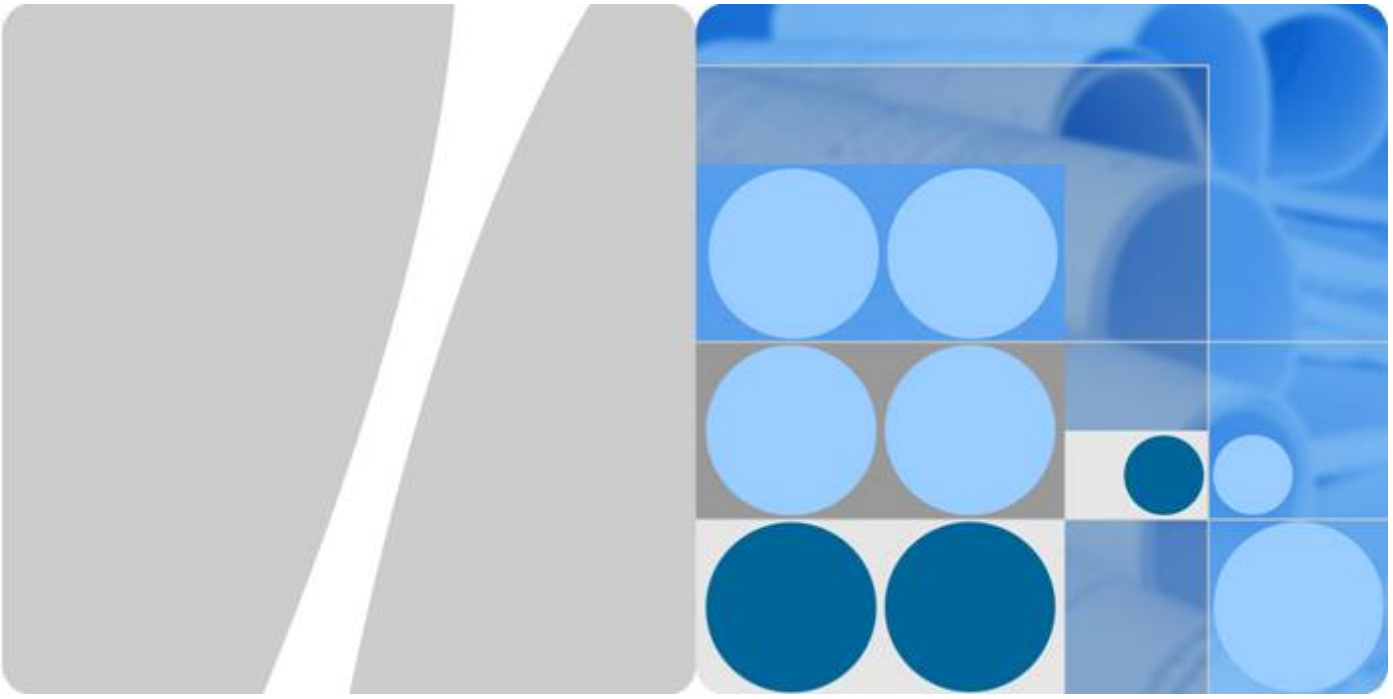


API 网关服务

用户指南

发布日期　2021-10-25

目 录

1 简介

API网关（API Gateway）是为您提供高性能、高可用、高安全的API托管服务，帮助您轻松构建、管理和部署任意规模的API。借助API网关，可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放及业务能力变现。

本手册主要介绍企业或开发者如何通过API网关开放自身的服务、数据，实现业务能力变现。如何获取并调用他人在API网关开放的API，减少开发时间与成本。

2 快速入门

2.1 概述

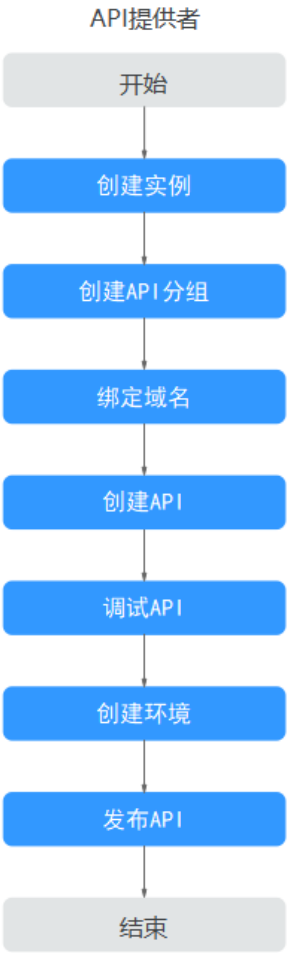
API网关（API Gateway）是为您提供高性能、高可用、高安全的API托管服务，帮助您轻松构建、管理和部署任意规模的API。借助API网关可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放及业务能力变现。

若您想快速体验开放API和调用API的操作流程，请参考**开放API**和**调用API**。这里以APP认证类型的**简易认证**举例，端到端操作快速上手。

2.2 开放 API

2.2.1 开放 API 流程

作为API提供者开放API，您需要先后完成以下流程：



1. 创建实例。
   API网关共享版不需要创建实例
2. **创建API分组**
   API分组相当于API的集合，您在创建API前，需要先创建API分组。
3. **绑定域名**
   开放API前，您需要为API分组绑定独立域名（即自定义域名），API调用者通过访问独立域名来调用您开放的API。
4. **创建API**
   创建API包括定义API前后端的请求路径、参数、请求相关协议等。
5. **调试API**
   提供调试功能，调试API接口，验证服务是否正常。
6. **创建环境（可选）**
   API可以同时提供给不同的场景调用，如生产环境（RELEASE）及其他自定义环境。RELEASE是默认存在的环境，无需创建。
7. **发布API**
   只有在将API发布到环境后，API才支持被调用。

2.2.2 创建 API 分组

步骤1 登录API网关控制台。

步骤2 在左侧导航栏选择“开放API > API分组”。

步骤3 单击“创建分组”，配置分组信息。

表 2-1 配置分组信息

参数	配置说明
分组名称	填写API分组名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	对分组的介绍。

步骤4 单击“确定”，创建API分组。系统会同时为其分配一个子域名，您可以用于调试API。

----结束

2.2.3 绑定域名

步骤1 在“API分组”页面，单击**创建API分组**中分组名称，进入分组详情页面。

步骤2 单击“域名管理”页签。

步骤3 单击“绑定独立域名”，填写要绑定的域名。

说明

填写的独立域名已备案，并且已CNAME解析到分组的子域名上。

步骤4 单击“确定”，将独立域名与API分组绑定。

----结束

2.2.4 创建 API

创建API分为4个步骤：

1. **设置基本信息**
2. **定义API请求**
3. **定义后端服务**
4. **定义返回结果**

设置基本信息

步骤1 在左侧导航栏选择“开放API > API管理”。

步骤2 单击“新建API”，设置API基本信息。

表 2-2 设置基本信息

参数	配置说明
API名称	填写API名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
所属分组	默认**创建API分组**中已创建分组。
网关响应	API网关未能成功处理API请求，从而产生的错误响应。 默认的网关响应为“default”。
类型	默认“公开”。
安全认证	选择API认证方式，此处选择“APP认证”。
支持简易认证	简易认证不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。此处开启简易认证，
标签	标签主要用于对API添加分类属性，方便在创建了大量API后，快速过滤和查找。
描述	API的描述。

步骤3 单击“下一步”。

----结束

定义 API 请求

步骤1 在“定义API请求”页面，配置API请求信息。

表 2-3 定义 API 请求

参数	配置说明
域名	**创建API分组**时，系统默认分配的一个子域名。
请求协议	选择API请求协议，此处选择“HTTPS”。
请求Path	接口请求的路径。
匹配模式	默认“绝对匹配”。
Method	接口调用方式，此处选择“POST”。
支持CORS	为方便起见，此处不开启。

步骤2 单击“下一步”。

----结束

定义后端服务

步骤1 在“定义后端服务”页面，配置后端服务信息。

步骤2 选择后端服务类型，此处选择“HTTP/HTTPS”。

表 2-4 HTTP/HTTPS 类型定义后端服务

服务参数	参数说明
协议	选择协议类型，此处选择“HTTP”。
请求方式	接口调用方式，此处选择“POST”。
使用VPC通道	选择“不使用”VPC通道访问后端服务。
后端服务地址	后端服务的地址。
后端请求Path	后端服务的路径。
后端超时	后端服务请求的超时时间。此处默认“5000”ms。
后端认证	后端服务对API调用增加自己的认证。为方便起见，此处不开启。

步骤3 单击“下一步”。

----结束

定义返回结果

步骤1 在“返回结果基础定义”页面，定义返回结果。

表 2-5 定义返回结果

信息项	描述
成功响应示例	成功调用API时，返回的响应信息示例。
失败响应示例	调用API失败时，返回的响应信息示例。

步骤2 单击“完成”，完成API的创建。

----结束

2.2.5 调试 API

步骤1 在“API管理”页面，在已**创建API**所在行，单击“更多 > 调试”。

步骤2 左侧为API请求参数配置区域，参数说明如**表2-6**所示。右侧为API发送的请求信息和API请求调用后的返回结果回显。

表 2-6 调试 API

参数	配置说明
协议	仅在API请求的“请求协议”为“HTTP&HTTPS”时，支持修改。
方法	仅在API请求的“Method”定义为“ANY”时，支持修改。
路径	API的请求path。
查询参数	Query的参数与参数值。
请求头	HTTP Headers的参数与参数值。
请求体	仅在API请求的“Method”定义为“PATCH”/“POST”/“PUT”时，支持修改。

步骤3 单击“发送请求”。

若调用成功时，状态码显示“200”。

----结束

2.2.6 创建环境（可选）

步骤1 在左侧导航栏选择“开放API > 环境管理”，进入到环境管理信息页面。

步骤2 单击“创建环境”，填写环境信息。

表 2-7 环境信息

参数	配置说明
环境名称	填写API环境名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	环境描述信息。

步骤3 单击“确定”，创建环境。

----结束

2.2.7 发布 API

步骤1 在左侧导航栏选择“开放API > API管理”，进入到API管理信息页面。

步骤2 在已**创建API**所在行，单击“发布”。

步骤3 选择API需要发布到的环境。

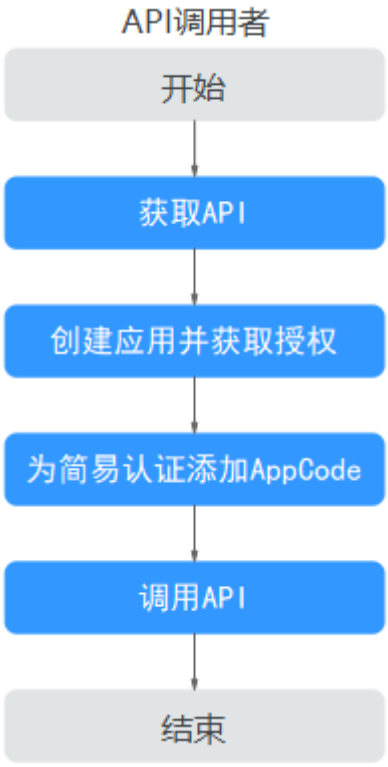
步骤4 单击“发布”。

----结束

2.3 调用 API

2.3.1 调用 API 流程

作为API调用者调用API，您需要完成以下流程：



1. 获取API

   从API提供者中获取API和文档信息。

2. **创建应用并获取授权**

   使用APP认证的API，需要在API网关中创建一个应用，并且绑定API后，才可以使用APP认证调用API。

3. **为简易认证添加AppCode**

   使用简易认证，API网关也仅校验AppCode。

4. **调用API**

   为简单起见，此处使用接口测试工具，通过APP认证方式中的凭证来实现对API的调用。

2.3.2 创建应用并获取授权

创建应用

步骤1 在左侧导航栏选择“调用API > 应用管理”，进入到应用管理信息页面。

步骤2 单击“创建应用”，填写应用信息。

表 2-8 应用信息

信息项	描述
应用名称	填写应用名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
描述	对应用的介绍。

步骤3 单击“确定”，创建应用。

步骤4 单击已创建应用名称，进入应用详情页面，查看AppKey和AppSecret。

----结束

绑定 API

步骤1 在绑定的API列表上方，单击“绑定API”。

步骤2 选择**开放API**中的运行环境、API分组和API，单击“绑定”，完成API绑定策略。

----结束

2.3.3 为简易认证添加 AppCode

步骤1 在应用列表中单击已**创建应用**名称，进入应用详情。

步骤2 单击“AppCode”页签。

步骤3 单击“添加AppCode”。

步骤4 在弹窗中选择“自动生成”生成方式。

步骤5 单击“确定”。

----结束

2.3.4 调用 API

使用接口测试工具配置调用信息。

步骤1 获取API请求信息。

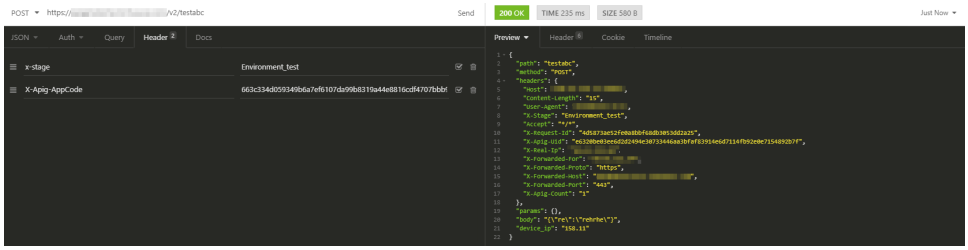
为简单起见，此处通过线下传递方式获取API及文档。API调用者可以从中获取API认证方式，请求方法，请求路径等信息。

