API 网关

用户指南

文档版本 18

发布日期 2025-02-10

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 APIG 业务使用流程

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。

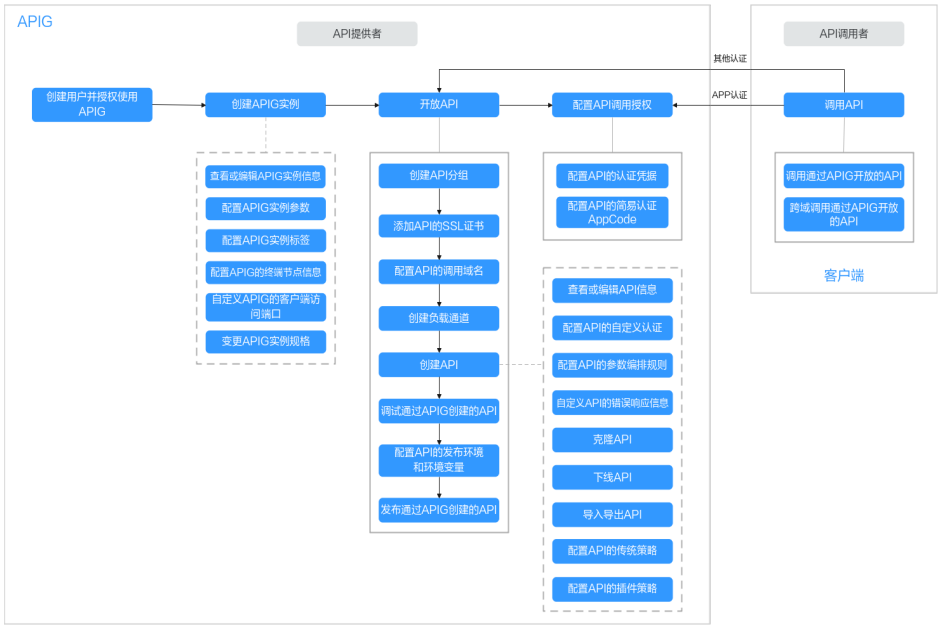
须知

API网关支持**专享版**和**共享版**（存量用户）功能。共享版功能已下线，当前仅存量用户可以使用，共享版功能操作指导请参考**共享版操作指导（仅存量用户使用）**，其余为专享版功能操作指导章节。

使用流程

使用API网关进行API的托管流程如下图所示。

图 1-1 业务使用流程



1. **创建用户并授权使用APIG**

   通过IAM服务创建用户并授权使用API网关，如果系统预置的APIG权限不满足授权要求，您也可以创建自定义策略。

2. **创建APIG实例**

   实例是一个独立的资源空间，所有的操作都是在实例内进行，不同实例间的资源相互隔离。因此，要开放API对外提供服务，首先需要创建实例。

   实例创建完成后，您可以通过**配置实例参数**调整组件的相关功能，**配置APIG实例标签**分组标记实例资源，**配置APIG的终端节点信息**连接终端节点服务，更多配置操作请参考**管理APIG实例**章节。

3. **开放API**

   将成熟的业务能力（如服务、数据等）作为后端服务，在API网关中开放API，提供给API调用者使用，实现业务能力变现。

   如果您需要把自己的认证系统用于API调用的认证鉴权，可以通过**配置API的自定义认证**来实现；需要对API进行参数编排，可以通过**配置API的参数编排规则**来实现；需要自定义API的错误响应信息，可以通过**自定义API的错误响应信息**来实现。更多API相关操作，请参考**管理API**。

4. **配置API调用授权（可选）**

   使用APP认证方式的API，需要配置调用授权，把API授权给指定的凭据。API调用者使用凭据的Key和Secret进行API请求的安全认证，也可以使用凭据的AppCode进行简易认证。

   如果您需要限制API调用者在某个时间周期内的API调用次数，可以通过**配置API认证凭据的配额控制**来实现；如果您需要控制访问API的IP地址（API调用者的IP地址），可以通过**配置API认证的凭据访问控制**来实现。

5. **调用API**

   通过获取API及API访问地址，调用API。根据API使用认证方式的不同，调用API时需要进行不同的认证鉴权操作。

2 创建用户并授权使用 APIG

如果您需要对您所拥有的API网关服务进行权限管理，您可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用API网关服务资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将API网关服务资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用API网关服务的功能。

本章节为您介绍对用户授权的方法，操作流程如**图2-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的**表2-1**，并结合实际需求进行选择。如果您需要对除API网关服务之外的其它服务授权，IAM支持服务的所有策略请参见**权限策略**。

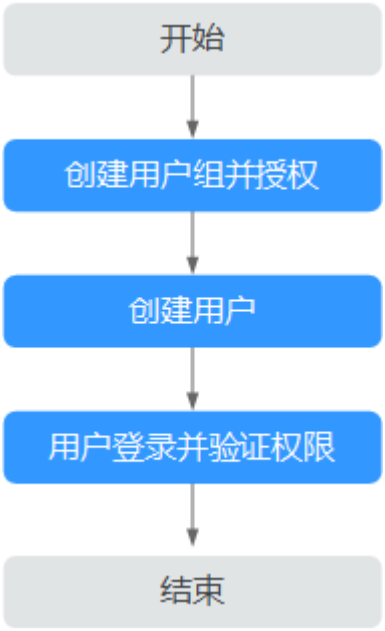
表 2-1 API 网关的系统角色或策略

系统角色/策略名称	描述	类别	依赖关系
APIG Administrator	API网关服务的管理员权限。拥有该权限的用户可以使用API网关服务的所有功能。	系统角色	如果在操作过程中涉及其他服务资源的创建、删除、变更等，则还需要在同项目中勾选对应服务的Administrator权限。
APIG FullAccess	API网关服务所有权限。拥有该权限的用户可以使用API网关服务的所有功能。	系统策略	无。

系统角色/策略名称	描述	类别	依赖关系
APIG ReadOnly Access	API网关服务的只读访问权限。拥有该权限的用户只能查看API网关服务的各类信息。	系统策略	无。

示例流程

图 2-1 给用户授权 API 网关服务权限流程



1. **创建用户组并授权**
   在IAM控制台创建用户组，并授予API网关服务的权限“APIG Administrator”或“APIG FullAccess”。
2. **创建用户并加入用户组**
   在IAM控制台创建用户，并将其加入**1**中创建的用户组。
3. **用户登录**并验证权限
   新创建的用户登录控制台，验证API网关服务的权限。

APIG 自定义策略

如果系统预置的API网关权限，不满足您的授权要求，可以创建自定义策略。自定义策略中可以添加的授权项（Action）请参考**细粒度策略支持的授权项**。

目前华为云支持以下两种方式创建自定义策略：

- 可视化视图创建自定义策略：无需了解策略语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。

- JSON视图创建自定义策略：可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

具体创建步骤请参见：**创建自定义策略**。本章为您介绍常用的API网关自定义策略样例。

APIG 自定义策略样例

- 示例1：授权用户创建API、调试API的权限

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    apig:apis:create
                    apig:apis:debug
                "
            ]
        }
    ]
}
```

- 示例2：拒绝用户创建API分组

  拒绝策略需要同时配合其他策略使用，否则没有实际作用。用户被授予的策略中，一个授权项的作用如果同时存在Allow和Deny，则遵循Deny优先。

  如果您给用户授予APIG FullAccess的系统策略，但不希望用户拥有APIG FullAccess中定义的创建API分组权限，您可以创建一条拒绝创建API分组的自定义策略，然后同时将APIG FullAccess和拒绝策略授予用户，根据Deny优先原则，则用户可以执行除创建API分组外的所有操作。拒绝策略示例如下：

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "
                    apig:apis:create
                    apig:apis:debug
                "
            ]
        }
    ]
}
```

3 创建 APIG 实例

本小节指导您顺利创建实例，实例创建完成后，才能创建API并对外提供服务。

约束与限制

- 实例配额

  同一项目ID下，一个主账号默认只能创建5个实例。如果您需要创建更多实例，可**提交工单**，申请修改配额。

- 用户权限
  - 如果您使用系统角色相关权限，需要同时拥有“APIG Administrator”和“VPC Administrator”权限才能创建实例。
  - 如果您使用系统策略，则拥有“APIG FullAccess”即可。
  - 如果您使用自定义策略，请参考**APIG自定义策略**。
- 网络

  如果您使用192.x.x.x或10.x.x.x网段，APIG则会使用172.31.32.0/19作为内部网段； 如果您使用172.x.x.x网段，APIG则会使用192.168.32.0/19作为内部网段。

- 子网中可用私有地址数量

  API网关专享实例的基础版、专业版、企业版，以及铂金版分别需要3、5、6、7个私有地址。在铂金版的基础上，铂金版X依次增加4个私有地址。例如，铂金版x2需要11个私有地址，铂金版x4需要19个私有地址。请确保您选择的子网段有足够多的私有地址可用，私有地址可在虚拟私有云服务的控制台查询。

- 负载

  创建实例后，不支持修改虚拟私有云（负载）。

- 安全组

  仅墨西哥城一、北京一区域配置的安全组生效。在其他区域购买实例后默认开启ELB负载。开启ELB负载的实例的安全组不生效，如需禁用部分IP请使用**访问控制策略**。

准备网络环境

- 负载

  虚拟私有云（Virtual Private Cloud，简称VPC）。实例需要配置虚拟私有云（负载），在同一负载中的资源（如ECS），可以使用实例的私有地址调用API。

在创建实例时，建议配置和您其他关联业务相同负载，确保网络安全的同时，方便网络配置。

- 安全组

  安全组类似防火墙，控制谁能访问实例的指定端口，以及控制实例的通信数据流向指定的目的地址。安全组入方向规则建议按需开放地址与端口，这样可以保护实例的网络安全。

  实例绑定的安全组有如下要求：

  - 入方向：如果需要从公网调用API，或从其他安全组内资源调用API，则需要为实例绑定的安全组的入方向放开**80**（HTTP）、**443**（HTTPS）两个端口。
  - 出方向：如果后端服务部署在公网，或者其他安全组内，则需要为实例绑定的安全组的出方向放开后端服务地址与API调用端口。
  - 如果API的前后端服务与实例绑定了相同的安全组、相同的虚拟私有云，则无需专门为实例开放上述端口。

