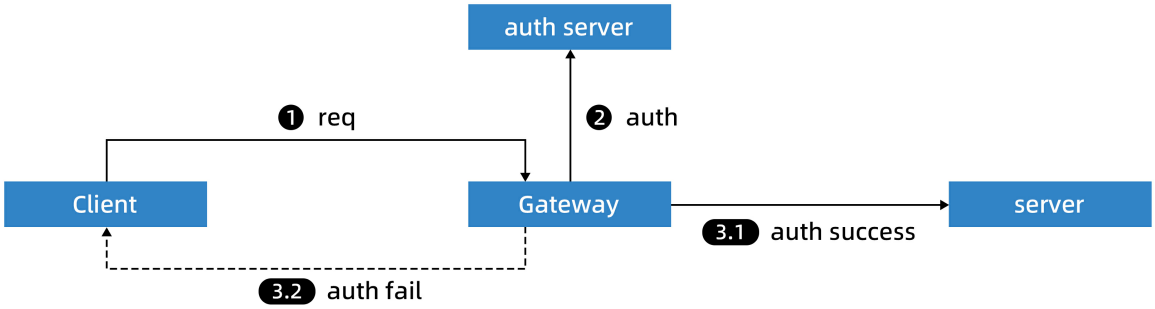
对于读多写少的 API，为了降低对后端 Server 的压力，网关可以对 API 的响应内容进行缓存。缓存的 Key 可以从 Header、Query、Cookie 和 Body 中进行选择，支持设置缓存的 TTL。

高级路由规则

API 网关支持根据 Header 或者权重设置自定义的路由规则，一个请求根据参数的不同从而路由到不同的 Server。当后端有多个 IP 时，支持设置负载均衡算法，当前支持随机和轮询两种算法。同时，API 网关也支持 SOFAStack 下标准的 LDC 路由机制，可以根据 LDC 规则进行请求转发。

外部授权

针对用户对自定义授权，如 OAUTH 能力的诉求，API 网关提供了外部授权的能力。允许客户端请求在到达网关后，先请求用户自定义一个远程 API 进行授权校验，如果校验通过，会转发给后端服务器，否则直接返回给客户端异常信息。该功能可以满足用户的定制化需求，使得 API 的管理更加自主可控。



参数映射

网关可以对客户端的数据进行转换，以另一种格式转发给服务端。同时也支持对服务端的响应进行转换后，返回给客户端。

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。

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。

运维监控

提供完整的服务和系统的日志、巡检和监控，包括 API 网关所有组件系统指标的监控以及运行环境指标的监控，例如：错误率，错误码分布，流入流量和流出流量等。同时，API 网关会记录自身服务处理的工作情况，包括各种异常情况的记录。对于经过网关的请求，网关都会带上 Traceid 透传到下游所有的链路，便于用户进行故障的定位。

6.附录：基础术语

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。

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。

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。