步骤2 增加Header参数名称：X-Apig-AppCode，参数值填**已生成的AppCode**。

步骤3 增加Header参数名称：x-stage，参数值为**运行环境**。若API发布到RELEASE环境不需执行此步骤。

步骤4 单击“Send”发送请求。

调用成功后，显示“200 OK”。


POST
Send
200 OK
TIME 235 ms
SIZE 580 B
Just Now
JSON
Auth
Query
Header 2
Docs
Preview
Header 6
Cookie
Timeline
x-stage
Environment_test
X-Apig-AppCode
663c334d059349b6a7efb107da99b8319a44e8816cdf4707bbbf
{
"path": "testabc",
"method": "POST",
"headers": {
"content-length": "15",
"X-Stage": "Environment_test",
"Accept": "*/*",
"X-Request-Id": "4d58730e52fe0a8bbf68db3053dd2a25",
"X-Apig-Uid": "663208be81ee6d2d2494e307334464a3bfaf83916e6d7114fb92e4e715489b7f",
"X-Forwarded-Proto": "https",
"X-Apig-Count": "1"
},
"params": {},
"body": "{\"rex\":\"rehrhe\"}",
"device_id": "358.11"
}

----结束

3 开放 API

3.1 API 分组管理

3.1.1 创建 API 分组

操作场景

创建API前，需要先创建API分组。API分组相当于API的集合，API提供者以API分组为单位，管理分组内的所有API。

说明

- 一个API只能属于某一个API分组。
- 每个用户最多创建50个API分组。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API分组”，进入到API分组信息页面。

步骤4 单击“创建分组”，弹出“创建分组”对话框。填写如表3-1所示信息。

表 3-1 分组信息表

信息项	描述
分组名称	API分组名称，用于将API接口进行分组管理。
描述	对分组的介绍。

步骤5 完成分组信息填写后，单击“确定”，创建API分组。

创建分组成功后，在“API分组”页面的列表中显示新创建的API分组。

说明

- API分组创建后，系统为分组自动分配一个内部测试用的子域名，此子域名每天最多可以访问1000次。
- 对外开放API时，您需要为API分组绑定您自己的独立域名。

----结束

后续操作

API分组创建成功后，您可以为此分组绑定域名，API调用者通过访问独立域名来调用您开放的API。

3.1.2 绑定域名

操作场景

开放API前，您需要为API分组绑定一个或多个独立域名，API网关通过独立域名定位到此分组。如果您未绑定独立域名，那么调用API时默认使用子域名，API网关对子域名的访问次数做了限制，每天最多可以访问1000次。

说明

- 每个分组最多可以绑定5个独立域名。
- 共享版中，不同分组下不能绑定相同的独立域名。

在绑定域名前，您需要理解以下2个概念：

- 子域名：API分组创建后，系统为分组自动分配一个内部测试用的子域名，此子域名唯一且不可更改，每天最多可以访问1000次。
- 独立域名：您自定义的域名，API调用者通过访问独立域名来调用您开放的API。

前提条件

1. 已有独立域名。
2. 已将独立域名CNAME解析到分组的子域名上，具体方法请参见《云解析服务用户指南》的“管理记录集”章节。

3. 如果API分组中的API支持HTTPS请求协议，那么在独立域名中需要添加SSL证书，请您提前准备SSL证书。此证书不支持导入，您需要填写证书的名称、内容和密钥。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API分组”，进入到API分组信息页面。

步骤4 通过以下任意一种方式，进入“域名管理”页签。

- 单击*分组名称*，进入分组详细信息页面。单击“域名管理”。
- 在待绑定域名的分组所在行，单击“更多 > 域名管理”。

步骤5 单击“绑定独立域名”，设置域名信息。

步骤6 单击“确定”，将独立域名与API分组绑定。

如果不再需要此域名时，在域名所在行，单击“解除绑定”。

步骤7 （可选）绑定SSL证书。API分组中的API支持HTTPS请求协议时，需要添加SSL证书。

1. 单击“添加SSL证书”，弹出“添加SSL证书”对话框。
2. 根据**已获取SSL证书**，输入证书名称、证书内容和密钥，单击“确定”，完成SSL证书的添加。

说明

- SSL证书目前仅支持pem类型，如需添加其它证书类型，可转换成pem类型后添加。
- 如果需要编辑此SSL证书，单击证书名称后的 ✎，修改证书名称。由于证书内容和密钥已经加密，不支持再次查看，如果需要修改，请重新输入新的证书内容或者密钥。
- 如果不再需要此SSL证书，在域名所在行，单击“删除SSL证书”。

----结束

常见问题

- 绑定域名失败常见原因：未将独立域名CNAME解析到分组的子域名上或域名重复。
- 添加SSL证书失败常见原因：生成证书的域名和实际添加证书所用的域名不一致。

后续操作

绑定独立域名后，您可以开始**创建API**，将API接口配置在API网关中，开放后端能力。

3.1.3 删除分组

操作场景

API分组在创建后，如需对创建的数据进行删除，可以删除此分组。

前提条件

已创建分组。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API分组”，进入到API分组信息页面。

步骤4 通过以下任意一种方式，进入“删除分组”对话框。

- 在待删除的API分组所在行，单击“更多 > 删除”。
- 单击“*分组名称*”，进入分组详情页面，在右上角单击“删除”。

步骤5 按照提示，在输入框中输入“DELETE”，单击“确定”，完成删除应用分组信息。

----结束

3.1.4 新增网关响应

操作场景

网关响应，指API网关未能成功处理API请求，从而产生的错误响应。API网关提供默认的网关响应（default），如果您需要自定义响应状态码或网关响应内容，可在API分组管理中新增网关响应，其中响应内容符合JSON格式即可。

例如，“default”网关的响应内容为：

```
{"error_code": "$context.error.code", "error_msg": "$context.error.message", "request_id": "$context.requestId"}
```

您可以自定义为：

```
{"errorcode": "$context.error.code", "errormsg": "$context.error.message", "requestid": "$context.requestId","apiId":"$context.apiId"}
```

JSON体的内容可以按需定制，包括增减字段内容。

说明

- API提供的默认网关响应“default”也可以编辑修改。
- 您可以新增多个网关响应，支持同一分组下不同API配置不同的网关响应内容。
- 网关响应所定义的错误类型固定且不可修改，具体见**网关错误响应类型说明**。
- 响应内容支持调用API网关运行时变量（$context变量），具体见**API网关运行时可获取变量**。

前提条件

已创建分组。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API分组”，进入到API分组信息页面。

步骤4 找到您要新增或编辑修改网关响应的分组，单击并进入分组详情页。

步骤5 单击其中的“网关响应”页签，即可新增网关响应。

说明

- 如需编辑具体某个响应的详情，右侧有“编辑”按钮，单击即可修改响应状态码、响应内容。
- 不论是“default”或是您自定义的网关响应，响应类型范围固定不可修改。您可以修改每种响应的状态码，以及响应内容。
- 响应内容的错误信息以及其他信息，可通过变量的方式获取，支持的变量见表3-3。

----结束

网关错误响应类型说明

API网关提供的错误响应类型见表3-2，其中响应状态码可以按实际需要做自定义修改。

表 3-2 API 网关的错误响应类型

错误说明	默认的响应状态码	详细说明
拒绝访问	403	拒绝访问，如触发配置的访问控制策略、或异常攻击检测拦截
自定义认证配置错误	500	自定义认证方异常，通信失败、返回异常响应等错误
自定义认证失败	500	自定义认证方返回认证失败
自定义认证身份来源错误	401	前端自定义认证的身份来源信息缺失或不合法错误
认证失败	401	认证失败，IAM或APP认证校验失败
认证身份来源缺失	401	认证身份来源信息缺失
后端超时	504	后端超时，与后端的网络交互超过预配置的时间错误
后端不可用	502	后端不可用，网络不可达错误
默认4XX	-	其它4XX类错误
默认5XX	-	其它5XX类错误
未找到匹配的API	-	未匹配到API
请求参数错误	404	请求参数校验失败、不支持的HTTP方法

错误说明	默认的响应状态码	详细说明
调用次数超出阈值	429	API调用次数超出所配置的流量策略阈值
应用未授权	401	使用的应用未被授权访问该API

API 网关运行时可获取变量

表 3-3 网关错误响应消息体支持的变量

运行时变量名称	描述
$context.apiId	API的ID
$context.appId	API调用者的APP对象ID
$context.requestId	当次API调用生成跟踪ID
$context.stage	API调用的部署环境
$context.sourceIp	API调用者的源地址
$context.authorizer.frontend.property	前端自定义认证响应的context映射的指定键值对的字符串值
$context.authorizer.backend.property	后端自定义认证响应的context映射的指定键值对的字符串值
$context.error.message	当前网关错误响应的错误信息
$context.error.code	当前网关错误响应的错误码
$context.error.type	当前网关错误响应的错误类型

3.2 API 管理

3.2.1 创建 API

操作场景

API提供者把API接口配置在API网关中，开放后端能力。

创建API主要分为四个步骤：设置基本信息、定义API请求、定义后端服务和定义返回结果。

说明

- API网关服务基于REST的API架构，API的开放和调用需要遵循RESTful相关规范。
- 每个用户最多可以创建200个API。

前提条件

- 已创建API分组。如果未创建API分组，可在本操作页面中创建API分组。
- 如果后端服务需要使用VPC通道，请先**创建VPC通道**，或在本操作页面中创建VPC通道。

设置基本信息

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API列表信息页面。

步骤4 单击“新建API”，进入“新建API”页面。填写如**表3-4**所示信息。

表 3-4 基本信息

信息项	描述
API名称	API名称，根据规划自定义。建议您按照一定的命名规则填写API名称，方便您快速识别和查找。
所属分组	API所属分组。 如果尚未创建API分组，单击“新建分组”，为API新创建一个分组。
网关响应	网关响应指API网关未能成功处理API请求，从而产生的错误响应。 API网关提供默认的网关响应（default）。如果您需要自定义响应状态码或网关响应内容，可在API分组管理中**新增网关响应**，按照您自己的响应内容，符合JSON格式即可。
类型	API类型： • 公开。

信息项	描述
安全认证	API认证方式： ● APP认证：表示由API网关服务负责接口请求的安全认证。 ● IAM认证：表示借助IAM服务进行安全认证。 ● 自定义认证：用户有自己的认证系统或服务（如使用OAuth认证），可选择“自定义认证”。 ● 无认证：表示不需要认证。 各种认证方式下的API调用稍有不同，具体请参考《开发指南》。 推荐使用APP认证方式。 **须知** ● 认证方式为IAM认证时，任何API网关租户均可以访问此API，可能存在恶意刷流量，导致过量计费的风险。 ● 认证方式为无认证时，任何公网用户均可以访问此API，可能存在恶意刷流量，导致过量计费的风险。 ● 认证方式为自定义认证时，需要在函数工作流服务中写一段函数，对接用户自己的认证系统或服务。如果当前Region没有上线函数工作流服务，则不支持自定义认证。
支持简易认证	**仅当“安全认证”选择“APP认证”时可配置。** 简易认证指APP认证方式下调用API时，在HTTP请求头部消息增加一个参数X-Apig-AppCode，而不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。 注意仅支持HTTPS方式调用，不支持HTTP方式。具体使用请参考**为简易认证添加AppCode**。 **说明** 如果首次创建API未开启简易认证，那么之后开启简易认证，需要重新发布API。请参考**发布API**发布。
自定义认证	**“安全认证”选择“自定义认证”时需要配置。** 自定义认证需要提前创建，可单击右侧的“新建自定义认证”链接创建。
标签	标签主要用于对API添加分类属性，方便在创建了大量API后，快速过滤和查找。
描述	API的描述。

步骤5 单击“下一步”，进入“定义API请求”页面。

----结束

定义 API 请求

步骤1 在“定义API请求”页面，填写如**表3-5**所示信息。

表 3-5 定义 API 请求

信息项	描述
域名	系统默认分配的一个子域名。
请求协议	分为三种类型： • HTTP • HTTPS • HTTP&HTTPS 传输重要或敏感数据时推荐使用HTTPS。
请求Path	接口请求的路径。 格式如：/users/{userId}/projects • {}中的变量为请求参数，表示匹配"/"之间的一整段，不支持匹配"/"之间的一部分，例如/abc{userId}。若匹配模式为绝对匹配，则尾部的请求参数可以添加+号，例如/users/{p+}，其中变量p匹配1或多段"/"之间的部分。 • 请求Path中包含请求参数时，必须设置对应的入参定义。 • 内容区分大小写。
匹配模式	分为两种模式： • 绝对匹配：调用的请求Path固定为创建时填写的API请求Path。 • 前缀匹配：调用的请求Path将以创建时填写的API请求Path为前缀，支持接口定义多个不同Path。 例如，请求路径为/test/AA，使用前缀匹配时，通过/test/AA/CC可以访问，但是通过/test/AACC无法访问。 **说明** 使用前缀匹配时，匹配剩余的路径将透传到后端。 例如，使用前缀匹配，前端请求路径定义为/test/，后端请求路径定义为/test2/，通过/test/AA/CC访问API，则后端收到的请求url为/test2/AA/CC。
Method	接口调用方式：GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY • 其中ANY表示该API支持任意请求方法。 • 当“Method”为“POST”/“PUT”/“PATCH”/“ANY”时，您可以在“请求体内容描述”中增加对于请求体的描述信息。
支持CORS	是否开启跨域访问CORS（cross-origin resource sharing）。 CORS允许浏览器向跨域服务器，发出XMLHttpRequest请求，从而克服了AJAX只能同源使用的限制。 CORS请求分为两类： • 简单请求：头信息之中，增加一个Origin字段。 • 非简单请求：在正式通信之前，增加一次HTTP查询请求。 开启CORS（非简单请求）时，您需要单独创建一个“Method”为“OPTIONS”的API，具体步骤请参见**开启跨域访问**。