创建实例

步骤1 进入**购买实例**页面。

步骤2 根据下表参数说明，配置实例参数。

表 3-1 API 网关实例参数说明

参数	说明
计费模式	实例的收费方式，当前支持“按需计费”方式。
区域	指APIG实例部署的区域，建议和您其他的业务部署在相同区域，这样不同的业务可以在负载内以子网方式通信，节省公网带宽成本，降低网络延时。
可用区	实例所在的可用区，不同可用区之间物理隔离，但内网互通。 ● APIG实例支持同时选择多个可用区，进行跨可用区部署，提升实例高可用性。 ● APIG不支持跨可用区迁移实例。 **如果创建单AZ实例，需要创建两个AZ的两个实例来提升业务可靠性，否则当一个AZ故障后，会导致业务不可用。**
实例名称	实例的名称，根据规划自定义。以中英文字符开头，由中英文字符、数字、中划线、下划线组成，长度为3~64个字符。
实例规格	当前开放基础版、专业版、企业版、铂金版实例。不同实例规格，对API请求的并发支持能力不同，具体请参考**规格说明**章节。 **说明** 目前仅北京四、华东二、利雅得、香港区域支持选择更多铂金版规格。

参数	说明
可维护时间窗	指允许云服务技术支持对实例进行维护的时间段。如果有维护需要，技术支持会提前与您沟通确认。 建议选择业务量较少的时间段。
企业项目	使用企业用户登录时，可选择实例所属企业项目。 有关企业项目的资源使用、迁移以及用户权限等，请参考**《企业管理用户指南》**。
公网入口	指允许外部服务通过弹性IP地址，调用实例创建的API。开启“公网入口”，需要绑定一个“弹性IP地址”，弹性IP地址另行**收费**。 • 除墨西哥城一、北京一区域外，在其他区域**开启公网入口**后，弹性IP地址由网关随机分配，不支持选择已有弹性IP地址。您可以根据业务预估设置合适的“入公网带宽”，入公网带宽费用按小时计算，以弹性IP服务的价格为准。 • 您需要使用独立域名/调试域名访问，使用调试域名访问时存在单日访问次数限制。可在创建API分组后，为分组绑定独立域名，独立域名需要解析到实例的弹性IP地址。 例如您有一个API，请求协议为HTTPS，Path为/apidemo，开启了公网访问，并为分组绑定了独立域名后，可使用https://{domain}/apidemo这个URL访问您的API。其中，{domain}表示已绑定到分组的独立域名，目标端口443可默认缺省。
公网出口	指允许API的后端服务部署在外部网络，APIG为实例开启公网出口。您可以根据业务预估设置合适的“出公网带宽”，出公网带宽费用按小时计费，以弹性IP服务的价格为准。
网络	指为实例绑定到一个VPC，并为其分配子网。 • 使用已创建的VPC和子网，请在下拉列表选择当前账号下创建的VPC和子网。 • 使用共享VPC和子网，请在下拉列表选择其他账号共享给当前账号的VPC和子网。 共享VPC基于**资源访问管理**（Resource Access Manager，简称RAM）服务的机制，VPC的所有者可以将VPC内的子网共享给一个或者多个账号使用。通过共享VPC功能，可以简化网络配置，帮助您统一配置和运维多个账号下的资源，有助于提升资源的管控效率，降低运维成本。有关VPC子网共享的更多信息，请参见**共享VPC**。 • 使用新的VPC和子网，请单击“控制台”，参考**创建虚拟私有云**章节创建待使用的新VPC和子网。

参数	说明
安全组	安全组用于设置端口访问规则，定义哪些端口允许被外部访问，以及允许访问外部哪些地址与端口。 例如，后端服务部署在外部网络，则需要设置相应的安全组规则，允许访问后端服务地址与API调用端口。 如果开启公网入口，安全组入方向需要放开80（HTTP）和443（HTTPS）端口的访问权限。 **说明** • 仅在墨西哥城一、北京一区域配置的安全组生效，在其他区域购买实例后默认开启ELB负载。开启ELB负载的实例的安全组不生效，如需禁用部分IP请使用**访问控制策略**。 • 开启ELB负载：ELB作为网关入口的负载均衡器，入口支持跨VPC访问。但在开启公网入口时，弹性IP地址由网关随机分配，不支持选择已有弹性IP地址。
终端节点服务名称	填写终端节点服务名称。购买实例后，同步创建VPC终端节点服务，可以被终端节点连接和访问。 如果填写了终端节点服务名称，购买实例后，在实例详情中的“终端节点管理”页签下展示名称为{region}.{终端节点服务名称}.{终端节点服务ID}；如果终端节点服务名称为空，购买实例后，在实例详情中的“终端节点管理”页签下展示名称为{region}.{apig}.{终端节点服务ID}。
标签	通过标签对实例资源进行标记，批量分类实例资源，实现对实例资源进行分组查询、分析及管理。如果没有标签选择可单击“查看预定义标签”创建，也可以直接输入标签键值创建。 实例创建完成后，也可以在**配置APIG实例标签**中设置。 如您的组织已经设定API网关服务的相关标签策略，则需按照标签策略规则为实例添加标签。标签如果不符合标签策略的规则，则可能会导致创建实例失败，请联系组织管理员了解标签策略详情。
描述	实例的描述信息。长度为1~255个字符。

步骤3 单击“立即购买”，进入实例规格确认页面。

步骤4 规格确认无误后，勾选服务协议，支付费用后，开始创建实例，界面显示创建进度。

----结束

后续操作说明

实例创建成功后，您可以开始创建和管理您的API。进入实例控制台后，概览界面展现实例信息、网络配置、配置参数等信息。

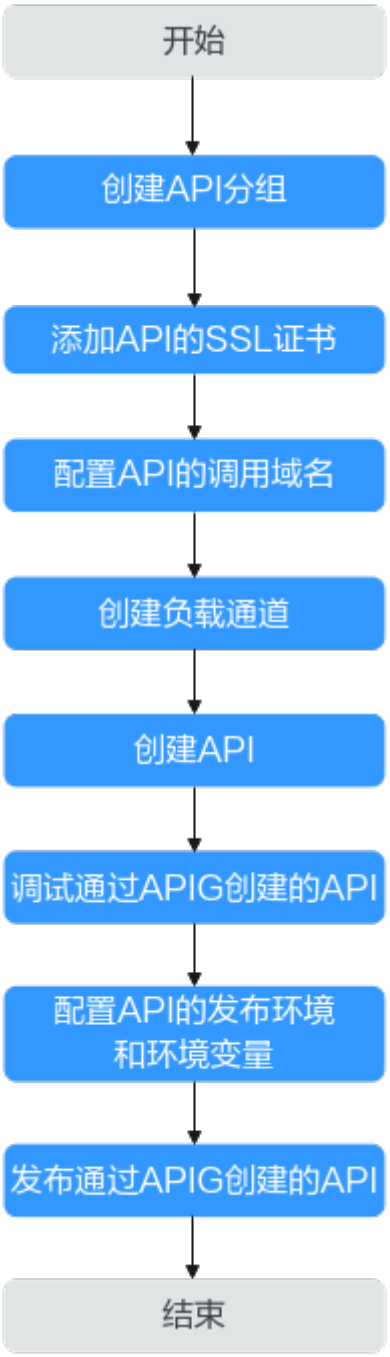
其中，实例名称、描述、时间窗、安全组，以及弹性IP地址等可以修改。

如果您要删除实例，请确认无业务影响后删除实例即可。

4 开放 API

4.1 开放 API 流程

企业或开发者通过API网关开放自身的服务与数据，实现业务能力变现。



1. **创建API分组**

   每个API都归属到某一个API分组下，在创建API前应提前创建API分组。

2. **添加API的SSL证书**

   如果API分组中的API支持HTTPS请求协议，需要为独立域名添加SSL证书。反之，跳过此步骤。

3. **配置API的调用域名**

   在开放API前，您需要为API分组绑定一个独立域名，供API调用者访问API使用。

   在绑定独立域名前，您可以使用系统为API分配的调试域名进行API调试，每天最多可以访问调试域名1000次。**系统自动分配的域名不能用于生产业务，且仅限应用程序调试使用。**

4. **创建API的负载通道（可选）**

   如果需要访问指定服务器中已部署的后端服务，可通过创建负载通道来实现。反之，跳过此步骤。

5. **创建API**

   把已有后端服务封装为标准RESTFul API或GRPC API，并对外开放。

   API创建成功后，您可根据业务需求**配置API策略**，**管理API**等。

6. **调试APIG创建的API**

   通过APIG提供的在线调试功能验证API服务是否正常可用。

7. **配置API的发布环境和环境变量（可选）**

   API可以同时提供给不同的环境调用，如生产、测试或开发。RELEASE是系统默认的发布环境，如果使用RELEASE环境，可跳过配置发布环境步骤。

   如果API的后端服务信息中定义了环境变量，则需要在环境中添加对应的变量。通过环境变量，可实现同一个API，在不同环境中调用不同的后端服务。

8. **发布APIG创建的API**

   把API发布到环境中，API只有在发布到环境后，才支持被调用。

4.2 创建 API 分组

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。

目前支持以下创建分组方式：

- 直接创建

  创建一个简单的分组，不包含API，用户可自行创建API。具体步骤请参见**创建API分组**。

- 导入API设计文件

  从本地导入已有的API设计文件，并同步创建API分组。具体步骤请参见**通过API设计文件导入API**。

- 导入CCE工作负载

  导入云容器引擎（Cloud Container Engine，简称CCE）工作负载，开放CCE服务能力。导入时，可同步创建API分组。具体步骤请参见**通过CCE工作负载导入API**。

说明

实例创建后，有一个DEFAULT分组，可直接通过虚拟私有云地址调用默认分组中的API。

约束与限制

- 一个API只能属于一个API分组。
- API分组创建后，系统为分组自动分配一个内部测试用的调试域名，此调试域名每天最多可以访问1000次。**您也可以在控制台上API分组详情的“分组信息”页面关闭“调试域名开关”来关闭调试域名，关闭后将隐藏调试域名，且不能通过调试域名调用API。**
- 调试域名不能用于生产业务，且仅限应用程序调试使用。
- 调试域名默认只能在与实例相同VPC内的服务器上解析和访问，如果调试域名要支持公网解析与访问，请在实例上绑定公网入口弹性IP。