步骤2 （可选）设置入参定义。

入参定义是指您调用API时，需要传入的参数的说明。

1. 单击“添加入参定义”，弹出“添加入参定义”对话框。
2. 输入如**表3-6**所示信息。

表 3-6 入参定义

信息项	描述
参数名	参数的名称，如果参数在“PATH”位置，那么参数名称需要和“请求Path”中的名称相同。 **说明** – 参数名不能是x-apig- 、x-sdk-开头，不区分大小写。 – 参数名不能是x-stage，不区分大小写。 – 参数位置为HEADER时，参数名不能是“Authorization”和“X-Auth-Token”，不区分大小写，也不支持下划线。
参数位置	选择参数在请求中的位置。参数位置有如下三种：PATH、HEADER、QUERY。 **说明** 当您定义了PATH中的参数时，该参数需要在“请求Path”中同步定义。
类型	字段的类型，包含String和Number。 **说明** 入参如果为boolean，请选择String。
必填	请求API时，此参数是否为必填。如果选择“是”，API网关将校验请求中是否包含此参数，如果不包含，则拒绝该请求。
默认值	“必填”为“否”时，默认值生效。请求中不包含此参数时，API网关自动增加默认值发送给后端服务。
最小长度	参数值的最小长度，仅允许输入数字。
最大长度	参数值的最大长度，仅允许输入数字。
示例	参数值的填写示例。
描述	对于此参数的描述。

3. 单击“确定”，完成入参定义的设置。

步骤3 单击“下一步”，进入“定义后端服务”页面。

----结束

定义后端服务

API网关支持定义多个策略后端，即满足一定条件后转发给指定的API后端服务，用以满足不同的调用场景。例如为了区分普通调用与特殊调用，可以定义一个“策略后端”，通过调用方的源IP地址，为特殊调用方分配专用的后端服务。

除了定义一个默认的API后端服务，一个API共可以定义5个策略后端。

步骤1 定义默认后端。

添加策略后端前必须定义一个默认后端，当不满足任何一个策略后端的API请求，都将转发到默认的API后端。

在“定义后端服务”页面，选择API后端服务类型。

后端服务类型参数描述见**表3-7**、**表3-8**、**表3-9**。

表 3-7 HTTP/HTTPS 类型定义后端服务

服务参数	参数说明
协议	HTTP或HTTPS，定义的后端服务协议须与用户的后端业务协议保持一致。 **说明** • 支持WebSocket通信。 • 传输重要或敏感数据时推荐使用HTTPS。
请求方式	接口调用方式，包括GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY。 其中ANY表示该API支持任意请求方法。
使用VPC通道	是否使用VPC通道访问后端服务。 • **若使用VPC通道，选择已创建的VPC通道名称。** **说明** – VPC通道中，云服务器的安全组必须允许100.125.0.0/16网段访问，否则将导致健康检查失败及业务不通。 • **若不使用VPC通道，需要设置后端服务地址。** 格式：“主机:端口”，主机为IP地址/域名，未指定端口时，HTTP协议默认使用80端口，HTTPS协议默认使用443端口。 端口范围：1 ~ 65535。 如果需要创建变量标识，则填写“#变量名#”，如#ipaddress#。支持创建多个变量标识，如#ipaddress##test#。
自定义host头域（可选）	**仅当“使用VPC通道”选择“使用”时可配置。** 在请求被发送到VPC通道中主机前，允许您自定义请求的Host头域，默认将使用请求中原始的Host头域。
后端请求Path	后端服务的路径，即服务的uri，可以包含路径参数，以{路径参数}形式表示，比如/getUserInfo/{userId}。 如果请求路径中含有环境变量，则使用#变量名#的方式将环境变量定义到请求路径中，如/#path#。支持创建多个环境变量，如/#path##request#。
后端超时	后端服务请求的超时时间。 如果在API调试过程中，遇到后端响应超时之类的错误，请适当调大后端超时时间，以便排查原因。

服务参数	参数说明
后端认证	当您的后端服务需要对API调用增加自己的认证，则需要开启后端认证。 后端认证需要先添加一个**自定义认证**，自定义认证通过函数工作流服务实现，在函数工作流服务中编写一个函数，实现您的认证鉴权流程，或者使用函数调用您的统一鉴权服务。 **说明** 后端认证依赖函数工作流服务，此功能仅在部分区域开放。

表 3-8 FunctionGraph 类型定义后端服务

服务参数	参数说明
FunctionURN	函数请求唯一标识。 单击“添加”，添加所需的FunctionURN。
版本	函数的版本。
调用类型	• Synchronous：同步调用。指后端函数工作流服务收到调用请求后立即执行并返回调用结果，客户端发送请求后同步等待，收到后端响应后关闭连接。 • Asynchronous：异步调用。客户端不关注请求调用的结果，服务端收到请求后将请求排队，排队成功后请求就返回，服务端在空闲的情况下会逐个处理排队的请求。
后端超时	参考**表3-7**中的后端超时。
后端认证	参考**表3-7**中的后端认证。

表 3-9 Mock 类型定义后端服务

服务参数	参数说明
Mock返回结果	Mock一般用于开发调试验证。在项目初始阶段，后端服务没有搭建好API联调环境，可以使用Mock模式，将预期结果固定返回给API调用方，方便调用方进行项目开发。
后端认证	参考**表3-7**中的后端认证。

说明

- 如果“后端请求Path”中设置了环境变量，在API调试页面将无法调试API。
- 如果“后端请求Path”中设置了环境变量，则必须在待发布环境上配置变量名和变量值，否则变量无法赋值，API将无法正常调用。
- 环境变量名严格区分大小写。

步骤2 （可选）添加后端策略。

添加多个后端策略后，通过不同的策略条件，请求被转发到不同的后端服务中。

1. 单击“添加后端策略”。
2. 策略后端增加的参数，具体如表3-10所示，其他参数说明参见表3-7。

表 3-10 后端策略参数

信息项	描述
后端策略名称	您自定义的名称，用于识别不同的后端策略。
生效方式	- 满足任一条件：只要满足策略条件中的任意一项，此后端策略就可以生效。 - 满足全部条件：只有满足所有的策略条件，此后端策略才生效。
策略条件	使后端策略生效的条件，具体如表3-11所示。

表 3-11 策略条件

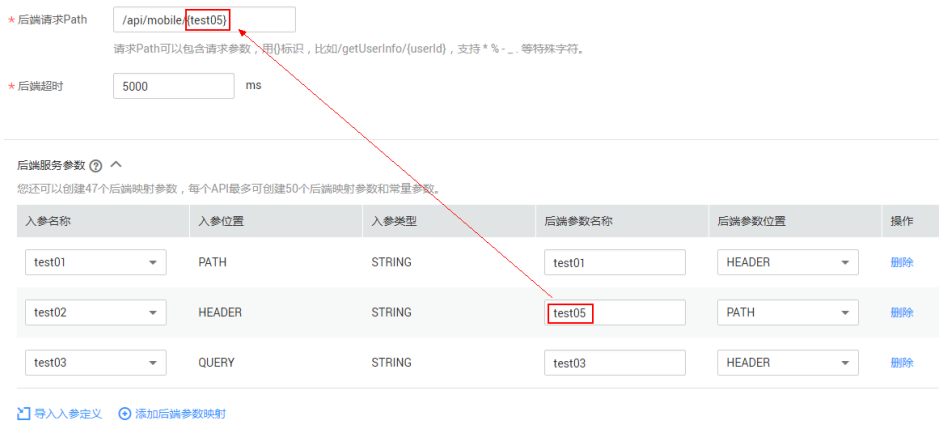
信息项	描述
条件来源	- 源地址：以访问API的请求地址作为策略条件来源。 - 请求入参：以请求入参参数作为策略条件来源。 **须知** 选择“请求入参”作为策略条件时，入参需要在API前端请求中配置好，如在Header中添加一个参数。
参数名称	- 当“条件来源”为“请求入参”时，需要设置。选择已创建的入参参数名称。
参数位置	仅在“条件来源”为“请求入参”时，展示请求入参的参数位置。
条件类型	仅在“条件来源”为“请求入参”时，需要设置。 - 相等：请求参数值必须为输入值时，条件成立。 - 枚举：请求参数值只需要和枚举值中任何一个值相同，条件成立。 - 匹配：请求参数值只需要和正则表达式中任何一个值相同，条件成立。
条件值	- “条件类型”为“相等”时，输入一个值。 - “条件类型”为“枚举”时，输入多个值，以英文逗号隔开。 - “条件类型”为“匹配”时，输入一个范围，例如：[0-5]。 - “条件来源”为“源地址”时，输入一个或多个IP地址，以英文逗号隔开。

步骤3 （可选）配置后端服务参数。

将调用API时传入的参数映射到后端服务对应的位置。

1. 在“后端服务参数”右侧单击，通过以下任意一种方法配置后端服务参数。
   - 单击“导入入参定义”，系统自动添加已创建的所有入参参数。
   - 单击“添加后端参数映射”，按照需求添加您所需要的后端参数映射。
2. 根据后端服务实际的参数名称和参数位置修改映射关系，如图3-1所示。

图 3-1 配置后端服务参数



   a. 参数在“PATH”位置，那么参数名称需要和“后端请求Path”中的名称相同。
   b. 调用API的请求参数名称、位置可以与后端参数名称、位置不同。

      说明

      - 参数名不能是x-apig- 、x-sdk-开头，不区分大小写。
      - 参数名不能是x-stage，不区分大小写。
      - 参数位置为HEADER时，参数名不区分大小写，也不支持下划线。

   c. 如上图，test01和test03在调用API时分别配置于PATH和QUERY位置，后端服务通过映射，将在HEADER位置接收test01和test03的值。test02在调用API时配置于HEADER位置，后端服务通过映射，将在PATH位置以参数名test05来接收test02的值。

      例如，test01为abc，test02为def，test03为xyz。

      调用API请求：

      ```
      curl -ik -H 'test02:def' -X GET https://www.example01.com/v1.0/abc?test03=xyz
      ```

      后端服务请求：

      ```
      curl -ik -H 'test01:abc' -H 'test03:xyz' -X GET https://www.example02.com/v1.0/def
      ```

步骤4 （可选）设置常量参数。

如果后端服务需要接收API调用者不可见的常量，可以通过设置常量参数来实现。API网关在请求后端服务时，将常量参数增加到指定请求位置，并将请求发送给后端服务。

1. 在“常量参数”右边单击，显示常量参数列表。
2. 单击“添加常量参数”，输入如表3-12所示信息。

表 3-12 常量参数

信息项	描述
常量参数名	常量参数的名称，如果参数在“PATH”位置，那么参数名称需要和“后端请求Path”中的名称相同。 **说明** – 参数名不能是x-apig- 、x-sdk-开头，不区分大小写。 – 参数名不能是x-stage，不区分大小写。 – 参数位置为HEADER时，参数名不区分大小写，也不支持下划线。
参数位置	选择参数在请求中的位置。 参数位置有如下三种：PATH、QUERY、HEADER
参数值	输入参数的值。
描述	对于此常量参数的描述。

说明

– API网关将包含常量参数的请求发送给后端服务前，会对特殊参数值进行百分号编码，请确保后端服务支持百分号编码。例如，参数值**[apig]**，在百分号编码后变为**%5Bapig%5D**。
– “PATH”位置的参数值会对如下字符进行百分号编码：ASCII码为0到31的字符、?、>、<、/、%、#、"、[、\、]、^、`、{、|、}、空白符、ASCII码为127到255的字符。
– “QUERY”位置的参数值会对如下字符进行百分号编码：ASCII码为0到31的字符、>、=、<、+、&、%、#、"、[、\、]、^、`、{、|、}、空白符、ASCII码为127到255的字符。

步骤5 （可选）设置系统参数。

系统参数指API网关服务处理API请求时的系统运行时参数信息，包括网关内置参数、前端认证参数、后端认证参数等，API的后端服务获取到这些信息，可以用于做一些辅助性的访问控制或提供自定义认证能力。

1. 在“系统参数”右边单击 ，显示系统参数列表。
2. 单击“添加系统参数”，输入如**表3-13**所示信息。

表 3-13 系统参数

信息项	描述
系统参数类型	– 网关内置参数：API网关支持配置的参数。 – 前端认证参数：前端自定义认证返回结果中的参数。在基本信息中，使用“自定义认证”后，才可以选择此参数类型。 – 后端认证参数：后端自定义认证返回结果中的参数。在定义后端服务中，开启“后端认证”后，才可以选择此参数类型。

信息项	描述
系统参数名称	– “系统参数类型”为“网关内置参数”时，支持选择如下参数：sourceIp（API调用的源地址）、stage（API调用的环境名称）、apiId（API调用的API ID）、appId（API调用的APP ID）、requestId（当次API调用生成的请求ID）。 – “系统参数类型”为“前端认证参数”/“后端认证参数”时，此参数名称必须和自定义认证函数返回结果中的参数名称一致。 自定义认证函数的编写以及返回结果参数的获取方法，请参考API网关开发指南。
后端参数名称	将系统参数映射到后端参数中。设置需要映射的后端参数名称。 **说明** – 参数名不能为x-apig- 、x-sdk-开头，不区分大小写。 – 参数名不能是x-stage，不区分大小写。 – 参数位置为HEADER时，参数名不支持下划线且名称重复时不区分大小写。
后端参数位置	设置需要映射的后端参数位置。
描述	对于此系统参数的描述。

步骤6 单击“下一步”，进入“返回结果基础定义”页面。

----结束

定义返回结果

步骤1 在“返回结果基础定义”页面，填写如**表3-14**所示信息。

表 3-14 定义返回结果

信息项	描述
成功响应示例	成功调用API时，返回的响应信息示例。
失败响应示例	调用API失败时，返回的响应信息示例。

步骤2 单击“完成”，完成API的创建。

API创建完成后，在API列表页面单击API名称，查看API详细信息。

----结束

后续操作

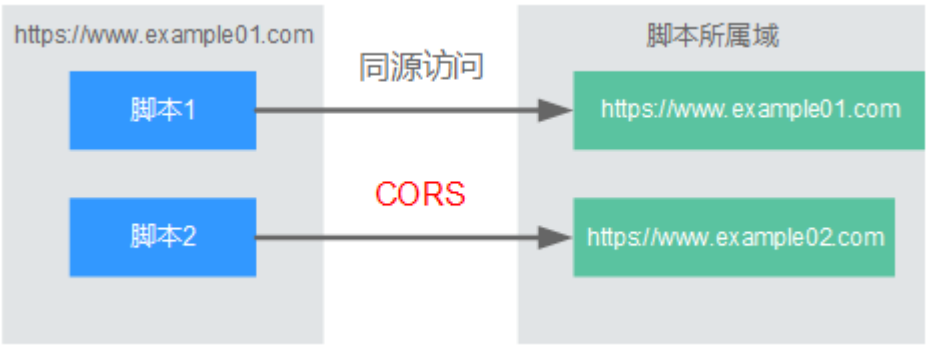
您创建完API后，通过**调试API**，验证服务是否正常。

3.2.2 开启跨域访问

什么是跨域访问

浏览器出于安全性考虑，会限制从页面脚本内发起的跨域访问（CORS）请求，此时页面只能访问同源的资源，而CORS允许浏览器向跨域服务器，发送XMLHttpRequest请求，从而实现跨域访问。

图 3-2 跨域访问



浏览器将CORS请求分为两类：

- **简单请求**

  简单跨域请求的场景需要满足以下两个条件：

  a. 请求方法是HEAD，GET，或者POST。

  b. HTTP的头信息不超出以下范围：

  - Accept
  - Accept-Language
  - Content-Language
  - Last-Event-ID
  - Content-Type：取值范围：application/x-www-form-urlencoded、multipart/form-data、text/plain

  对于简单请求，浏览器自动在头信息之中，添加一个Origin字段，Origin字段用于说明本次请求来自哪个源（协议+域名+端口）。服务器根据这个值，决定是否同意这次请求。服务器响应消息中包含“Access-Control-Allow-Origin”时，表示同意请求。

- **非简单请求**

  不满足简单请求两个条件的都为非简单请求。

  对于非简单请求，在正式通信之前，浏览器会增加一次HTTP查询请求，称为预检请求。浏览器询问服务器，当前页面所在的源是否在服务器的许可名单之中，以及可以使用哪些HTTP请求方法和头信息字段。预检通过后，浏览器向服务器发送简单请求。

开启跨域访问

API网关默认不开启跨域访问，如果您需要开启，请参考以下说明完成跨域配置。

- **简单请求的跨域访问**

  如果是创建新的API，在定义API请求时，打开“支持跨域（CORS）”开关。详细的使用指导，可参考**简单请求**。

- **非简单请求的跨域访问**

  须知

  非简单请求的跨域访问需要在API的分组中**创建一个“Method”为“OPTIONS”的API，作为预检请求**。

  预检请求API的参数设置，请参考以下说明填写。详细的使用指导可参考**非简单请求**。

  a. 在API的基本信息中，安全认证选“无认证”。

  b. 定义API请求时，参数填写说明如下：

     - 请求协议：选择与已开启CORS的API相同的请求协议
     - 请求Path：填斜杠/
     - Method：选择“OPTIONS”
     - 支持CORS：选择开启CORS

  c. 后端服务选择Mock。

简单请求

对于简单请求，您需要**开启简单跨域访问**。

场景一：已开启CORS，且后端服务响应消息中未指定跨域头时，API网关接受任意域的请求，并返回“Access-Control-Allow-Origin”跨域头，示例如下：

浏览器发送一个带Origin字段的请求消息：

```
GET /simple HTTP/1.1
Host: www.test.com
Orgin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin：此字段必选，表示请求消息所属源，上例中请求来源于“http://www.cors.com”，API网关/后端服务根据这个值，决定是否同意本次请求。

后端服务返回响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

API网关响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

Access-Control-Allow-Origin：此字段必选，“*”表示API网关接受任意域的请求。

场景二：已开启CORS，且后端服务响应消息中指定跨域头时，后端服务响应的跨域头将覆盖API网关增加的跨域头，示例如下：

浏览器发送一个带Origin字段的请求消息：

```
GET /simple HTTP/1.1
Host: www.test.com
Orgin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

Origin：此字段必选，表示请求消息所属源，上例中请求来源于“http://www.cors.com”，API网关/后端服务根据这个值，决定是否同意本次请求。

后端服务返回响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

Access-Control-Allow-Origin：表示后端服务接受“http://www.cors.com”的请求。

API网关响应消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: http://www.cors.com

{"status":"200"}
```

后端服务响应消息中的跨域头覆盖API网关响应消息中的跨域头。

非简单请求

对于非简单请求，您需要**开启跨域访问**，并且创建一个“Method”为“OPTIONS”的API。

“Method”为“OPTIONS”的API和普通API的区别如下：

- 所属分组：选择已开启CORS的API所在的分组。
- 安全认证：可选择“无认证”。无论选择哪种认证方式，API网关都按照无认证处理。

- 请求协议：选择与已开启CORS的API相同的请求协议。
- 请求Path：填斜杠/即可，也可选择与已开启CORS的API相同或者匹配的请求Path。
- Method：选择“OPTIONS”。
- 支持CORS：选择开启CORS。

假设后端服务类型为Mock，示例如下：

浏览器发送“Method”为“OPTIONS”的API请求：

```
OPTIONS /HTTP/1.1
User-Agent: curl/7.29.0
Host: localhost
Accept: */*
Origin: http://www.cors.com
Access-Control-Request-Method: PUT
Access-Control-Request-Headers: X-Sdk-Date
```

- Origin：此字段必选，表示请求消息所属源。
- Access-Control-Request-Method：此字段必选，表示请求会使用哪些HTTP请求方法。
- Access-Control-Request-Headers：此字段可选，表示请求会额外发送的头信息字段。

后端服务返回消息：无

API网关返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 02:38:48 GMT
Content-Type: application/json
Content-Length: 1036
Server: api-gateway
X-Request-Id: c9b8926888c356d6a9581c5c10bb4d11
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: X-Stage,X-Sdk-Date,X-Sdk-Nonce,X-Proxy-Signed-Headers,X-Sdk-Content-Sha256,X-Forwarded-For,Authorization,Content-Type,Accept,Accept-Ranges,Cache-Control,Range
Access-Control-Expose-Headers: X-Request-Id,X-Apig-Latency,X-Apig-Upstream-Latency,X-Apig-RateLimit-Api,X-Apig-RateLimit-User,X-Apig-RateLimit-App,X-Apig-RateLimit-Ip,X-Apig-RateLimit-Api-Allenv
Access-Control-Allow-Methods: GET,POST,PUT,DELETE,HEAD,OPTIONS,PATCH
Access-Control-Max-Age: 172800
```

- Access-Control-Allow-Origin：此字段必选，“*”表示API网关接受任意域的请求。
- Access-Control-Allow-Headers：当请求消息中包含此字段时，此字段必选。表示允许跨域的所有请求头信息字段。
- Access-Control-Expose-Headers：表示跨域访问允许查看的返回头信息字段。
- Access-Control-Allow-Methods：此字段必选，表示API网关支持的所有HTTP请求方法。
- Access-Control-Max-Age：此字段可选，表示本次预检的有效期，单位：秒。在有效期内，无需再次发出预检请求。

浏览器发送一个带Origin字段的请求头：

```
PUT /simple HTTP/1.1
Host: www.test.com
Orgin: http://www.cors.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept: application/json
Date: Tue, 15 Jan 2019 01:25:52 GMT
```

后端服务返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway

{"status":"200"}
```

API网关返回消息：

```
HTTP/1.1 200 OK
Date: Tue, 15 Jan 2019 01:25:52 GMT
Content-Type: application/json
Content-Length: 16
Server: api-gateway
X-Request-Id: 454d689fa69847610b3ca486458fb08b
Access-Control-Allow-Origin: *