创建 API 分组

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击“创建API分组 > 直接创建”，根据下表参数说明，在弹框中填写分组信息。

表 4-1 分组信息表

参数	说明
分组名称	API分组名称，用于将API接口进行分组管理。 支持中文、英文、数字、中划线、下划线、点、斜杠、中英文格式下的小括号和冒号、中文格式下的顿号，且只能以英文、汉字或数字开头，长度为3~255个字符。
描述	对分组的介绍。长度为0~1000个字符。

步骤5 单击“确定”，创建完成。

----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。

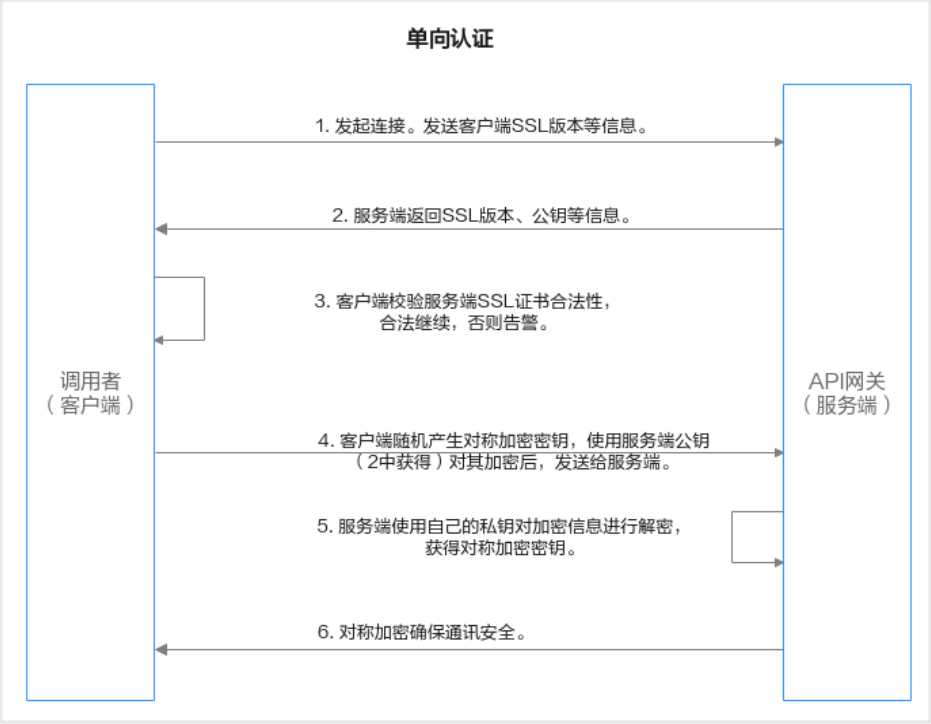
4.3 添加 API 的 SSL 证书

如果API分组中的API支持HTTPS请求协议，则在绑定独立域名后，还需为独立域名添加SSL证书。SSL证书是进行数据传输加密和身份证明的证书，支持单向认证和双向认证两种认证方式。

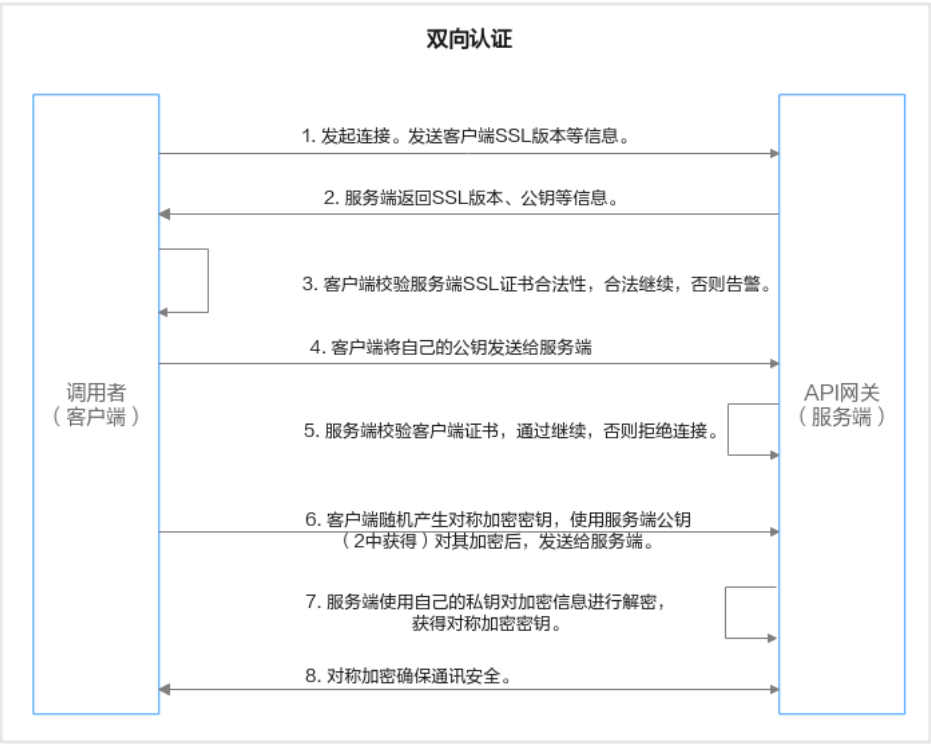
须知

如果不配置SSL证书，将无法保障请求的链路安全，请谨慎配置。

- 单向认证：客户端与服务端连接时，客户端需要验证所连接的服务端是否正确。



- 双向认证：客户端与服务端连接时，除了客户端需要验证所连接的服务器是否正确之外，服务端也需要验证接入的客户端是否正确。



约束与限制

- 仅支持添加pem编码格式的SSL证书。
- 添加的SSL证书仅支持RSA、ECDSA加密算法。

前提条件

- 已获取SSL证书。
- 使用双向认证时，需要获取CA证书。

创建 SSL 证书

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“SSL证书管理”页面，单击“创建SSL证书”。

步骤5 根据下表参数说明，配置证书。

表 4-2 SSL 证书配置

参数	配置说明
证书名称	填写SSL证书的名称，根据规划自定义。建议您按照一定的命名规则填写SSL证书名称，方便您快速识别和查找。 支持中文、英文、数字、英文格式的下划线，必须以英文或中文开头，长度为4~50个字符。
可见范围	• 当前实例：仅在当前实例下展示此证书。 • 全局：在当前账号和当前region的所有实例下都会展示此证书。
算法类型	选择证书所使用的加密算法类型，可选择RSA或ECC。 • RSA：目前在全球应用广泛的非对称加密算法，兼容性在三种算法中最好，支持主流浏览器和全平台操作系统。一般采用2048位或3072位的加密长度。 • ECC：椭圆曲线加密算法。相比于RSA，ECC加密速度快、效率更高、服务器资源消耗低，目前已在主流浏览器中得到推广，成为新一代主流算法。一般采用256位加密长度。
证书内容	填写pem编码格式的SSL证书内容。 以文本方式打开待添加证书里的PEM格式证书文件（后缀名为“.pem”），将证书内容复制到“证书内容”中即可。 如果证书为非pem编码格式，可参考**转换证书为PEM格式**进行证书格式转换。
密钥	填写pem编码格式的SSL证书密钥。 以文本方式打开待上传证书里的KEY格式或PEM格式的私钥文件（后缀名为“.pem”或“.key”），将私钥复制到“密钥”中即可。

参数	配置说明
CA	**双向认证时，需要填写CA证书，CA证书会同时校验服务端证书和客户端证书。**CA证书上传后，独立域名需要绑定SSL证书来开启双向认证。以文本方式打开上述证书内容的CA证书文件（后缀名为“.pem”），将内容复制到“CA”中即可。 ● 如果证书为非pem编码格式，可参考**转换证书为PEM格式**进行证书格式转换。 ● 如果当前实例不支持配置CA证书，可**提交工单**升级实例。

步骤6 单击“确定”。

证书创建完成后，进入API分组页面为独立域名**绑定SSL证书（可选）**。

----结束

转换证书为 PEM 格式

格式类型	转换方式（通过OpenSSL工具进行转换）
CER/CRT	将“cert.crt”证书文件直接重命名为“cert.pem”。
PFX	● 提取私钥命令，以“cert.pfx”转换为“key.pem”为例。 openssl pkcs12 -in cert.pfx -nocerts -out key.pem ● 提取证书命令，以“cert.pfx”转换为“cert.pem”为例。 openssl pkcs12 -in cert.pfx -nokeys -out cert.pem
P7B	1. 证书转换，以“cert.p7b”转换为“cert.cer”为例。 openssl pkcs7 -print_certs -in cert.p7b -out cert.cer 2. 将“cert.cer”证书文件直接重命名为“cert.pem”。
DER	● 提取私钥命令，以“privatekey.der”转换为“privatekey.pem”为例。 openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem ● 提取证书命令，以“cert.cer”转换为“cert.pem”为例。 openssl x509 -inform der -in cert.cer -out cert.pem

更新 SSL 证书

进入证书列表页面，找到待更新证书，在“操作”列单击“编辑”，修改证书信息即可。

- 更新SSL证书不影响API的调用。

- 如果待更新证书已绑定独立域名，那么所有访问这个域名的客户端都会看到更新后的证书。
- 如果更新的SSL证书已绑定独立域名且更新的内容新增CA证书，那么独立域名侧默认关闭“支持客户端认证”即关闭HTTPS双向认证；如果更新的SSL证书已绑定独立域名且更新的内容无CA证书，那么独立域名侧默认关闭“支持客户端认证”即未开启HTTPS双向认证。

4.4 配置 API 的调用域名

API分组创建后，系统为分组自动分配一个内部测试用的调试域名，此调试域名每天最多可以访问1000次。因此，在开放API前，您需要为API分组绑定独立域名，用户通过独立域名访问分组内的API。最多可以添加5个独立域名，不限访问次数。

独立域名可分为内网域名和公网域名两种：

- 内网域名：部署在云服务平台内的业务系统，可以使用内网域名访问API。
- 公网域名：部署在云服务平台外的业务系统，可以使用公网域名访问API。

您也可以使用系统分配的调试域名（子域名）访问API分组内的API，该调试域名唯一且不可修改，每天最多可以访问1000次，仅适用于内部测试使用。

当独立域名为泛域名（例如*.aaa.com）时，用户可以通过泛域名的所有子域名（例如default.aaa.com，1.aaa.com）访问所绑定分组下的所有API。

约束与限制

- 调试域名默认只能在与实例相同VPC内的服务器上解析和访问，如果调试域名要支持公网解析与访问，请在实例上绑定公网入口弹性IP。
- 调试域名不能用于生产业务，且仅限应用程序调试使用。
- 同一实例下的不同分组不能绑定相同的独立域名。
- 独立域名绑定端口时，同一域名不支持绑定相同端口。
- 同一域名不同端口，无论哪个端口绑定/修改/解绑SSL证书、开启/关闭客户端认证，所有端口都会同步生效。
- 如果您通过负载通道访问后端服务，那么独立域名绑定的端口需与负载通道中**后端服务器的访问端口**保持一致。
- 独立域名绑定端口后，如果您通过IP地址访问非DEFAULT分组下的API，那么需要在请求消息中添加Header参数“host”，host值必须带有对应的访问协议的端口（默认的80/443端口，host值可以不带）。
- 如果您通过IP地址访问API，则无法使用域名证书完成SSL认证，除非配置了IP证书。因此，不推荐使用IP地址访问API，否则无法保证链路安全。
- 启用http to https自动重定向时，由于浏览器限制，非GET或非HEAD方法的重定向可能导致数据丢失，因此，API请求方法限定为GET或HEAD。仅当API的请求协议选择“HTTPS”或“HTTP&HTTPS”，且独立域名已绑定SSL证书时重定向生效。

获取域名

1. 申请域名。
   - 云服务平台内业务系统访问API的场景，需获取**内网域名**作为独立域名。具体请参考**创建内网域名**。

- 云服务平台外业务系统访问API的场景，需获取**公网域名**作为独立域名。具体可通过域名注册商申请。

2. 在域名上添加实例“虚拟私有云访问地址”的A类型记录集，具体请参考**增加A类型记录集**。

   或者在域名上添加API分组“调试域名”的CNAME类型记录集，具体请参考**增加CNAME类型记录集**。

3. 如果API分组中的API支持HTTPS请求协议，则需要为独立域名添加SSL证书。您需要提前获取SSL证书的内容和密钥，并**创建SSL证书**。

绑定独立域名

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“域名管理”区域，单击“绑定独立域名”。

步骤6 根据下表参数说明，在弹窗中配置域名信息。

表 4-3 独立域名配置

参数	说明
域名	填写要**绑定的域名**。
支持最小TLS版本	传输层安全性协议（TLS：Transport Layer Security），是一种安全协议，目的是为互联网通信提供安全及数据完整性保障。选择域名访问所使用的最小TLS版本，TLS1.1或TLS1.2，推荐使用TLS1.2。暂不支持TLS 1.0或TLS 1.3。 该配置仅对HTTPS生效，不影响HTTP或者其他访问方式。您可以在**配置参数**页面通过“ssl_ciphers”参数配置HTTPS的加密套件。
支持http to https自动重定向	当用户的API采用http协议访问时，由于http没有传输安全与认证安全保障，可以开启自动重定向功能将API升级为安全的https协议访问，同时兼容已有的http协议。 仅当API的请求协议选择“HTTPS”或“HTTP&HTTPS”，且独立域名已绑定SSL证书时重定向生效。**由于浏览器限制，非GET或非HEAD方法的重定向可能导致数据丢失，因此API请求方法限定为GET或HEAD。**
HTTP端口	默认值“80”，HTTP协议的默认端口。您可以自定义入端口，相关操作请参考**自定义APIG的客户端访问端口**。不使用HTTP端口，选择“禁止”即可。
HTTPS端口	默认值“443”，HTTPS协议的默认端口。您可以自定义入端口，相关操作请参考**自定义APIG的客户端访问端口**。不使用HTTPS端口，选择“禁止”即可。

步骤7 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“解绑域名”。

----结束

绑定 SSL 证书（可选）

如果API分组中的API支持HTTPS请求协议，则需要为独立域名绑定SSL证书。否则跳过此步骤。

步骤1 在域名所在行单击“选择SSL证书”。

步骤2 在选择SSL证书弹窗中勾选要绑定的SSL证书，然后单击“确定”，完成SSL证书的绑定。

- 如果选择的SSL证书上传过CA证书，可以勾选“开启客户端认证”即开启HTTPS双向认证。**注意，开启/关闭客户端认证会对现有业务有影响，请谨慎操作。**
- 如果证书列表中无可用的SSL证书，可单击“创建SSL证书”，新增SSL证书，具体操作配置请参考**创建SSL证书**。

----结束

常见问题

- 绑定域名失败常见原因：未**解析域名**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。

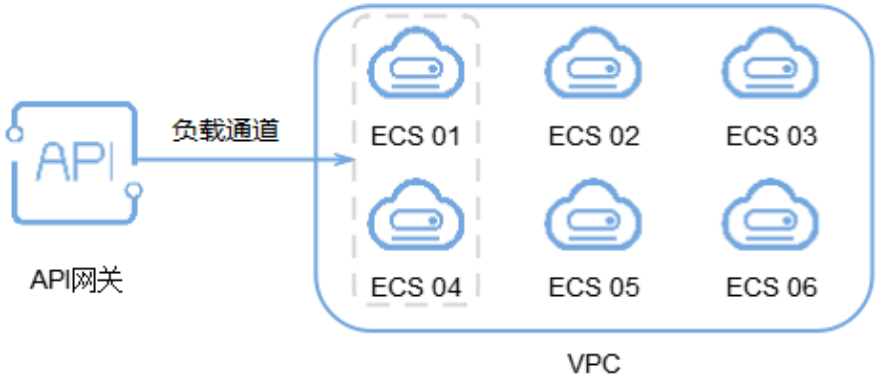
4.5 创建 API 的负载通道（可选）

负载通道主要用于将服务通过API网关**专享版**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，同时负载通道具有负载均衡功能（服务器通道类型），以及自动同步服务节点变更的能力（微服务通道类型）和使用已有的负载通道能力（引用负载通道类型），从而实现后端服务的负载均衡或自动同步服务节点的变更或重复使用负载通道。

创建负载通道后，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负载通道。

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

图 4-1 通过 API 网关访问负载通道中的 ECS



注意事项

- 创建**服务器**通道类型须注意以下事项：

  API网关与负载通道中的服务器之间网络互通。
- 创建**云容器引擎微服务**通道类型需注意以下事项：
  - 仅支持华为云CCE Turbo集群、VPC网络模型的CCE集群。
  - 您需要确保当前实例与CCE集群所属同一个VPC中，或通过其他方式保证两者网络可达，否则创建后调用API会出现失败场景。
  - 选择VPC网络模型的CCE集群时，您需要在实例详情界面的路由配置中添加CCE集群的容器网段，否则创建后调用API会出现失败场景。
  - 创建微服务类型的负载通道后，负载通道会监测工作负载下所有实例的地址变化，并更新到负载通道中。

前提条件

- 用户需要具备VPC Administrator角色权限。
- 如果通道类型为服务器，已创建云服务器。
- 如果通道类型为云容器引擎微服务，**已创建集群**，集群类型为CCE集群（VPC网络模型）或Turbo集群，并且**已创建工作负载**。

须知

- 如果当前实例不支持微服务通道类型，请联系技术支持升级实例到最新版本。
- 已创建的工作负载需配置Pod标签，在**微服务配置**时可通过Pod标签来指定工作负载，如用于工作负载服务的版本区分等。具体操作请参考**标签与注解**。
  - 在CCE控制台通过“创建负载”方式创建工作负载时，配置Pod标签。进入创建工作负载页面，在“高级配置 > 标签与注释 > Pod标签”区域配置即可。
  - 在CCE控制台通过“YAML创建”方式创建工作负载时，配置Pod标签。例如“app=service01”

```
spec:
  replicas: 2
  selector:
    matchLabels:
      app: 'service01'
```

创建负载通道

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 单击“负载通道”页签，进入到负载通道列表页面。

步骤5 单击“创建负载通道”，根据下表参数说明，配置基本信息。

表 4-4 基本信息配置

参数	说明
通道名称	自定义负载通道名称，用于识别不同的负载通道。支持中文、英文、数字、下划线、中划线、点，且只能以英文和中文开头，长度为3~64个字符。
端口	负载通道中主机的端口号，即用户的后端业务端口号。 取值范围为1~65535。
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：结合弹性服务器权重值，将请求轮流转发到每一台服务器。 • 加权最少：结合弹性服务器权重值，将请求转发到具有最少活跃连接数的那台服务器。 • 源地址哈希：由请求的来源IP地址决定请求被转发到哪一台云服务器，相同源地址的请求始终会转发到同一台服务器，除非该云服务器不可用。 • URI哈希：由请求的路径决定请求被转发到哪一台云服务器，相同路径的请求始终会转发到同一台服务器，除非该云服务器不可用。

参数	说明
通道类型	• 选择服务器类型，API的请求将被分发到通道中的弹性云服务器或指定的服务器IP，具体操作请参见**步骤6**。 • 选择微服务类型，API的请求将被分发到通道中的微服务IP，具体操作请参见**步骤7**。 • 选择引用负载通道，可以引用其他已有的负载通道，具体操作请参见**步骤8**。

步骤6 选择通道类型为服务器时，配置通道内服务器。

说明

负载通道支持私网ELB，可通过指定服务器地址配置。

- 选择云服务器。
  a. 单击“创建服务器分组”。
  根据下表参数说明，在弹窗中填写服务器分组信息，单击“确定”。

  表 4-5 服务器分组配置

参数	说明
分组名称	填写服务器分组的名称，根据规划自定义。建议您按照一定的命名规则填写分组名称，方便您快速识别和查找。 支持中文、英文、数字、下划线、中划线、点，且只能以英文和中文开头，长度为3~64个字符。
权重	填写服务器分组的权重值，权重值越大，转发到该分组下服务器的请求数量越多。默认为1，取值范围为0~100。
描述	填写分组的描述信息。长度为1~255个字符。

  b. 单击“添加云服务器”。
  在弹窗中，选择子网并勾选要添加的云服务器，单击“确定”。
  c. 配置完成后，进行**健康检查配置**。
- 指定服务器地址。
  a. 单击“创建服务器分组”。
  在弹窗中填写服务器分组信息，单击“确定”。配置参数请参考**表4-5**。
  b. 单击“添加后端服务器地址”，根据下表参数说明，在列表中填写后端服务器地址。