{"status":"200"}
```

3.2.3 调试 API

操作场景

API创建后需要验证服务是否正常，管理控制台提供调试功能，您可以添加HTTP头部参数与body体参数，调试API接口。

说明

- 后端路径中含有环境变量的API，不支持调试。
- 如果API已绑定流控策略，在调试API时，流控策略无效。

前提条件

- 已创建API分组和分组内的API。
- 已搭建完成后端服务。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 通过以下任意一种方法，进入API调试页面。

- 在待调试的API所在行，单击“更多 > 调试”。
- 单击“*API名称*”，进入API详情页面。在右上角单击“调试”。

左侧为API请求参数配置区域，参数说明如表3-15所示。右侧为API发送的请求信息和API请求调用后的返回结果回显。

表 3-15 调试 API

参数名称	说明
协议	仅在API请求的“请求协议”为“HTTP&HTTPS”时，支持修改。
方法	仅在API请求的“Method”定义为“ANY”时，支持修改。
后缀	仅在API请求的“匹配模式”为“前缀模式”时，支持自定义路径。
路径	API的请求path。
路径参数	仅在API请求的“请求Path”中存在“{}”时，支持修改。
请求头	HTTP Headers的参数与参数值。
查询参数	Query的参数与参数值。
请求体	仅在API请求的“Method”定义为“PATCH”/“POST”/“PUT”时，支持修改。

说明

不同类型的请求，调试界面展现的信息项有差异。

步骤5 添加请求参数后，单击“发送请求”。

右侧返回结果回显区域打印API调用的Response信息。

- 调用成功时，返回HTTP状态码为“200”和Response信息。
- 调试失败时，返回HTTP状态码为4*xx*或5*xx*，具体错误信息请参见**错误码**。

步骤6 您可以通过调整请求参数与参数值，发送不同的请求，验证API服务。

说明

如果需要修改API参数，请在右上角单击“编辑”，进入API编辑页面。

----结束

后续操作

API调试成功后，您可以将API**发布到环境**，以便API调用者调用。或者出于API的安全性考虑，为API**创建流控策略**、**创建访问控制策略**和**创建并使用签名密钥**。

3.2.4 授权 API

操作场景

API在创建后，通过指定授权给某些应用，让指定应用能够调用API。

说明

- 仅在API发布到环境后，才支持被调用。
- 仅在API为APP认证时，才支持授权给应用。

前提条件

- 已创建API分组和分组内的API。
- （可选）已创建环境。
- 已创建应用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 通过以下任意一种方法，进入“授权应用”页面。

- 在待授权的API所在行，单击“授权”，进入“授权API”页面。单击“添加应用”，弹出“授权应用”对话框。
- 勾选待授权的API，单击“授权”，进入“授权API”页面。单击“添加应用”，弹出“授权应用”对话框。
- 通过API详情页面进入，步骤如下：
  a. 单击待授权的API名称，进入API详情页面。
  b. 单击“授权信息”，进入“授权信息”页签。
  c. 单击“添加授权”，弹出“授权应用”对话框。

说明

如果需要批量将多个API授权同一个应用，则勾选待授权的API，单击“授权”，进入“授权API”页面。单击“添加应用”，弹出“授权应用”对话框。最多同时授权1000个API。

步骤5 选择API授权环境，查询并勾选应用后，单击“授权”。

步骤6 授权成功后，可以在“授权信息”/“授权API”中查看已授权的应用。

说明

如果已授权的应用列表中包含无需授权的应用，在此应用所在行单击“解除授权”，将无需授权的应用删除。

----结束

后续操作

您将API授权给指定应用后，可以通过不同语言的SDK调用此API。

3.2.5 发布 API

操作场景

创建完成的API，支持发布到不同的环境。API只有在发布到环境后，才支持被调用。API网关支持查看API发布历史（如版本、发布说明、发布时间和发布环境），并支持回滚到不同的API历史版本。

说明

- 已发布的API，在修改信息后，需要重新发布才能将修改后的信息同步到环境中。
- 同一个API在每个环境中最多记录10条最新的发布历史。

前提条件

- 已创建API分组和分组内的API。
- 已创建环境。

发布 API

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 通过以下任意一种方法，进入“发布API”页面。

- 在待发布的API所在行，单击“发布”。
- 单击“*API名称*”，进入API详情页面。在右上角单击“发布”。

说明

如果需要批量发布API，则勾选待发布的API，单击“发布”。最多同时发布1000个API。

步骤5 选择API需要发布到的环境，并填写发布说明。

说明

- 如果API在选择的环境中已发布，再次发布即为覆盖该环境的API。
- 如果在选择的环境时没有自己需要的环境，可以创建一个自己需要的环境。

步骤6 单击“发布”，完成API发布。

----结束

查看发布历史

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 单击待查看发布历史的API名称，进入API详情页面。

步骤5 单击“发布历史”，进入“发布历史”页签。

查看API的发布历史信息。

步骤6 在版本所在行，单击“查看版本”，弹出此版本详细信息对话框。

查看API基本信息、API请求、后端请求、入参定义、参数映射、常量参数和返回结果。

步骤7 如果想要设置之前版本为当前版本，则在版本所在行，单击“切换至此版本”，弹出“切换至此版本”对话框。

单击“确定”，完成版本的切换。此时版本号旁边显示“当前版本”，说明设置成功。

API调用者调用此API时，API参数为“当前版本”设置的参数，不是最后一次编辑保存的API参数。

例如，2018年8月1日发布在RELEASE环境的API匹配模式设置为“绝对匹配”，2018年8月20日修改API匹配模式设置为“前缀匹配”，并发布到RELEASE环境。然后设置2018年8月1日发布的版本为当前版本，此时API调用者调用此API时，API的匹配模式为“绝对匹配”。

----结束

3.2.6 下线 API

操作场景

已发布的API因为其他原因需要暂停对外提供服务，可以暂时将API从相关环境中下线。

须知

该操作将导致此API在指定的环境无法被访问，请确保已经告知使用此API的用户。

前提条件

- 已创建API分组和分组内的API。
- API已发布到该环境。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 通过以下任意一种方法，下线API。

- 在待下线的API所在行，单击“更多 > 下线”，弹出“下线API”对话框。

- 单击“*API名称*”，进入API详情页面。在右上角单击“下线”，弹出“下线API”对话框。

说明

如果需要批量下线API，则勾选待下线的API，单击“下线”。最多同时下线1000个API。

步骤5 选择API需要下线的环境，单击“确定”，完成API下线。

----结束

后续操作

您将API下线后，可以通过**删除API**，释放此API所占用的资源。

3.2.7 删除 API

操作场景

已发布的API不再提供服务，可以将API删除。

须知

- 该操作将导致此API无法被访问，可能会影响正在使用此API的应用或者用户，请确保已经告知用户。
- 已发布的API，需要先下线API，再删除。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 通过以下任意一种方法，弹出“删除API”对话框。

- 在待删除的API所在行，单击“更多 > 删除”。
- 单击“*API名称*”，进入API详情页面。在右上角单击“删除”。

说明

如果需要批量删除API，则勾选待删除的API，单击“删除”。最多同时删除1000个API。

步骤5 按照提示，在输入框中输入“DELETE”，单击“确定”，完成API删除。

----结束

3.2.8 导入 API

操作场景

Swagger是基于OpenAPI规范构建的开源工具，可以帮助您设计、构建、记录以及使用Rest API。API网关支持导入Swagger 2.0定义的API到已有的API分组或新的API分组。

导入API支持单个API导入和批量API导入，主要取决于Swagger文件中包含的API数量。

前提条件

- 已获取待导入API的Swagger文件，导入前您需要在API定义中补全API网关的。
- API分组和API的配额满足需求。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 单击“导入API”，进入“导入API”界面。

步骤5 选择如表3-16所示参数。

表 3-16 导入 API

参数名称	说明
导入方式	导入方式包含以下2种： • 导入到新的分组：将API定义导入到一个新的分组，导入过程中系统会自动创建一个新的API分组，并将导入的API归属到该分组。 • 导入到已有分组：将API定义导入到一个已有的分组，导入过程中不会删除分组中已有的API，只是将新增的API导入分组。
API分组	仅在选择“导入到已有分组”时，需要选择API分组。
是否覆盖	勾选后，当导入的API名称与已有的API名称冲突时，导入的API会覆盖已有的API。 仅在选择“导入到已有分组”时，需要选择是否覆盖。
扩展覆盖	当导入API扩展信息（ACL，流控）与已有的API扩展信息冲突时，会覆盖已有API扩展信息。

步骤6 单击“导入参数”下方的“文件”，选择待导入的API文件。

支持yaml和json两种文件格式的API导入，界面可预览待导入API内容。

步骤7 （可选）修改待导入API的全局配置。

您可以修改全局配置，如前后端的请求配置，也可以修改具体的接口配置。

步骤8 单击“快速上线”，完成API导入。

说明

导入的API不会自动发布到环境，需要您手动发布。

----结束

后续操作

将导入成功的API**发布到环境**中，以便API调用者调用。

3.2.9 导出 API

操作场景

导出JSON或YAML格式的API。API网关支持单个API导出和批量API导出。

前提条件

已创建API分组和API。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“导出API”，进入“导出API”界面。

步骤4 设置如**表3-17**所示参数。

表 3-17 导出 API

参数名称	说明
API分组	选择待导出API所在的API分组。
运行环境	选择待导出API所在的环境。
API	默认导出API分组所在环境的所有的API，如果需要导出个别API，单击“自定义导出API”，勾选需要导出的API名称。

参数名称	说明
API定义范围	• 基础定义：包括API前端请求定义和响应定义，不包括后端服务定义。其中API前端请求定义除了Swagger规范定义项外，还包括API网关的一些Swagger扩展字段。 • 全量定义：包括API前端请求定义、后端服务定义和响应定义。 • 扩展定义：包括API前端请求定义、后端服务定义和响应定义，还包括API关联的流量控制、访问控制等策略对象的定义。
导出格式	选择JSON或YAML。
自定义版本	为导出的API自定义版本号，如果没有指定版本号，默认使用当前时间。

步骤5 单击“导出”，右侧显示导出结果。

----结束

3.3 流量控制

3.3.1 创建流控策略

操作场景

流量控制可限制单位时间内API的被调用次数，保护后端服务。

为了提供持续稳定的服务，您可以通过创建流控策略，针对部分API进行流量控制。

流控策略和API本身是相互独立的，只有将流控策略绑定API后，流控策略才对绑定的API生效。

说明

- 每个用户最多可创建30个流控策略。
- 同一个环境中，一个API只能被一个流控策略绑定，但一个流控策略可以绑定多个API。
- 若API未绑定流控策略，则系统默认流控限制为200次/秒。

前提条件

需要绑定的**API已发布**。

创建流控策略

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤4 单击“创建流控策略”，弹出“创建流控策略”对话框。输入如**表3-18**所示信息。

表 3-18 流控策略信息

信息项	描述
策略名称	API流控策略名称。
类型	分“基础流控”和“共享流控”两类。 ● 基础流控针对单个API进行流量统计和控制； ● 共享流控针对绑定了该策略的所有API进行总流量统计和控制。
时长	流量限制的时长。 ● 与“API流量限制”配合使用，表示单位时间内的单个API请求次数上限。 ● 与“用户流量限制”配合使用，表示单位时间内的单个用户请求次数上限。 ● 与“应用流量限制”配合使用，表示单位时间内的单个APP请求次数上限。 ● 与“源IP流量限制”配合使用，表示单位时间内的单个IP地址请求次数上限。
API流量限制	单个API被调用次数上限。 与“时长”配合使用，表示单位时间内的单个API请求次数上限。
用户流量限制	单个用户调用API次数上限，**仅适用于API的安全认证方式为IAM认证时**。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个用户请求次数上限。 ● 如果主帐号下有多个子用户访问API，按主帐号累计的调用次数进行限制。
应用流量限制	单个应用调用API次数上限，**仅适用于API的安全认证方式为APP认证时**。 ● 不超过“用户流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个应用请求次数上限。
源IP流量限制	单个IP地址调用API次数上限。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个IP地址请求次数上限。
描述	关于控制策略的描述。

步骤5 单击“确定”，完成流量控制策略的创建。

创建成功后，流量控制页面增加显示新创建的策略。您可以将相关API绑定到该策略，以实现流量控制。

----结束

绑定 API

步骤1 在“流量控制”页面，通过以下任意一种方法，进入“绑定API”页面。

- 在待绑定的流量控制策略所在行，单击“绑定API”，进入已绑定API列表页面。单击“绑定API”。
- 单击策略名称，进入策略详情页面。在“绑定的API列表”页签中单击“绑定API”。

步骤2 选择“API分组”、“环境”以及“API名称”，筛选所需的API。

步骤3 勾选API，单击“绑定”，完成API绑定策略。

说明

在流控策略绑定API后，如果API不需要调用此策略，单击“解除”，解除绑定。如果需要批量解绑API，则勾选待解绑的API，单击“解除”。最多同时解绑1000个API。

----结束

后续操作

- 如果某个应用希望受流量策略控制，可以通过对该策略增加特殊应用实现，具体参考**添加特殊应用或租户**。增加特殊应用后，此应用的应用流量限制受增加特殊应用时设置的阈值限制，API流量限制和用户流量限制受策略限制。
- 如果某个租户希望受流量策略控制，可以通过对该策略增加特殊租户实现，具体参考**添加特殊应用或租户**。增加特殊租户后，此租户的用户流量限制受增加特殊租户时设置的阈值限制，API流量限制和应用流量限制受策略限制。

3.3.2 删除流控策略

操作场景

当已创建的流控策略不再提供服务时，可以将此流控策略删除。

前提条件

已创建流控策略。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤4 通过以下任意一种方式，弹出“删除流控策略”对话框。

- 在待删除的流控策略所在行，单击“删除”。

- 单击待删除的策略名称，进入流量控制详情页面，在右上角单击“删除”。

说明

- 仅在流控策略未绑定任何API时，支持删除，否则请先解绑API。在流量控制详情页面，单击待解绑API所在行的“解除”。
- 如果需要批量删除流控策略，则勾选待删除的流控策略，单击“删除”。最多同时删除1000个流控策略。