  表 4-6 后端服务器配置

参数	说明
后端服务器地址	填写后端服务器的IP地址。

参数	说明
是否备用节点	开启后对应后端服务器为备用节点，仅当非备用节点全部故障时工作。
端口	填写后端服务器的访问端口号。端口为0时，使用负载通道的端口。 取值范围为0~65535。
启停状态	选择是否启用服务器，只有启用后，请求才会分发到该服务器上。

c. 配置完成后，进行**健康检查配置**。

步骤7 选择通道类型为微服务时，配置微服务和服务器分组。

1. 根据下表参数说明，配置微服务信息。

表 4-7 云容器引擎微服务配置

参数	说明
微服务类型	默认云容器引擎CCE类型。
集群	选择集群，可单击“查看云容器引擎CCE”查看。 已创建的CCE集群与API网关实例属于同一个VPC，或者二者之间通过对等连接等方式保证网络可达。通过同一个VPC（有扩展网段等）、对等连接等方式连接网络时，需要在控制台将CCE集群详情中的“容器网段”添加到API网关实例详情中的“路由”上，否则会导致API网关到容器网络不通。
命名空间	选择CCE集群的命名空间。命名空间是对一组资源和对象的抽象整合。

参数	说明
工作负载类型	– 无状态负载 Deployment：在运行中始终不保存任何数据或状态的工作负载称为无状态负载 。 – 有状态工作负载 Statefulset：在运行过程中会保存数据或状态的工作负载称为有状态工作负载。 – 守护进程集 DaemonSet：守护进程集可以确保全部（或者某些）节点上仅运行一个Pod实例，当有节点加入集群时，也会为其新增一个Pod 。 当有节点从集群移除时，这些Pod会被回收。 **说明** 删除DaemonSet将会删除它创建的所有Pod。 工作负载类型的介绍请参考**工作负载概述**。
服务标识名 服务标识值	选择工作负载的Pod标签，通过Pod标签指定某个工作负载。服务标识名为Pod标签的键，服务标识值为Pod标签的值。 Pod标签相关内容指导，请参考**标签与注解**。

2. 配置服务器分组。
   单击“添加服务器分组”，根据下表参数说明，配置信息。

表 4-8 云容器引擎微服务的服务器分组配置

参数	说明
服务器分组名称	默认为服务标识值，用户也可根据业务需求修改。支持中文、英文、数字、下划线、中划线、点，且只能以英文和中文开头，长度为3~64个字符。
权重分配	填写服务器分组的权重值，权重值越大，转发到该分组下服务器的请求数量越多。默认为1，取值范围为0~100。 **分发算法**选择哈希算法时，权重默认为1，且不支持修改。
后端服务端口	后端服务器的访问端口号。不指定端口号或端口号为0时，默认使用负载通道的端口号。 取值范围为0~65535。
工作负载名称	选择CCE工作负载。

参数	说明

标签	选择工作负载的Pod标签。如果服务标识名和服务标识值不唯一，且不能指定某个工作负载时，还可以通过选择其他Pod标签指定某个工作负载。
	例如，工作负载01和工作负载02的app相同，可通过选择version或test_name区分工作负载01或工作负载02。
	工作负载01：
	`spec:`
	`  replicas: 2`
	`  selector:`
	`  matchLabels:`
	`  app: 'app01'`
	`  version: 'v1'`
	工作负载02：
	`spec:`
	`  replicas: 2`
	`  selector:`
	`  matchLabels:`
	`  app: 'app01'`
	`  test_name: 'test_value'`

3. 配置完成后，进行**健康检查配置**。

步骤8 选择通道类型为引用负载通道时，根据下表参数说明，配置服务器分组。

表 4-9 服务器分组配置

参数	说明
服务器分组名称	根据规划自定义。建议您按照一定的命名规则填写分组名称，方便您快速识别和查找。 支持中文、英文、数据、下划线、中划线、点，且只能以英文和中文开头，取值范围为3~64字符。
权重分配	填写服务器分组的权重值，权重值越大，转发到该分组下服务器的请求数量越多。默认：1，取值范围为0~100。 **分发算法**选择哈希算法时，权重默认为1，且不支持修改。
被引用的负载通道	选择需要引用的负载通道。
描述	填写分组的描述信息。

配置完成后，进行**健康检查配置**。

步骤9 配置健康检查。

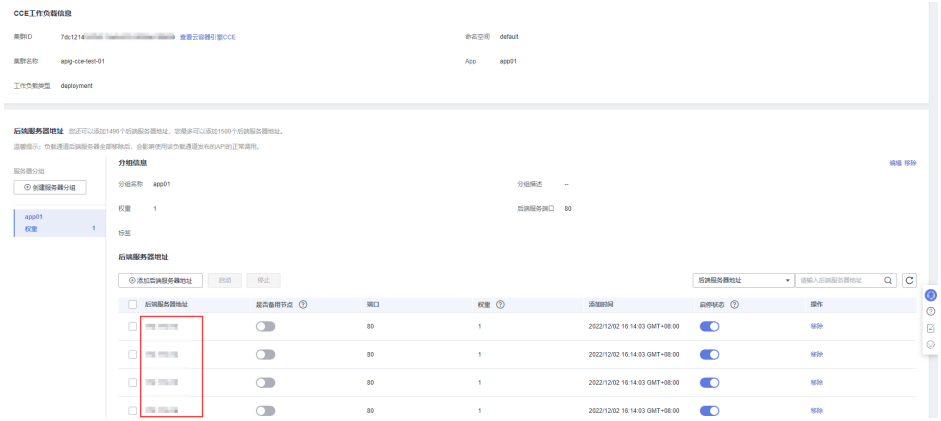
表 4-10 基本信息配置

参数	说明
协议	使用以下协议，对负载中主机执行健康检查。 ● TCP ● HTTP ● HTTPS 默认为TCP协议。
双向认证	**仅在协议为“HTTPS”时，需要设置。** 开启后，API网关将认证API后端服务。双向认证所需的证书配置说明，请参考**配置参数**。
路径	**仅在协议不为“TCP”时，需要设置。** 健康检查时的目标路径。
请求类型	● GET ● HEAD
检查端口	健康检查的目标端口。 缺省时，检查端口为负载通道的端口号。
正常阈值	判定负载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。 取值范围为2 ~ 10。缺省值为2。
异常阈值	判定负载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。 取值范围为2 ~ 10。缺省值为5。
超时时间	检查期间，无响应的时间，单位为秒。 取值范围为2 ~ 30。缺省值为5。
间隔时间	连续两次检查的间隔时间，单位为秒。 取值范围为5 ~ 300。缺省值为10。
HTTP响应码	**仅在协议不为“TCP”时，需要设置。** 检查目标HTTP响应时，判断成功使用的HTTP响应码。

步骤10 单击“完成”，完成负载通道的创建。

如果通道类型为微服务，CCE工作负载的“实例IP”变更（增删改），“后端服务器地址”会同步变更。

图 4-2 微服务类型负载通道详情



----结束

后续操作

1. 确认APIG实例已添加路由。**通过同一个VPC（有扩展网段等）、对等连接等方式连接CCE负载与APIG实例的网络时，需要添加路由。**
   a. 进入云容器引擎控制台，在“集群管理”页面单击已创建的CCE集群名称。
   b. 在“总览”页面的“网络信息”区域查看“容器网段”，并记录。
   c. 进入API网关控制台，在“实例管理”页面单击对应的实例名称。
   d. 在“实例信息”页面的“路由”区域查看已添加的路由与容器网段是否一致。如果不一致，请添加。
2. **创建API**，将部署在负载中的后端服务开放API。

相关文档

使用API网关开放云容器引擎CCE工作负载

4.6 创建 API

4.6.1 通过 APIG 创建 REST API

REST API（Representational State Transfer Application Programming Interface）是基于HTTP协议，通过对API的操作来实现客户端和服务器之间的通信，一种用于构建网络应用程序的软件架构风格。它广泛应用于Web开发、移动应用程序开发和云服务等领域，成为了现代应用程序开发的重要组成部分。

API的开放和调用需要遵循RESTful相关规范，创建REST API分以下步骤：

- **配置API的前端信息**
  支持配置前端定义、安全配置和请求参数。
- **配置API的后端信息**
  支持配置默认后端、策略后端和返回结果。

前提条件

- 已创建API分组。如果未创建API分组，请**创建API分组**。
- 如果后端服务需要使用负载通道，请**创建负载通道**。
- 如果需要使用自定义认证方式进行API的安全认证，请**创建自定义认证**。

配置 API 的前端信息

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面，单击“创建API > 创建API”。

1. 根据下表参数信息，配置前端定义。

   说明

   创建API时，当API所属分组、请求方法、请求路径、匹配模式都重复时，API无法创建成功。

表 4-11 前端定义

参数	说明
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。 支持中文、英文、数字、中划线、下划线、点、斜杠、中英文格式下的小括号和冒号、中文格式下的顿号，且只能以英文、中文和数字开头，长度为3~255个字符。
所属分组	API所属的分组。选择已有的分组，如果需要新建分组，单击“**新建分组**”即可创建。
URL	前端地址由请求方法、请求协议、子域名和路径组成。 – 请求方法：GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY。其中ANY表示该API支持任意请求方法。 – 请求协议：HTTP、HTTPS、HTTP&HTTPS，传输重要或敏感数据时推荐使用HTTPS。 API网关支持WebSocket数据传输，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。 – 子域名：所在分组的调试域名。 – 路径：API的请求路径。请求路径可以包含请求参数，请求参数使用{}标识，例如/a/{b}，也可以通过配置“+”号做前缀匹配，例如：/a/{b+}。注意，请求路径中的字母区分大小写。