步骤5 单击“确定”，完成流控策略的删除。

----结束

3.3.3 添加特殊应用或租户

操作场景

如果需要为某个应用/租户设置特定的流控值，则通过添加特殊应用/租户可以实现。

前提条件

已创建应用，或已获取其他应用ID/租户ID。

添加特殊应用

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤4 单击待添加特殊应用的流控策略的名称，进入流控详情页面。

步骤5 单击“特殊应用”，进入特殊应用页面。

步骤6 单击“添加特殊应用”，弹出“添加特殊应用”对话框。

步骤7 通过以下两种方式，添加特殊应用。

- 添加已有应用：单击“已有应用”，选择已有应用，输入阈值。
- 添加其他应用：单击“其他”，输入其他用户的应用ID和阈值。

说明

阈值不超过API流量限制值，且必须为正整数。

----结束

添加特殊租户

步骤1 登录管理控制台。

步骤2 鼠标移动到已登录用户名，在下拉列表中单击“我的凭证”。

步骤3 在“我的凭证”页面查看帐号ID和项目ID。

步骤4 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤5 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤6 单击待添加特殊租户的流控策略的名称，进入流控详情页面。

步骤7 单击“特殊租户”，进入特殊租户页面。

步骤8 单击“添加特殊租户”，弹出“添加特殊租户”对话框。

步骤9 输入如表3-19所示信息。

表 3-19 特殊租户信息

信息项	描述
租户ID	步骤3中获取的帐号ID或项目ID。 ● 绑定APP认证的API时，租户ID为项目ID。 ● 绑定IAM认证的API时，租户ID为帐号ID，不支持细分到IAM用户维度。
阈值	固定时间段内，此租户访问API的最大值。 不能超过API流量限制值。

步骤10 单击“确定”，完成特殊租户的添加。

说明

特殊租户流控值和用户流量限制值共同作用时，以特殊租户流控值为准。

例如：API流量限制值为10，用户流量限制值为3，时长为1分钟，特殊租户（租户ID为A）流控值为2，特殊租户（租户ID为B）流控值为4，租户A在1分钟内最多可以访问绑定了该流控策略的API 2次，租户B在1分钟内最多可以访问绑定了该流控策略的API 4次。

----结束

3.3.4 删除特殊应用或租户

操作场景

在特殊应用/租户没有作用之后，删除为流控策略添加的特殊应用/租户。本节以删除特殊应用为例。

前提条件

- 已创建流控策略。
- 已添加特殊应用/租户。

删除特殊应用

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤4 单击待删除特殊应用的流量控制策略的名称，进入流量控制详情页面。

步骤5 单击“特殊应用”，进入“特殊应用”页面。

步骤6 在待删除的特殊应用所在行，单击“删除”，弹出“删除特殊应用”对话框。

步骤7 单击“确定”，完成对特殊应用的删除。

----结束

删除特殊租户

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤4 单击待删除特殊租户的流量控制策略的名称，进入流量控制详情页面。

步骤5 单击“特殊租户”，进入“特殊租户”页面。

步骤6 在待删除的特殊租户所在行，单击“删除”，弹出“删除特殊租户”对话框。

步骤7 单击“确定”，完成对特殊租户的删除。

----结束

3.4 访问控制

3.4.1 创建访问控制策略

操作场景

访问控制策略是API网关提供的API安全防护组件之一，主要用来控制访问API的IP地址和帐户，您可以通过设置IP地址或帐户的黑白名单来拒绝/允许某个IP地址或帐户访问API。

访问控制策略和API本身是相互独立的，只有将访问控制策略绑定API后，访问控制策略才对绑定的API生效。

说明

- 每个用户最多可以创建100个访问控制策略。
- 同一个环境中一个API只能被一个访问控制策略绑定，一个访问控制策略可以绑定多个API。

创建访问控制策略

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 访问控制”，进入访问控制策略列表页面。

步骤4 单击“创建访问控制策略”，弹出“创建访问控制策略”对话框。

步骤5 输入表3-20如所示信息。

表 3-20 访问控制策略信息

信息项	描述
策略名称	访问控制策略的名称。
限制类型	控制访问API的类型。 ● IP地址：允许/禁止访问API的IP地址。 ● 帐号名：允许/禁止访问API的帐号名。
动作	包括“允许”和“禁止”。 和“限制类型”配合使用，允许/禁止访问API的IP地址/帐号名。
IP地址	输入需要允许或者禁止访问API的IP地址，或IP地址范围。 仅在“限制类型”为“IP地址”时，需要设置。 **说明** 允许或禁止访问的IP地址条数，分别可以配置最多100条。
帐号名	输入需要允许或者禁止访问API的IAM帐号，**仅适用于API的安全认证方式为IAM认证时**。 仅在“限制类型”为“帐号名”时，需要设置。支持输入多个账户名，以英文“,”隔开，如aaa,bbb。 **说明** 仅支持IAM帐号维度的访问控制，不能对单个IAM用户进行访问控制。

步骤6 单击“确定”，完成访问控制策略的创建。您可以将相关API绑定到该策略，以实现访问控制。

----结束

绑定 API

步骤1 在“访问控制”页面，通过以下任意一种方法，进入“绑定API”页面。

- 在待绑定的访问控制策略所在行，单击“绑定API”，进入已绑定API列表页面。单击“绑定API”。
- 单击策略名称，进入策略详情页面。单击“绑定API”。

步骤2 选择“API分组”、“环境”以及“API名称”，筛选所需的API。

步骤3 勾选API，单击“绑定”，完成API绑定策略。

说明

在访问控制策略绑定API后，如果API不需要调用此策略，单击“解除”，解除绑定。如果需要批量解绑API，则勾选待解绑的API，单击“解除”。最多同时解绑1000个API。

----结束

3.4.2 删除访问控制策略

操作场景

当已创建的访问控制策略不再需要时，可以将此访问控制策略删除。

前提条件

已创建访问控制策略。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 访问控制”，进入访问控制策略列表页面。

步骤4 通过以下任意一种方式，弹出“删除访问控制策略”对话框。

- 在待删除的访问控制策略所在行，单击“删除”。
- 单击待删除的访问控制策略名称，进入访问控制详情页面，在右上角单击“删除”。

说明

- 仅在访问控制策略未绑定任何API时，支持删除，否则请先解绑API。
- 如果需要批量删除访问控制策略，则勾选待删除的访问控制策略，单击“删除”。最多同时删除1000个访问控制策略。

步骤5 单击“确定”，完成访问控制策略的删除。

----结束

3.5 环境管理

3.5.1 创建环境和环境变量

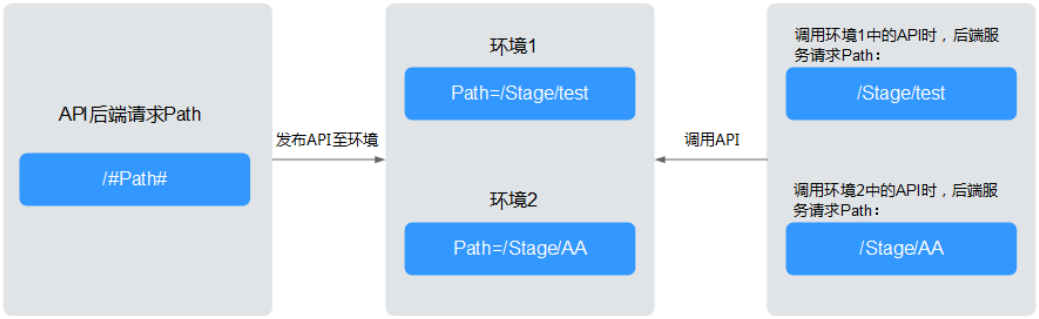
操作场景

API可以同时提供给不同的环境调用，如生产、测试或开发。RELEASE是默认存在的环境，无需创建。且API网关提供环境变量功能，通过创建环境变量，实现在不同的环境定义不同的API调用路径。

环境变量是指在环境上创建可管理的一种变量，该变量固定在环境上。通过创建环境变量，实现同一个API，在不同环境中调用不同的后端服务。

当创建API时定义了变量标识，则需要在环境中添加变量。例如创建API时定义了变量名为“Path”，在环境1中创建了变量名“Path”，变量值“/Stage/test”，则API在发布到环境1时，使用“/Stage/test”代替“Path”，API调用者在环境1中调用此API时，后端服务请求Path为“/Stage/test”。在环境2中创建了变量名“Path”，变量值“/Stage/AA”，则API在发布到环境2时，使用“/Stage/AA”代替“Path”，API调用者在环境2中调用此API时，后端服务请求Path为“/Stage/AA”。

图 3-3 环境变量示意



说明

- 每个用户最多创建10个环境。
- 每个分组在任意一个环境中，最多创建50个变量。

前提条件

已**创建API分组**。

创建环境

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 环境管理”，进入到环境管理信息页面。

步骤4 单击“创建环境”，弹出“创建环境”对话框。填写如**表3-21**所示信息。

表 3-21 环境信息

信息项	描述
环境名称	API环境名称。
描述	环境描述信息。

步骤5 单击“确定”，创建环境。

创建环境成功后，在“环境管理”页面的列表中显示新创建的环境。

----结束

访问环境

通过RESTful API可以访问API默认的RELEASE环境，如果访问其他环境，需要在请求头中添加X-Stage头，内容为环境名。例如访问名为“DEVELOP”的环境，则添加“X-Stage:DEVELOP”。

说明

API网关管理控制台的“调试”功能，固定为调试环境，不支持携带环境变量调试。

创建环境变量

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > API分组”，进入到API分组信息页面。

步骤4 通过以下任意一种方式，进入“变量管理”页签。

- 单击待操作的分组名称，进入分组详细信息页面。单击“变量管理”。
- 在待创建环境变量的分组所在行，单击“更多 > 变量管理”。

步骤5 在“环境”中选择待添加变量的环境名称，单击“添加变量”，弹出“新增变量”对话框。

步骤6 填写如表3-22所示信息。

表 3-22 新增变量

信息项	描述
变量名称	变量的名称，必须与创建API时定义的变量标识完全相同。
变量值	变量路径。

步骤7 单击“确定”，完成变量的添加。

说明

如果不再需要此变量时，在变量所在行单击“删除”。

在实际发送API请求中，环境变量名称与变量值会明文传递，请勿携带隐私信息。

----结束

后续操作

创建完环境和环境变量后，您可以将API发布到环境，以便API调用者调用。

3.5.2 删除环境

操作场景

已创建的环境不再提供服务，可以将环境删除。

前提条件

已创建环境。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“开放API > 环境管理”，进入到环境管理信息页面。

步骤4 在待删除的环境所在行，单击“删除”，弹出“删除环境”对话框。

说明

仅在环境未被API发布时，支持删除。

步骤5 单击“确定”，完成环境管理信息。

----结束

3.6 签名密钥

3.6.1 创建并使用签名密钥

操作场景

签名密钥用于后端服务验证API网关的身份，在API网关请求后端服务时，保障后端服务的安全。

签名密钥是由一对Key和Secret组成，签名密钥需要绑定到API才能生效。当签名密钥绑定API后，API网关向后端服务发送此API的请求时，会增加相应的签名信息，此时需要后端服务依照同样方式进行签名，通过比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

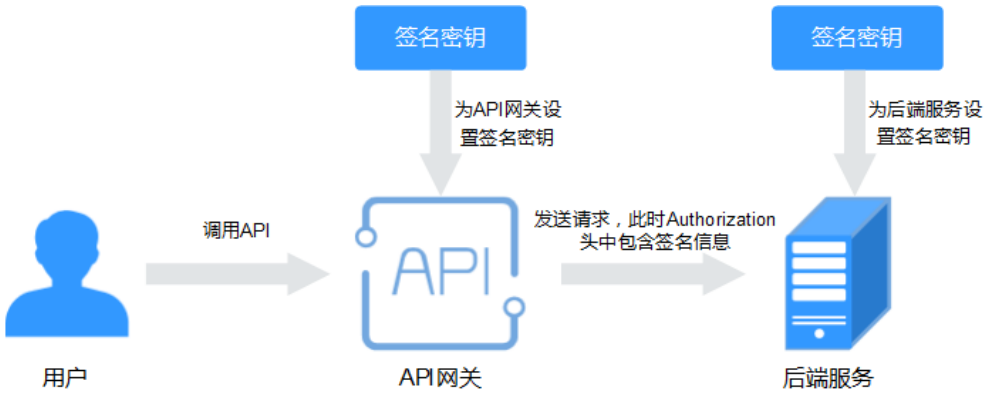
说明

- 每个用户最多创建30个签名密钥。
- 同一个环境中一个API只能被一个签名密钥绑定，一个签名密钥可以绑定多个API。

使用流程

1. 在控制台创建签名密钥。
2. 将新创建的签名密钥绑定API。
3. API网关将签名后的请求发送到后端服务，此时Authorization头中包含签名信息。后端服务通过不同的开发语言（例如Java、Go、Python、JavaScript、C#、PHP、C++、C、Android等）进行签名，比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

图 3-4 签名密钥流程图



创建签名密钥

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > 签名密钥”，进入签名密钥管理信息页面。

步骤4 单击“创建密钥”，弹出“创建密钥”对话框。

步骤5 填写如表3-23所示信息。

表 3-23 密钥信息

信息项	描述
密钥名称	自定义名称，用于识别不同的密钥。
Key	与“Secret”配合使用，表示签名密钥对。
Secret	与“Key”配合使用，表示签名密钥对。
确认Secret	填写与Secret一致的值。

步骤6 单击“确定”，完成密钥的创建。

----结束

绑定 API

步骤1 单击“开放API > 签名密钥”，进入签名密钥管理信息页面。

步骤2 通过以下任意一种方法，查看签名密钥已绑定API列表页面。

- 在待绑定API的密钥所在行，单击“绑定API”，进入“签名密钥绑定API”页面。
- 单击待绑定API的密钥名称，进入密钥详情页面。

步骤3 单击“绑定API”，弹出“绑定API”对话框。

步骤4 选择“API分组”、“环境”以及“API名称”，筛选所需的API。

步骤5 勾选API，单击“绑定”，完成密钥绑定API。

说明

在签名密钥绑定API后，如果API不再需要此密钥，单击“解除”，解除绑定。

----结束

验证签名结果

参考《开发指南》的“对后端服务进行签名”章节对后端服务进行签名，比对签名结果和API网关传过来的Authorization头中签名是否一致来校验API的合法性。

3.6.2 删除签名密钥

操作场景

如果某一个密钥不再提供服务，则可以将其删除。

前提条件

已创建密钥。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > 签名密钥”，进入签名密钥管理信息页面。

步骤4 通过以下任意一种方法，弹出“删除密钥”对话框。

- 在待删除的密钥所在行，单击“删除”。
- 单击“*密钥名称*”，进入签名密钥详情页面。在右上角单击“删除”。

说明

仅在签名密钥未绑定任何API时，支持删除，否则请先解绑API。

步骤5 单击“确定”，完成密钥的删除。

----结束

3.7 VPC 通道

3.7.1 创建 VPC 通道

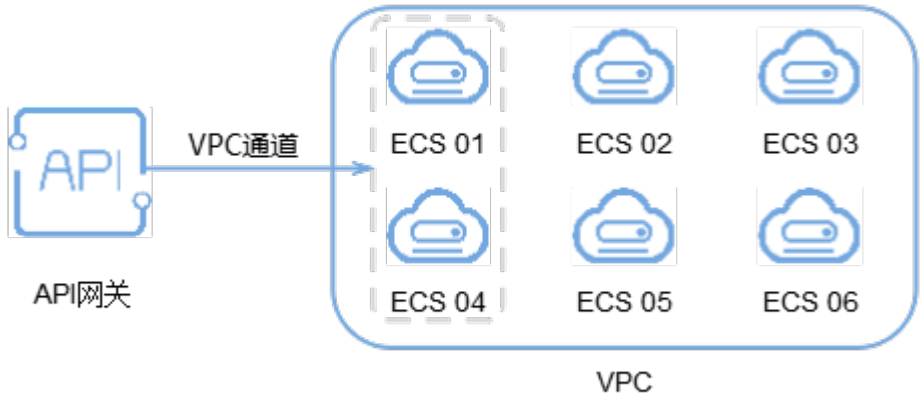
操作场景

VPC通道主要用于将部署在VPC内的服务通过API网关开放给外部访问，它的优势在于使用VPC的内部子网通信，网络时延更低，同时VPC通道具有负载均衡功能，从而实现后端服务的负载均衡。

创建VPC通道后，在创建API，且后端服务类型为HTTP/HTTPS时，后端服务地址可以直接使用已创建的VPC通道。每个用户最多创建30个VPC通道。

例如，VPC中包含6台ECS，已创建一条VPC通道，其中ECS 01和ECS 04已添加到VPC通道中，此时API网关通过VPC通道可以直接访问VPC中的ECS 01和ECS 04。

图 3-5 通过 API 网关访问 VPC 通道中的 ECS



前提条件

已创建云服务器。

创建快速通道

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤4 单击“创建快速通道”，进入“新建VPC通道”页面，填写如表3-24所示信息。

表 3-24 VPC 通道配置

信息项	描述
通道名称	自定义VPC通道名称，用于识别不同的VPC通道。
端口	VPC通道中主机的端口号，即用户的后端业务端口号。 取值为1 ~ 65535。

信息项	描述
分发算法	通过分发算法确定请求被发送到哪台主机。 分发算法包含如下几种： ● 加权轮询 ● 加权最少连接 ● 源地址哈希 ● URI哈希
协议	使用以下协议，对VPC中主机执行健康检查。 ● TCP ● HTTP ● HTTPS 默认为TCP协议。
路径	健康检查时的目标路径。 仅在协议不为“TCP”时，需要设置。
检查端口	健康检查的目标端口。 缺省时为VPC中主机的端口号。
正常阈值	判定VPC通道中主机正常的依据为：连续检查*x*成功，x为您设置的正常阈值。 取值为2 ~ 10。缺省时为2。
异常阈值	判定VPC通道中主机异常的依据为：连续检查*x失败*，x为您设置的异常阈值。 取值为2 ~ 10。缺省时为5。