参数	说明
网关响应	网关响应指未能成功处理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。
匹配模式	选择API请求路径的匹配模式。 – 绝对匹配：API请求中的请求路径要与“路径”的配置一致。 – 前缀匹配：API请求中的请求路径要以“路径”的配置为前缀。前缀匹配支持接口定义多个不同Path。例如，“路径”为/test/AA，使用前缀匹配时，通过/test/AA/BB和/test/AA/CC都可以访问API，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。 – 使用前缀匹配时，以最长路径优先规则匹配。例如，两个API都开启前缀匹配，“路径”为/test/AA和/test/AA/BB，请求/test/AA/BB/c会匹配路径为/test/AA/BB的API。 – 当两个API的所属分组、请求方法、请求路径都相同时，优先调用匹配模式为绝对匹配的API。
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。 支持英文，数字，中文，_-*#%.:，且只能以英文，中文开头，长度为1~128个字符。支持输入多个标签，不同标签以英文逗号分隔。
描述	API的描述。长度为1~1000个字符。
内容格式类型	是否开启API请求的内容格式类型，开启后APIG会按照选择的内容格式类型向后端传输API请求。长度为1~20480个字符。 支持选择“application/json”、“application/xml”、“text/plain”和“multipart/form-data”。选择内容格式类型前，请确保后端服务支持待选择的内容格式类型。
请求体内容描述	填写API请求中请求体的描述信息，用于帮助API调用者理解如何正确封装API请求。

参数	说明
请求体Base64编码	对与FunctionGraph交互场景的Body体进行Base64编码，默认开启。**仅当满足以下任意条件时，Base64编码才生效：** - **自定义认证** - **后端配置为FunctionGraph类型** - **绑定断路器策略，且断路器后端降级策略FunctionGraph类型** 如需关闭Base64编码，仅当内容格式类型为“application/json”时才可关闭。

2. 根据下表参数信息，配置安全配置。

表 4-12 安全配置

参数	说明
类型	API类型： - 公开：选择“公开”类型时，API支持上架。 - 私有：选择“私有”类型时，当该API所在分组上架时，该API不会上架。
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。推荐使用APP认证方式。 - 华为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。API网关对收到的调用请求不做身份认证，只需要按照API提供者提供的接口说明，封装规范的请求，发送给API网关即可。API网关把请求内容**透传**给后端服务。因此，如果您希望在API后端服务进行鉴权，可以使用“无认证”方式，API调用方传递鉴权所需字段给后端服务，由后端服务进行鉴权。 各种认证方式下的API调用稍有不同，具体请参考**调用APIG开放的API**。 **须知** - 认证方式为华为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。

参数	说明
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。 注意支持HTTPS方式调用，不支持HTTP方式。具体使用请参考**配置APIG的API简易认证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APIG创建的API**发布。
支持双重认证	**仅当“安全认证”选择“APP认证”或“华为IAM认证”时可配置。** 是否对API的调用进行双重安全认证。如果选择启用，则在使用APP认证或IAM认证对API请求进行安全认证时，同时使用自定义的函数API对API请求进行安全认证。
自定义认证	**仅当“安全认证”选择“自定义认证”时需要配置。** 选择已创建的前端类型自定义认证。若没有可用的自定义认证，可单击右侧的“新建自定义认证”，创建一个前端类型的自定义认证。
支持跨域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“请求方法”为“OPTIONS”的API，具体操作请参考**开启跨域访问**。

3. （可选）根据实际需要定义API的请求参数，请求参数定义见下表。

   说明

   建议不要设置敏感信息，防止泄露。

表 4-13 请求参数

参数	说明
参数名	参数的名称，如果参数在“Path”位置，参数名称会同步“路径”中的名称。 支持英文，数字，点，中划线，下划线，且只能以英文开头，长度为1-32个字符。 – 参数名不能以x-apig- 、x-sdk-开头，不能是x-stage，不区分大小写。 – 参数位置为HEADER时，API认证为IAM认证的API的参数名不能是“Authorization”和“X-Auth-Token”，API认证为APP认证的API的参数名不能是“Authorization”。不区分大小写。
参数类型	字段的类型，包含STRING和NUMBER。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。
透传	请求参数是否透传到后端服务。
枚举	请求参数的枚举值，请求参数的值只能从枚举值中选择，多个枚举值间用英文逗号隔开。
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。
编排规则	选择编排规则。创建编排规则请参考**配置API的参数编排规则**。
字节限制	– 最大长度/最大值：“类型”为“STRING”时，设置参数值的最大字符串长度，“类型”为“NUMBER”时，设置参数值的最大值。 – 最小长度/最小值：“类型”为“STRING”时，设置参数值的最小字符串长度，“类型”为“NUMBER”时，设置参数值的最小值。
示例	参数值的填写示例。
描述	对于此参数的描述。

步骤6 单击“下一步”，进入**配置API的后端信息**。

----结束

配置 API 的后端信息

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“后端配置”页面，选择API后端服务类型。

后端服务类型有HTTP&HTTPS、FunctionGraph和Mock，具体参数描述见**表4-14**、**表4-15**、**表4-16**。

说明

- FunctionGraph依赖于函数工作流服务FunctionGraph，如果当前环境中未部署FunctionGraph服务，则后端服务类型FunctionGraph不可用。
- 在后端服务还不具备的场景下，可以使用Mock模式，将预期结果固定返回给API调用方，方便调用方进行调试验证。

表 4-14 HTTP&HTTPS 类型定义后端服务

参数	说明
负载通道	是否使用负载通道访问后端服务。

参数	说明
URL	URL地址由请求方法、请求协议、负载通道/后端服务地址和路径组成。 • 请求方法 GET、POST、DELETE、PUT、PATCH、HEAD、OPTIONS、ANY，其中ANY表示该API支持任意请求方法。 • 请求协议 HTTP或HTTPS，传输重要或敏感数据时推荐使用HTTPS。 – API网关支持WebSocket数据传输，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。 – 定义的后端服务协议须与用户的后端业务协议保持一致。 • 负载通道 **仅在使用负载通道时，需要设置**。选择已创建的负载通道名称，或者**新建负载通道**。 **负载通道中，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。** • 后端服务地址 **仅在不使用负载通道时，需要设置**。 填写后端服务的访问地址，格式：“主机:端口”。主机为后端服务的访问IP地址/域名；端口为后端服务的端口。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。 如果后端服务地址中需要携带环境变量，则使用“#变量名#”的形式将环境变量添加到后端服务地址中，如#ipaddress#。支持添加多个环境变量，如#ipaddress##test#。 **说明** IP地址/域名可以是公网IP（支持云服务器的弹性IP地址、用户自己服务器的公网IP地址、ELB地址）/公网域名，前提需要开启实例的公网出口。可以是内网的IP，不可以是内网域名。 2022年10月30日后创建的实例支持APIG与后端服务tls握手阶段向后端服务传SNI。 • 路径 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#。

参数	说明
	说明 • 在URL中配置了变量标识后，在API调试页面将无法调试。 • 如果在URL中设置变量，那么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。 • 变量名严格区分大小写。
自定义host头域	**仅在使用负载通道时，可设置。** 自定义后端服务请求中的Host头域，默认使用请求中原始的host头域。
后端超时(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms。 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。 **说明** 如果当前的超时时间范围不能满足实际业务需求，请在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。如果您修改了超时时间上限，需要同步修改此处的超时时间。
重试次数	后端服务请求失败后的重试次数，默认值为0，取值范围-1~10。 • 值为-1时，表示不开启重试功能，但除POST和PATCH外的其他请求类型会默认重试1次。 • 值为0~10时，表示开启重试功能，并根据设置的值执行重试。当值为0时，不重试。 **使用负载通道时**，重试次数应小于负载通道中已启用的后端服务器个数。
TLS双向认证	**仅在协议为“HTTPS”时，可设置。** 选择是否在API网关和后端服务间启用双向认证，如果选择“使用backend_client_certificate配置的证书做客户端认证”，您需在实例的**配置参数**中提前配backend_client_certificate证书。
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服务实现，在函数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** 后端认证依赖函数服务，此功能仅在部分区域开放。

表 4-15 FunctionGraph 类型定义后端服务

参数	说明
函数名	添加函数后，函数名自动生成。

参数	说明
函数URN	函数请求唯一标识。 单击“添加”，添加所需的函数URN。
版本或别名	选择函数的版本或别名，函数的版本或别名功能请参考**版本管理**章节或**别名管理**章节。
调用类型	选择函数的调用类型。 • Synchronous：同步调用。指后端函数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(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms。 • 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。 • 如果当前的超时时间范围不能满足实际业务需求，请在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。如果您修改了超时时间上限，需要同步修改此处的超时时间。
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服务实现，在函数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** 后端认证依赖函数服务，此功能仅在部分区域开放。

表 4-16 Mock 类型定义后端服务

参数	说明
Mock自定义返回码	选择API响应的HTTP状态码。
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	当您的后端服务需要对API调用增加自己的认证，则开启后端认证。 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服务实现，在函数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** 后端认证依赖函数服务，此功能仅在部分区域开放。

参数	说明
添加header参数	自定义API响应的header参数。 单击“添加header参数”，并填写参数名、参数值和参数描述。

步骤2 （可选）配置默认后端的后端服务参数，将调用API时传入的请求参数映射到后端服务请求的对应位置。如果5.3中未定义请求参数，可直接跳过此步骤。

1. 在“后端服务参数”下，可通过以下任意一种方法添加后端服务参数。
   - 单击“导入入参定义”，把所有已定义的API请求参数添加到后端服务参数。
   - 单击“添加后端参数映射”，按需逐个添加后端服务参数。
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4-3所示。

图 4-3 配置后端服务参数

   a. 后端参数在“PATH”位置，那么参数名称需要和“路径”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，也不支持下划线开头。

   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。

      假设test01为aaa，test02为bbb，test03为ccc。

      API调用请求：

      ```
      curl -ik -H 'test02:bbb' -X GET https://example.com/v1.0/aaa?test03=ccc
      ```

      后端服务请求：

      ```
      curl -ik -H 'test01:aaa' -H 'test03:ccc' -X GET https://example.com/v1.0/bbb
      ```

步骤3 （可选）配置默认后端的常量参数。如果后端服务需要接收固定的常量信息，可以通过设置常量参数来实现。API网关向后端服务发送请求时，将常量参数添加到请求的指定位置，然后将请求发送给后端服务。