超时时间	检查期间，无响应的时间，单位为秒。 取值为2 ~ 30。缺省时为5。
间隔时间	连续两次检查的间隔时间，单位为秒。 取值为5 ~ 300。缺省时为10。
HTTP响应码	检查目标HTTP响应时，判断成功使用的HTTP响应码。 仅在协议不为“TCP”时，需要设置。

步骤5 单击“下一步”，进入“添加云服务器”页面。

步骤6 单击“添加云服务器”，弹出“添加云服务器”对话框。

步骤7 勾选需要添加的云服务器，单击“添加”。

说明

待添加的云服务器的安全组必须允许100.125.0.0/16网段访问，否则将导致健康检查失败及业务不通。

步骤8 单击“完成”，完成快速通道的创建。

----结束

创建私网 ELB 通道

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤4 单击“创建私网ELB通道”，弹出“创建私网ELB通道”对话框。

步骤5 输入通道名称，选择ELB实例，单击“确定”，完成私网ELB通道的创建。

说明

- 一个ELB实例仅能创建一个VPC通道，创建完成后不支持更新操作。
- 创建ELB实例的具体步骤请参见，目前只支持购买增强型负载均衡，且“类型”为“私网”。

----结束

后续操作

创建API，将部署在VPC中的后端服务开放API，从而实现后端服务的负载均衡。

3.7.2 删除 VPC 通道

操作场景

已创建的VPC通道不再需要时，可以直接删除。

说明

如果API已经使用VPC通道，且API已发布到环境，此时无法删除此VPC通道。

前提条件

已创建VPC通道。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤4 通过以下任意一种方法，弹出“删除VPC通道”对话框。

- 在待删除的VPC通道所在行，单击“删除”。
- 单击“*VPC通道名称*”，进入VPC通道详情页面。在右上角单击“删除”。

步骤5 单击“确定”，完成VPC通道的删除。

----结束

3.7.3 编辑健康检查配置

操作场景

VPC通道创建完成后，可通过编辑健康检查配置修改健康检查项。

前提条件

已创建VPC通道。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤4 单击“*VPC通道名称*”，进入VPC通道详情页面。

步骤5 单击“健康检查”，进入“健康检查”页签。

步骤6 单击“编辑”，弹出“编辑健康检查配置”对话框。

步骤7 编辑如表3-25所示信息。

表 3-25 健康检查

信息项	描述
协议	使用以下协议，对VPC中主机执行健康检查。 ● TCP ● HTTP ● HTTPS 默认为TCP协议。
路径	健康检查时的目标路径。 仅在协议不为“TCP”时，需要设置。
检查端口	健康检查的目标端口。 缺省时为VPC中主机的端口号。
正常阈值	判定VPC中主机正常的依据为：连续检查*x*成功，x为您设置的正常阈值。 取值为2 ~ 10。缺省时为2。
异常阈值	判定VPC中主机异常的依据为：连续检查*x失败*，x为您设置的异常阈值。 取值为2 ~ 10。缺省时为5。
超时时间	检查期间，无响应的时间，单位为秒。 取值为2 ~ 30。缺省时为5。

信息项	描述
间隔时间	连续两次检查的间隔时间，单位为秒。 取值为5 ~ 300。缺省时为10。
HTTP响应码	目标HTTP响应时使用的HTTP代码。 仅在协议不为“TCP”时，需要设置。

步骤8 单击“确定”，完成健康检查配置的修改。

----结束

3.7.4 在 VPC 通道中编辑云服务器配置

操作场景

在创建VPC通道后，可以通过编辑云服务器为VPC通道增加/删除云服务器或编辑云服务器的权重。

前提条件

已创建VPC通道。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤4 单击“*VPC通道名称*”，进入VPC通道详情页面。

步骤5 单击“云服务器”，进入“云服务器”页签。

步骤6 根据您的需要为VPC通道增加/删除云服务器或编辑云服务器的权重。

- 增加云服务器
  a. 单击“添加云服务器”，弹出“添加云服务器”对话框。
  b. 勾选需要添加的云服务器，并且设置权重，单击“添加”。

  说明

  待添加的云服务器的安全组必须允许100.125.0.0/16网段访问，否则将导致健康检查失败及业务不通。
- 删除云服务器
  a. 在待删除的云服务器所在行，单击“删除”，弹出“删除云服务器”对话框。
  b. 单击“确定”。
- 编辑云服务器权重

a. 在待编辑权重的云服务器所在行，单击。

b. 输入需要的权重值，单击 。

- 批量编辑云服务器权重
  a. 勾选待编辑权重的云服务器，单击“批量编辑权重”，弹出“编辑权重”对话框。
  b. 为每台云服务器设置对应的权重值，单击“确定”。

----结束

3.8 自定义认证

3.8.1 创建自定义认证

操作场景

自定义认证包含两种认证：前端自定义认证和后端自定义认证。

- 前端自定义认证：如果您希望使用自己的认证系统，而不是APP认证/IAM认证对API的访问进行认证鉴权时，您可以使用自定义认证，通过您自定义的函数进行认证鉴权。
- 后端自定义认证：当不同的后端服务使用不同的认证系统时，导致您需要为不同的认证系统定制化开发API，而APIG通过自定义认证功能，将多种认证系统集成，简化API开发的复杂度。您只需要在APIG中创建自定义的函数认证，APIG通过此函数对接后端认证系统，获取后端服务的访问授权。

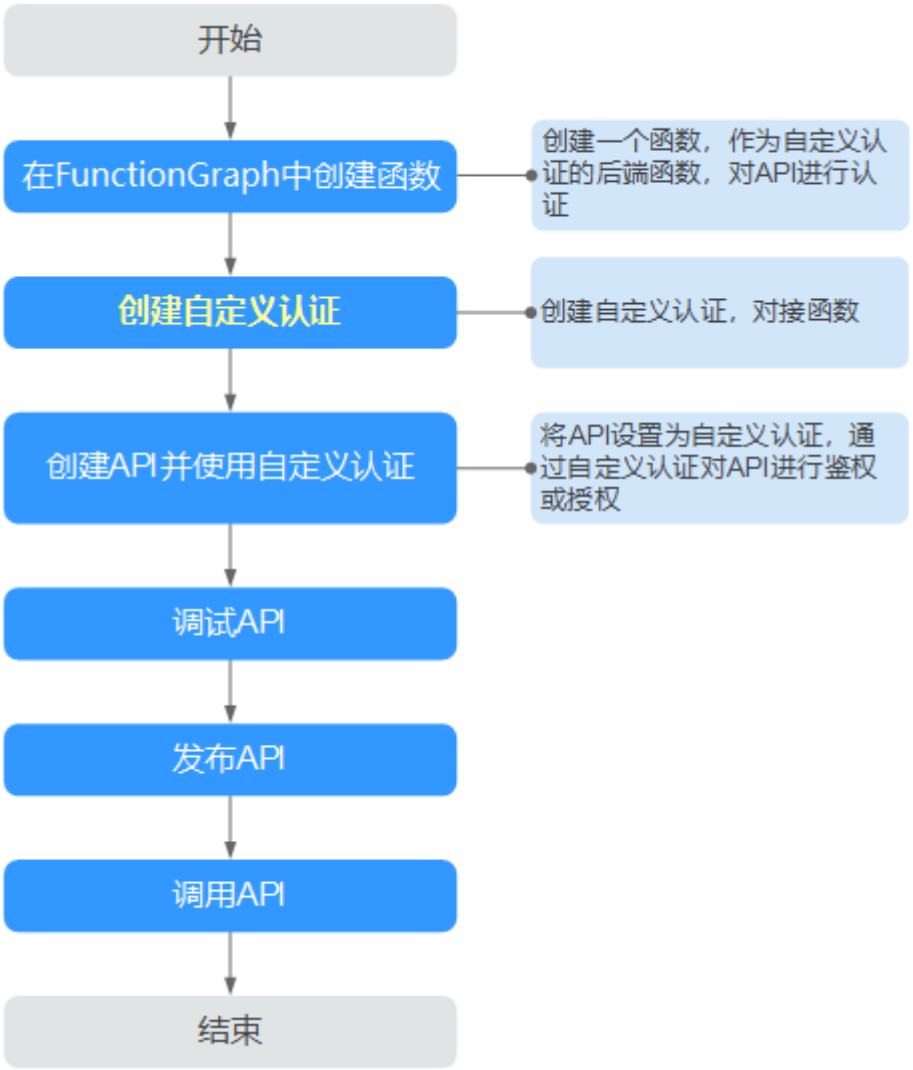
说明

自定义认证依赖函数工作流服务。如果当前Region没有上线函数工作流服务，则不支持使用自定义认证。

自定义认证的具体使用指导，可参考API网关《开发指南》的自定义认证相关章节。

使用自定义认证调用API的流程如下图所示：

图 3-6 使用自定义认证调用 API



前提条件

已在函数工作流服务中完成函数创建。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 在“开放API > 自定义认证”页签，单击“创建自定义认证”，弹出“创建自定义认证”对话框。

步骤4 填写如表3-26所示信息。

表 3-26 自定义认证参数

信息项	描述
认证名称	您自定义的认证名称，用于区分不同的自定义认证。
类型	• 前端：对API的访问进行认证鉴权。 • 后端：对后端服务的访问授权。
函数地址	选择在FunctionGraph中创建的函数。
身份来源	设置用于认证的请求参数。 当“类型”为“前端”，且“缓存时间”不为0时，必须设置此参数。使用缓存时，此参数将作为搜索条件来查询认证结果。
缓存时间	设置认证结果缓存的时间。 值为0时代表不缓存，最大支持3600秒。
用户数据	您自定义的请求参数，APIG调用函数时，与“身份来源”一同作为请求参数。

步骤5 单击“创建”，完成自定义认证的创建。

----结束

3.8.2 删除自定义认证

操作场景

当自定义的认证已不再需要时，可以删除自定义认证。

说明

- 自定义认证依赖函数工作流服务。如果当前Region没有上线函数工作流服务，则不支持使用自定义认证。
- 已在API中使用的自定义认证无法被删除。

前提条件

已**创建自定义认证**。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 在“开放API > 自定义认证”页签，在待删除的自定义认证所在行，单击“删除”，弹出“删除自定义认证”对话框。

步骤4 单击“确定”。

----结束

3.9 监控

3.9.1 支持的监控指标

功能说明

本节定义了API网关服务上报云监控服务的监控指标的命名空间，监控指标列表和维度定义，用户可以通过云监控服务提供管理控制台来检索API网关服务产生的监控指标和告警信息。

命名空间

共享版：SYS.APIG

API 网关监控指标

表 3-27 API 网关共享版监控指标说明

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
avg_latency	平均延迟毫秒数	该指标用于统计测量api接口平均响应延时时间	≥0 单位：毫秒	测量对象：单个API 测量维度：api_id	1分钟
input_throughput	流入流量	该指标用于统计测量api接口请求流量	≥0 单位：Byte/KB/MB/GB	测量对象：单个API 测量维度：api_id	1分钟
max_latency	最大延迟毫秒数	该指标用于统计测量api接口最大响应延时时间	≥0 单位：毫秒	测量对象：单个API 测量维度：api_id	1分钟
output_throughput	流出流量	该指标用于统计测量api接口返回流量	≥0 单位：Byte/KB/MB/GB	测量对象：单个API 测量维度：api_id	1分钟
req_count	接口调用次数	该指标用于统计测量api接口调用次数	≥0	测量对象：单个API 测量维度：api_id	1分钟

指标ID	指标名称	含义	取值范围	测量对象&维度	监控周期（原始指标）
req_count_2xx	2xx调用次数	该指标用于统计测量api接口调用2xx的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_4xx	4xx异常次数	该指标用于统计测量api接口返回4xx错误的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_5xx	5xx异常次数	该指标用于统计测量api接口返回5xx错误的次数	≥0	测量对象：单个API 测量维度：api_id	1分钟
req_count_error	异常次数	该指标用于统计测量api接口总的错误次数	≥0	测量对象：单个API 测量维度：api_id	1分钟

维度

表 3-28 API 网关共享版监控指标测量维度

Key	Value
api_id	API

3.9.2 创建告警规则

操作场景

通过创建告警规则，您可自定义监控目标与通知策略，及时了解API网关服务运行状况，从而起到预警作用。

告警规则包括告警规则名称、监控对象、监控指标、告警阈值、监控周期和是否发送通知等参数。

前提条件

API已被调用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 单击*API名称*，进入“总览”页面。

步骤5 单击“查看更多监控”，进入云监控界面，参考《云监控服务用户指南》的“创建告警规则”章节为API网关创建告警规则。

----结束

3.9.3 查看监控指标

操作场景

云监控对API网关的运行状态进行日常监控，可以通过控制台直观的查看API网关各项监控指标。

前提条件

已创建API分组和分组内的API。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 单击“开放API > API管理”，进入到API管理信息页面。

步骤4 单击*API名称*，进入“总览”页面。

查看API的各项监控指标。

步骤5 单击“查看更多监控”，进入云监控界面，查看更多监控数据。

说明

监控数据保留周期为两天，如果需要长时间保留，需要配置OBS桶，将监控数据保存至OBS桶中。

----结束

4 调用 API

4.1 应用管理

4.1.1 创建应用并获取授权

操作场景

使用APP认证的API，需要在API网关中创建一个应用，以生成应用ID和密钥对（AppKey、AppSecret）。将创建的应用绑定API后，才可以使用APP认证调用API。在API调用过程中，把密钥对替换SDK中的密钥对，API网关服务根据密钥对进行身份核对，完成鉴权。关于使用APP认证的方法，具体请参考《开发指南》。

说明

- 使用无认证/IAM认证的API，无需创建应用。
- 每个用户最多创建50个应用。

创建应用

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 单击“创建应用”，弹出“创建应用”对话框。填写如表4-1所示信息。

表 4-1 应用信息

信息项	描述
应用名称	应用名称。
描述	对应用的介绍。

步骤5 单击“确定”，创建应用。

创建应用成功后，在“应用管理”页面的列表中显示新创建的应用和应用ID。

步骤6 单击*应用名称*，进入应用详情页面，查看AppKey和AppSecret。

----结束

绑定 API

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 通过以下任意一种方法，进入“绑定API”页面。

- 在待绑定API的应用所在行，单击“绑定API”，进入“绑定API”界面。单击“绑定API”。
- 单击待绑定API的应用名称，进入应用详情页面。单击“绑定API”。

步骤5 选择授权环境，勾选API，单击“绑定”，完成API绑定策略。

绑定成功后，可以在应用详情页面查看已绑定的API。

说明

- 如果待添加绑定API列表中包含无需绑定的API，在此API所在行单击“解绑”，将无需绑定的API删除。
- 如果需要调试已绑定的API，单击“调试API”，进入调试页面。

----结束

后续操作

通过不同认证方式**调用API**。

4.1.2 删除应用

操作场景

已创建的应用不再提供服务，可以将应用删除。

前提条件

已创建应用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 通过以下任意一种方式，进入“删除应用”对话框。

- 在待删除的应用所在行，单击“删除”。
- 单击“*应用名称*”，进入应用详情页面，在右上角单击“删除”。

说明

仅在应用未绑定任何API时，支持删除，否则请先解绑API。

步骤5 单击“确定”，完成应用的删除。

----结束

4.1.3 重置 AppSecret

操作场景

重置AppSecret，将AppSecret的值重新改变。重置完成后，原先的AppSecret将失效，绑定此应用的API将无法调用，请更新AppSecret，并重新调用API。

前提条件

已创建应用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 单击待重置AppSecret的应用名称，进入应用详情页面。

步骤5 在右上角单击“重置AppSecret”，弹出“重置AppSecret”对话框。

步骤6 单击“确定”，完成AppSecret的重置。

----结束

4.1.4 为简易认证添加 AppCode

操作场景

简易认证指调用API时，在HTTP请求头部消息增加一个参数X-Apig-AppCode（参数值填应用详情中“AppCode”的值），而不需要对请求内容签名，API网关也仅校验AppCode，不校验请求签名，从而实现快速响应。

当使用APP认证，且开启了简易认证模式，API请求既可以选择使用Appkey和AppSecret做签名和校验，也可以选择使用AppCode进行简易认证。

说明

- 为了确保安全，简易认证仅支持HTTPS方式调用API，不支持HTTP。
- 每个应用最多可创建5个AppCode。

前提条件

已创建应用。

生成 AppCode

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

步骤3 选择“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 单击待查看的应用名称，进入应用详情页面。

步骤5 单击“AppCode”页签，进入AppCode的管理界面。

步骤6 单击“添加AppCode”，生成AppCode。可自动生成，也可手动输入。

----结束

使用 AppCode 进行 API 请求的简易认证

步骤1 在创建API时，选择“APP认证”并且开启“支持简易认证”。

说明

如果您修改已有API为简易认证，需要在修改完成后，将API重新发布，使简易认证模式生效。

步骤2 将支持简易认证的API绑定到已创建的应用。

步骤3 发送请求时，增加请求头部参数“X-Apig-AppCode”，省略请求签名相关信息。

以Curl方式为例，增加头部参数名称：X-Apig-AppCode，参数值填**已生成的AppCode**。