在“常量参数”下，单击“添加常量参数”，添加后端服务请求的常量参数。

须知

常量参数会明文展示，为防止信息泄露，请谨慎配置。

表 4-17 常量参数配置

参数	说明
常量参数名	填写常量参数的名称。“参数位置”为“PATH”时，参数名需要与“路径”中的参数名称一致。 **说明** • 参数名不能以x-apig- 、x-sdk-开头，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开头，不区分大小写。
参数位置	选择常量参数在后端服务请求中的位置，可选择“PATH”、“HEADER”和“QUERY”。
参数值	填写常量参数的值。
描述	填写常量参数的描述信息。

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[api]，在百分号编码后变为%5Bapi%5D。
- 对于PATH位置的参数值，API网关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。
- 对于QUERY位置的参数值，API网关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4 （可选）配置默认后端的系统参数。如果后端服务需要接收系统运行时产生的参数信息，如网关内置参数、前端认证参数和后端认证参数等，可以通过设置系统参数来实现。API网关向后端服务发送请求时，将系统参数添加到请求的指定位置，然后将请求发送给后端服务。

1. 在“系统参数”下，单击“添加系统参数”，根据下表参数说明，添加后端服务请求的系统参数。

表 4-18 系统参数配置

参数	说明
系统参数类型	选择系统参数的类型。 – 网关内置参数：支持配置的系统参数。 – 前端认证参数：前端自定义认证返回结果中的参数。在**配置API的前端信息**中，“安全认证”选择“自定义认证”或使用双重认证时，才可以选择此参数。 – 后端认证参数：后端自定义认证返回结果中的参数。在**配置API的后端信息**中，“后端认证”开启时，才可以选择此参数。
系统参数名	填写系统参数的名称。 – “系统参数类型”为“网关内置参数”时，支持选择如下参数： ▪ sourceIp：API调用者的源地址。 ▪ stage：API调用的部署环境。 ▪ apiId：API的ID。 ▪ appId：API调用者的APP ID。 ▪ requestId：当次调用API所生成的请求ID。 ▪ serverAddr：网关服务器的地址 。 ▪ serverName：网关服务器的名称。 ▪ handleTime：本次调用API的处理时间。 ▪ providerAppId：API提供者的凭据ID。 ▪ apiName：API的名称，需要发布API后才可使用此参数。 ▪ appName：调用API所使用的凭据名称。 ▪ clientCertCN：开启客户端认证时，API请求携带的客户端证书中的CN（Common Name）字段。 – 系统参数类型为“前端认证参数”或“后端认证参数”时，支持自定义参数，但是此参数必须为自定义认证返回结果中的参数。 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**创建用于前端自定义认证的函数**。

参数	说明
后端参数名称	填写系统参数需要映射的后端参数名称。 **说明** – 参数名不能以x-apig- 、x-sdk-开头，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开头，不区分大小写。
后端参数位置	选择后端参数在后端服务请求中的位置，可选择“PATH”、“HEADER”和“QUERY”。
描述	填写系统参数的描述信息。

步骤5 （可选）添加策略后端。

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 添加策略后端。
2. 后端策略增加的参数，具体如**表4-19**所示，其他参数说明参考**表4-14**、**表4-15**和**表4-16**。

表 4-19 后端策略参数

参数	说明
后端策略名称	您自定义的名称，用于识别不同的后端策略。 支持英文、数字、下划线和中划线，只能以英文字母开头，长度为3~64个字符。
生效方式	选择策略后端的生效方式。 – 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	添加后端策略生效的条件，具体如**表4-20**所示。

表 4-20 策略条件

参数	说明
条件来源	策略条件中判断条件的来源。 – 源地址：以访问API的请求地址作为策略条件。 – 请求入参：以请求入参参数作为策略条件。 – Cookie：以API请求的Cookie信息作为判断条件。 – 系统参数-网关内置参数：以网关内置参数作为策略条件。网关内置参数指API网关处理API请求时的系统运行时参数信息。 – 系统参数-前端认证参数：以前端自定义认证返回结果中的参数作为策略条件。在**配置API的前端信息**中，“安全认证”选择“自定义认证”或使用双重认证时，才可以选择此参数。 **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。 – 如果未展示“系统参数”请联系技术支持升级实例。
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。 – 当“条件来源”为“系统参数”时，需要选择参数名称。 ▪ reqPath：请求URI，如“/a/b/c”。 ▪ reqMethod：请求方法，如“GET”。 – 当“条件来源”为“COOKIE”时，需要填写Cookie中的参数名称。支持英文、数字、点、下划线和中划线，长度为1-255个字符。
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	选择条件的判断类型，仅在“条件来源”为“请求入参”、“系统参数”、“COOKIE”时需要配置。 – 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。 **说明** 当“条件来源”为“系统参数”并且“参数名称”为“reqMethod”时，“条件类型”仅支持选择相等或枚举。

参数	说明
条件值	填写判断条件的值，长度为1~1024个字符。 – “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。 – “条件来源”为“系统参数-前端认证参数”时，且当条件值填写boolean类型时，需全部小写。

步骤6 定义返回结果。

在“返回结果基础定义”区域，根据下表参数说明，填写返回信息。

表 4-21 定义返回结果

参数	说明
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7 单击“完成”，进入“API运行”页面，可查看API详情。

----结束

创建 API 相关的 FAQ

API网关是否支持多后端节点方案?

为什么后端服务调用失败?

在API网关中创建完成API，调用时报“No backend available”错误，怎么解决?

后续操作

API创建完成后，通过**调试API**，验证服务是否正常。

4.6.2 通过 APIG 创建 GRPC API

API网关支持创建GRPC API。gRPC是RPC（远程过程调用）的一种，只需定义每个API的Request和Response，剩下的gRPC框架就可以完成。它的典型特征就是使用protobuf（protocol buffers）作为其接口定义语言（Interface Definition Language，缩写IDL），同时底层的消息交换格式也是使用protobuf。下表列出了GRPC API与REST API的区别：

表 4-22 GRPC 和 REST 区别

参数	GRPC	REST
消息编码	protobuf	JSON
传输协议	HTTP/2	HTTP
传输性能	传输内容少，速度快	传输内容多
传输形式	• 简单 RPC（Unary RPC） 发送单个请求，接收单个响应。 • 服务端流式 RPC（Server streaming RPC） 发送单个请求，接收多个响应。 • 客户端流式 RPC（Client streaming RPC） 发送多个请求，接收单个响应。 • 双向流式 RPC（Bi-directional streaming RPC） 发送多个请求，接收多个响应。	发送单个请求，接收单个响应。

当您的客户端和服务端都为GRPC类型时，可以通过创建GRPC类型的API来开放后端能力。GRPC适用于内部服务的调用，性能消耗低，传输率高，便于服务治理。

约束与限制

- 不支持API管理模块中的导入导出API功能、导入API设计文件、导入CSE微服务功能、导入CCE工作负载功能、调试API功能。
- 不支持后端降级策略中后端策略类型为Mock、HTTP&HTTPS、FunctionGraph的断路器策略。
- 不支持Base64编码配置。
- 不支持参数编排。

前提条件

- 已创建API分组。如果未创建API分组，请**创建API分组**。
- 如果后端服务需要使用负载通道，请**创建负载通道**。
- 后端服务已定义proto文件，即在proto文件中定义API的Request和Response。proto文件是用于定义数据结构和服务接口的文件，通常在gRPC中使用。它基于Protobuf语言，用于描述数据的结构和交互方式，充当客户端和后端服务之间通信的合同。

创建 GRPC API

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面，单击“创建API > 创建GRPC API”。

1. 根据下表参数信息，配置前端定义。

   创建API时，当API所属分组、请求方法、请求路径、匹配模式都重复时，API无法创建成功。

表 4-23 前端定义

参数	说明
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。 支持中文、英文、数字、中划线、下划线、点、斜杠、中英文格式下的小括号和冒号、中文格式下的顿号，且只能以英文、汉字和数字开头，长度为3~255个字符。
所属分组	API所属的分组。选择已有的分组，如果需要新建分组，单击“**新建分组**”即可创建。
URL	前端地址由请求方法、请求协议、子域名和路径组成。 – 请求方法：默认为POST。 – 请求协议：默认为GRPCS.。 – 子域名：所在分组的调试域名。 – 路径：需要根据实际业务从以下三种配置方式中选择配置。 ▪ / ▪ /{包名}.{服务名} ▪ /{包名}.{服务名}/{方法名} **说明** ▪ 包名、服务名、方法名从**proto文件**中获取。 ▪ 当前端路径设置“/{包名}.{服务名}/{方法名}”时，API的匹配模式才可以使用“绝对匹配”。
网关响应	网关响应指未能成功处理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。

参数	说明
匹配模式	选择API请求路径的匹配模式。 – 绝对匹配：API请求中的请求路径要与“路径”的配置一致。 – 前缀匹配：API请求中的请求路径要以“路径”的配置为前缀。前缀匹配支持接口定义多个不同Path。例如，“路径”为/test/AA，使用前缀匹配时，通过/test/AA/BB和/test/AA/CC都可以访问API，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。 – 使用前缀匹配时，以最长路径优先规则匹配。例如，两个API都开启前缀匹配，“路径”为/test/AA和/test/AA/BB，请求/test/AA/BB/c会匹配路径为/test/AA/BB的API。 – 当两个API的所属分组、请求方法、请求路径都相同时，优先调用匹配模式为绝对匹配的API。
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。 支持英文，数字，中文，_-*#%.:，且只能以英文，中文开头，长度为1~128个字符。支持输入多个标签，不同标签以英文逗号分隔。
描述	API的描述，长度为1~1000个字符。
请求体内容描述	填写API请求中请求体的描述信息，用于帮助API调用者理解如何正确封装API请求。