```
curl -X GET "https://api.exampledemo.com/testapi" -H "content-type: application/json"  -H "host: api.exampledemo.com" -H "X-Apig-AppCode: xhrJVJKABSOxc7d**********FZL4gSHEXkCMQC"
```

----结束

4.1.5 查看应用绑定的 API 详情

操作场景

在应用绑定API后，查看应用绑定的API详情。

前提条件

- 已创建应用。
- 应用已绑定API。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 选择“调用API > 应用管理”，进入到应用管理信息页面。

步骤4 单击待查看的应用名称，进入应用详情页面。

步骤5 单击待查看的API名称，进入API详情页面，查看API详情。

----结束

4.2 SDK

API网关开放的API，安全认证方式可选IAM认证、APP认证、自定义认证或无认证。四者的区别以及如何选择，请参考《开发指南》中关于“如何选择认证方式”的介绍。

本操作主要提供APP认证的SDK下载以及文档。

IAM认证请参考《开发指南》中关于“使用IAM认证调用API”的介绍。

操作场景

API使用APP认证时，请根据需要下载SDK包和文档，参考文档完成API的调用。

操作步骤

步骤1 登录管理控制台。

步骤2 单击管理控制台左上角 ，然后单击“API网关 APIG”。

步骤3 单击“调用API > SDK”，进入到SDK页面。

步骤4 在待下载的语言中，单击“下载SDK”，下载SDK包。

如需查看文档，请单击“SDK文档”。

----结束

4.3 调用已发布的 API

4.3.1 调用 API

获取 API 及文档

在调用API前，您需要向API提供者获取API的请求信息，包括访问域名、请求协议、请求方法、请求路径以及请求参数。

获取API：通过线下传递（如企业内部或者企业间合作）。

获取文档：如果API为云服务官方提供的服务，还可以在帮助中心获取参考文档。

根据API使用的安全认证方式，还要获取相关的请求认证信息：

- **APP认证**：
  - 签名认证：向API提供者获取该API所授权应用的Key和Secret（或客户端的AppKey和AppSecret），以及用于调用API的SDK。
  - 简易认证：向API提供者获取该API所在应用的AppCode。
  - 其他认证：向API提供者获取该API所授权应用的Key和Secret（或客户端的AppKey和AppSecret）。
- **IAM认证**：通过云服务平台的帐号凭证（帐号和密码获取Token或者AK/SK）进行认证。如果使用AK/SK进行认证，还需要向API提供者获取用于调用API的SDK。
- **自定义认证**：向API提供者获取请求参数中要携带的自定义认证信息。
- **无认证**：无需认证信息。

调用 API

步骤1 配置请求地址相关参数。

API调用场景	API请求参数配置
使用域名调用API	使用服务分配的子域名或服务绑定的域名调用API，无需另外配置。

步骤2 配置认证参数。

API认证方式	API请求参数配置
APP认证（签名认证）	使用获取的SDK对API请求进行签名，具体请参考《开发指南》的“使用APP认证调用API”章节。
APP认证（简易认证）	在API请求中添加Header参数“X-Apig-AppCode”，参数值为**获取API及文档**中获取到的AppCode。
IAM认证（Token认证）	先获取云服务平台的认证Token，然后在API请求中携带Token进行认证，具体请参考《开发指南》的“Token认证”章节。
IAM认证（AK/SK认证）	调用API时，使用获取的SDK对API请求进行签名，具体请参考《开发指南》的“AK/SK认证”章节。

API认证方式	API请求参数配置
自定义认证	在API请求参数中携带认证信息进行认证。
无认证	无需认证，可直接调用API。

----结束

4.3.2 响应消息头

调用API时，API网关增加如下响应消息头。

X-Apig-Mode: debug表示响应消息头增加API网关调试信息。

响应消息头	描述	说明
X-Request-Id	请求ID	所有合法请求，都会返回此参数
X-Apig-Latency	从API网关接收请求到后端返回消息头的用时	仅在请求消息头包含X-Apig-Mode: debug时，返回此参数
X-Apig-Upstream-Latency	从API网关请求后端到后端返回消息头的用时	仅在请求消息头包含X-Apig-Mode: debug，且后端服务类型不为Mock时，返回此参数
X-Apig-RateLimit-api	API流量控制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了API流量控制时，返回此参数
X-Apig-RateLimit-user	用户流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了用户流量限制时，返回此参数
X-Apig-RateLimit-app	应用流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了应用流量限制时，返回此参数
X-Apig-RateLimit-ip	源IP流量限制信息 示例：remain:9,limit:10,time:10 second	仅在请求消息头包含X-Apig-Mode: debug，且API配置了源IP流量限制时，返回此参数
X-Apig-RateLimit-api-allenv	API默认流控信息 示例：remain:199,limit:200,time:1 second	仅在请求消息头包含X-Apig-Mode: debug时，返回此参数

4.3.3 错误码

当调用API时，可能遇到如表4-2所示的错误码。

说明

- 通过《API参考》管理API，发生错误时，产生的错误码请参考。
- 使用APIG错误码时，请以错误码（如APIG.0101）为准，错误信息并非固定不变，有时会对错误信息进行优化修改。

表 4-2 错误码

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0101	The API does not exist or has not been published in the environment.	404	API不存在或未发布到环境	检查调用API所使用的域名、请求方法、路径和注册的API是否一致；检查API是否发布，如果发布到非生产环境，检查请求X-Stage头是否为发布的环境名；检查调用API使用的域名是否已经绑定到API所在的分组。
APIG.0101	The API does not exist.	404	API请求方法不存在	检查API请求方法是否与API定义的方法相同
APIG.0103	The backend does not exist.	500	无法找到后端	联系技术支持
APIG.0104	The plug-ins do not exist.	500	无法找到插件配置	联系技术支持
APIG.0105	The backend configurations do not exist.	500	无法找到后端配置	联系技术支持
APIG.0106	Orchestration error.	400	编排错误	检查API配置的前后端参数是否合理
APIG.0201	API request error.	400	请求格式不合法	使用合法的请求
APIG.0201	Request entity too large.	413	请求body过大（大于12M）	减小请求body大小
APIG.0201	Request URI too large.	414	请求URI过大（大于32K）	减小请求URI大小
APIG.0201	Request headers too large.	494	请求头过大（单个请求头大于32K或所有请求头总长度大于128K）	减小请求头大小

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0201	Backend unavailable.	502	后端不可用	检查API配置的后端地址是否可用
APIG.0201	Backend timeout.	504	后端超时	增大超时时间或缩小后端的处理时间
APIG.0201	An unexpected error occurred	500	内部错误	联系技术支持
APIG.0202	Backend unavailable	502	后端不可用	检查API配置的后端请求协议是否与后端服务请求协议一致
APIG.0204	SSL protocol is not supported: TLSv1.1	400	SSL协议版本不支持	使用支持的SSL协议版本
APIG.0301	Incorrect IAM authentication information.	401	IAM认证信息错误	检查token是否正确
APIG.0302	The IAM user is not authorized to access the API.	403	IAM用户不允许访问API	检查用户是否被黑白名单限制
APIG.0303	Incorrect app authentication information.	401	APP认证信息错误	检查请求的方法、路径、查询参数、请求体和签名使用的方法、路径、查询参数、请求体是否一致；检查客户端机器时间是否正确。请参考检查签名代码的问题。
APIG.0304	The app is not authorized to access the API.	403	APP不允许访问API	检查APP是否授权访问API
APIG.0305	Incorrect authentication information.	401	认证信息错误	检查认证信息是否正确
APIG.0306	API access denied.	403	不允许访问API	检查是否授权访问API
APIG.0307	The token must be updated.	401	token需要更新	重新从IAM获取token

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0308	The throttling threshold has been reached.	429	超出流控值限制	等待流控刷新后访问。如果触发子域名的单日请求数上限，请绑定独立域名。
APIG.0310	The project is unavailable.	403	project不可使用	使用其他project访问
APIG.0311	Incorrect debugging authentication information.	401	调试认证信息错误	联系技术支持
APIG.0401	Unknown client IP address.	403	无法识别客户端IP地址	联系技术支持
APIG.0402	The IP address is not authorized to access the API.	403	IP地址不允许访问	检查IP地址是否被黑白名单限制
APIG.0404	Access to the backend IP address has been denied.	403	后端IP不允许访问	后端IP地址或后端域名对应的IP地址不允许访问
APIG.0502	The app has been frozen.	405	APP被冻结	余额不足
APIG.0601	Internal server error.	500	内部错误	联系技术支持
APIG.0602	Bad request.	400	非法请求	检查请求是否合法
APIG.0605	Domain name resolution failed.	500	域名解析失败	检查域名拼写，以及域名是否绑定了正确的后端地址
APIG.0606	Failed to load the API configurations.	500	未加载API配置	联系技术支持
APIG.0607	The following protocol is supported: {xxx}	400	协议不被允许，允许的协议是*xxx*。 注意：xxx以实际响应中的内容为准。	改用支持的协议（HTTP/HTTPS）访问
APIG.0608	Failed to obtain the admin token.	500	无法获取管理帐户	联系技术支持
APIG.0609	The VPC backend does not exist.	500	找不到vpc后端	联系技术支持

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0610	No backend available.	502	没有可连接的后端	检查所有后端是否可用，如调用信息与实际配置是否一致。
APIG.0611	The backend port does not exist.	500	后端端口未找到	联系技术支持
APIG.0612	An API cannot call itself.	500	API调用自身	修改API后端配置，递归调用层数不能超过10层。
APIG.0613	The IAM service is currently unavailable.	503	IAM服务暂时不可用	联系技术支持
APIG.0705	Backend signature calculation failed.	500	计算后端签名失败	联系技术支持
APIG.0802	The IAM user is forbidden in the currently selected region	403	该IAM用户在当前region中被禁用	联系技术支持
APIG.1009	AppKey or AppSecret is invalid	400	AppKey或AppSecret不合法	检查请求的AppKey或AppSecret是否正确

5 审计

开通云审计服务

如果您需要收集、记录或者查询API网关服务的操作日志，用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景时，那么需要先开通云审计服务，具体请参见《云审计服务用户指南》的“开启云审计服务”章节。

云审计服务包含以下功能：

- 记录审计日志
- 审计日志查询
- 审计日志转储
- 事件文件加密
- 关键操作通知

查看审计日志

如果需要查看审计日志，具体步骤请参见《云审计服务用户指南》的“查看追踪事件”章节。

图 5-1 查看日志

查看关键操作列表

通过云审计，您可以记录与API网关相关的操作事件，便于日后的查询、审计和回溯。

关闭云审计服务

如果需要关闭云审计服务，具体步骤请参见《云审计服务用户指南》的“删除追踪器”章节。

6 API 配额管理

如果您需要修改默认限制值，请参考“帮助中心 > 其他 > 常见问题 > 如何申请扩大配额”。

表 6-1 API 网关配额管理明细

限制项	默认限制	能否修改
API分组数量	每个用户最多创建50个API分组。	√
API数量	每个用户最多创建200个API。	√
后端策略数量	每个用户最多创建5个后端策略。	√
应用数量	每个用户最多创建50个应用。应用配额包括用户自行创建的应用和API市场购买API生成的应用。	√
流控策略数量	● 每个用户最多创建30个流控策略。 ● 用户流量限制不超过API流量限制。 ● 应用流量限制不超过用户流量限制。 ● 源IP流量限制不超过API流量限制。	√
环境数量	每个用户最多创建10个环境。	√
签名密钥数量	每个用户最多创建30个签名密钥。	√
访问控制策略数量	每个用户最多可以创建100个访问控制策略。	√
VPC通道数量	每个用户最多创建30个VPC通道。	√
变量数量	每个分组在任意一个环境中，最多创建50个变量。	√
独立域名数量	每个分组最多可以绑定5个独立域名。	√
云服务器数量	每个VPC通道最多添加200个云服务器。	√
参数数量	每个API最多创建50个参数。	√

限制项	默认限制	能否修改
发布历史数量	同一个API在每个环境中最多记录10条最新的发布历史。	√
每个API的访问频率	不超过200次/秒。	√
特殊应用	每个流控策略最多可创建30个特殊应用。	√
特殊租户	每个流控策略最多可创建30个特殊租户。	√
子域名访问次数	每个子域名每天最多可以访问1000次。	x
调用请求包的大小	API每次最大可以调用12M的请求包	x
TLS协议	支持TLS1.1和TLS1.2，推荐使用TLS1.2。	x
实名认证	未实名认证的用户，无法进行任何的创建操作。	x