2. 根据下表参数信息，配置安全配置。

表 4-24 安全配置

参数	说明
类型	API类型： – 公开：选择“公开”类型时，API支持上架。 – 私有：选择“私有”类型时，当该API所在分组上架时，该API不会上架。

参数	说明
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。推荐使用APP认证方式。 – 华为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。API网关对收到的调用请求不做身份认证，只需要按照API提供者提供的接口说明，封装规范的请求，发送给API网关即可。API网关把请求内容**透传**给后端服务。因此，如果您希望在API后端服务进行鉴权，可以使用“无认证”方式，API调用方传递鉴权所需字段给后端服务，由后端服务进行鉴权。 各种认证方式下的API调用稍有不同，具体请参考**调用APIG开放的API**。 **须知** – 认证方式为华为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GRPC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。 注意支持GRPCS方式调用，不支持GRPC方式。具体使用请参考**配置APIG的API简易认证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APIG创建的API**发布。
支持双重认证	**仅当“安全认证”选择“APP认证”或“华为IAM认证”时可配置。** 是否对API的调用进行双重安全认证。如果选择启用，则在使用APP认证或IAM认证对API请求进行安全认证时，同时使用自定义的函数API对API请求进行安全认证。
自定义认证	**仅当“安全认证”选择“自定义认证”时需要配置。** 选择已创建的前端类型自定义认证。若没有可用的自定义认证，可单击右侧的“新建自定义认证”，创建一个前端类型的自定义认证。

参数	说明
支持跨域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GRPC查询请求。 开启CORS（非简单请求）时，您需要单独创建一个“请求方法”为“OPTIONS”的API，具体操作请参考**开启跨域访问**。

步骤6 单击“下一步”，配置后端服务。

步骤7 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“后端配置”页面，选择API后端服务类型。

后端服务类型有**表4-25**、**表4-26**。

说明

FunctionGraph依赖于函数工作流服务FunctionGraph，如果当前环境中未部署FunctionGraph服务，则后端服务类型FunctionGraph不可用。

GRPC API的后端FunctionGraph类型，当前仅贵阳一、上海一、北京四、上海二、圣地亚哥区域支持。

表 4-25 GRPC&GRPCS 类型定义后端服务

参数	说明
负载通道	是否使用负载通道访问后端服务。

参数	说明
URL	URL地址由请求方法、请求协议、负载通道/后端服务地址和路径组成。 ● 请求方法 默认为POST。 ● 请求协议 支持“GRPC”或“GRPCS”。定义的后端服务协议须与用户的后端业务协议保持一致。 ● 负载通道 **仅在使用负载通道时，需要设置**。选择已创建的负载通道名称，或者**新建负载通道**。 **负载通道中，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。** ● 后端服务地址 **仅在不使用负载通道时，需要设置**。 填写后端服务的访问地址，格式：“主机:端口”。主机为后端服务的访问IP地址/域名；端口为后端服务的端口。未指定端口时，GRPC协议默认使用80端口，GRPCS协议默认使用443端口。 如果后端服务地址中需要携带环境变量，则使用“#变量名#”的形式将环境变量添加到后端服务地址中，如#ipaddress#。支持添加多个环境变量，如#ipaddress##test#。 **说明** IP地址/域名可以是公网IP（支持云服务器的弹性IP地址、用户自己服务器的公网IP地址、ELB地址）/公网域名，前提需要开启实例的公网出口。可以是内网的IP，不可以是内网域名。 2022年10月30日后创建的实例支持APIG与后端服务tls握手阶段向后端服务传SNI。 ● 路径 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#。 **说明** ● 在URL中配置了变量标识后，在API调试页面将无法调试。 ● 如果在URL中设置变量，那么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。 ● 变量名严格区分大小写。
自定义host头域	**仅在使用负载通道时，可设置**。 自定义后端服务请求中的Host头域，默认将使用请求中原始的host头域。

参数	说明
后端超时(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms。 • 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。 • 如果当前的超时时间范围不能满足实际业务需求，请在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。如果您修改了超时时间上限，需要同步修改此处的超时时间。
重试次数	后端服务请求失败后的重试次数，默认值为0，取值范围-1~10。 • 值为-1时，表示不开启重试功能，但除POST和PATCH外的其他请求类型会默认重试1次。 • 值为0~10时，表示开启重试功能，并根据设置的值执行重试。当值为0时，不重试。 **使用负载通道时**，重试次数应小于负载通道中已启用的后端服务器个数。
TLS双向认证	**仅在协议为“GRPCS”时，可设置。** 选择是否在API网关和后端服务间启用双向认证，如果选择“使用backend_client_certificate配置的证书做客户端认证”，您需在实例的**配置参数**中提前配backend_client_certificate证书。
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服务实现，在函数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** 后端认证依赖函数服务，此功能仅在部分区域开放。

表 4-26 FunctionGraph 类型定义后端服务

参数	说明
函数名	添加函数后，函数名自动生成。
函数URN	函数请求唯一标识。 单击“添加”，添加所需的函数URN。
版本或别名	选择函数的版本或别名，函数的版本或别名功能请参考**版本管理**章节或**别名管理**章节。
调用类型	默认为Synchronous，同步调用。指后端函数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。

参数	说明
后端超时(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms。 • 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。 • 如果当前的超时时间范围不能满足实际业务需求，请在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。如果您修改了超时时间上限，需要同步修改此处的超时时间。
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服务实现，在函数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** 后端认证依赖函数服务，此功能仅在部分区域开放。

步骤8 （可选）添加策略后端。

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 添加策略后端。
2. 后端策略增加的参数，具体如**表4-27**所示，其他参数说明参考**表4-25**、**表4-26**。

表 4-27 后端策略参数

参数	说明
后端策略名称	您自定义的名称，用于识别不同的后端策略。 支持英文、数字、下划线和中划线，只能以英文字母开头，长度为3-64个字符。
生效方式	选择策略后端的生效方式。 – 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	添加后端策略生效的条件，具体如**表4-28**所示。

表 4-28 策略条件

参数	说明
条件来源	策略条件中判断条件的来源。 – 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。 – Cookie：表示以API请求的Cookie信息作为判断条件。 – 系统参数：以网关内置参数作为策略条件来源。网关内置参数指API网关处理API请求时的系统运行时参数信息。 **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。 – 如果未展示“系统参数”请联系技术支持升级实例。
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。 – 当“条件来源”为“系统参数”时，需要选择参数名称。 ▪ reqPath：请求URI，如“/a/b/c”。 ▪ reqMethod：请求方法，如“GET”。 – 当“条件来源”为“COOKIE”时，需要填写Cookie中的参数名称。
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”、“系统参数”、“COOKIE”时需要配置。 – 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。 **说明** 当“条件来源”为“系统参数”并且“参数名称”为“reqMethod”时，“条件类型”仅支持选择相等或枚举。

参数	说明
条件值	填写判断条件的值，条件值的长度为1~1024个字符。 - “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。 - “条件来源”为“系统参数-前端认证参数”时，且当条件值填写boolean类型时，需全部小写。

步骤9 单击“完成”，进入“API运行”页面，可查看API详情。

----结束

相关文档

基于API网关实现gRPC服务的路由转发

4.7 调试 APIG 创建的 API

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。

约束与限制

- 后端路径中含有环境变量的API，不支持调试。
- 如果API绑定了**插件策略**或**传统策略**，在调试API时，策略均不生效。
- 调试API时，后端超时时间最大支持60s。

前提条件

已**创建API**。

调试 API

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页签，选择待调试的API，单击“调试”。

步骤6 配置URL和API请求参数。

选择请求方法、请求协议、域名等，然后配置API请求参数。

域名可选调试域名或独立域名。当选择的独立域名为泛域名时，需要填写泛域名的子域名。

说明

当独立域名为泛域名时，用户可以通过泛域名的所有子域名访问所绑定分组下的所有API。
例如，某个泛域名为“*.aaa.com”，子域名可以为“default.aaa.com”和 “1.aaa.com”等。

步骤7 单击“调试”。

步骤8 在页面下方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“2*xx*”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**APIG的API错误码说明**。

步骤9 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。

----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添加策略**。

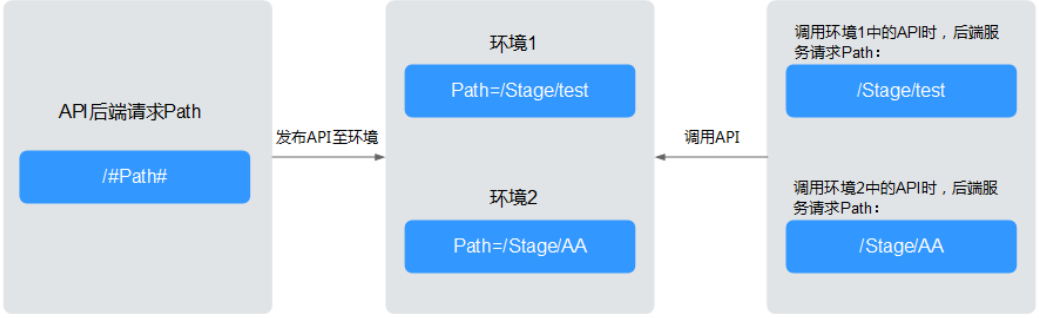
4.8 配置 API 的发布环境和环境变量（可选）

环境是指API的受限使用范围，API只有在发布到环境后，才能被调用。API可以被发布到不同的自定义环境中，如开发环境、测试环境等。RELEASE是系统默认的发布环境，也是正式发布环境。

环境变量是指在环境上创建的一种变量，该变量固定在环境上。如果API的后端服务信息中定义了环境变量，则需要在环境中添加对应的变量。通过环境变量，可实现同一个API，在不同环境中调用不同的后端服务。

例如创建API时，后端服务请求Path中定义了变量“Path”。在环境1中创建了变量“Path”，变量值“/Stage/test”，则API在发布到环境1时，使用“/Stage/test”代替“Path”，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“Path”，变量值“/Stage/AA”，则API在发布到环境2时，使用“/Stage/AA”代替“Path”，在环境2中调用此API时，后端服务请求Path为“/Stage/AA”。

图 4-4 环境变量示意图



创建环境

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 单击“环境管理”页签。

步骤5 单击“创建环境”，根据下表参数说明，填写环境信息。

表 4-29 环境信息

参数	说明
环境名称	API环境名称。支持英文，数字，下划线，且只能以英文开头，长度为3-64个字符。
描述	环境描述信息。长度为1-255个字符。

步骤6 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。

用户调用开放的API时，默认是调用RELEASE环境的API。如果要访问其他环境上的API，需要在API请求中添加Header参数“X-Stage”，参数值为环境名。例如要访问环境名为“Develop”上的API，则在API请求的Header参数中添加“X-Stage: Develop”。

----结束

创建环境变量

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“环境变量”区域，选择环境。如果未创建环境，可单击“创建环境”创建。

步骤6 单击“添加环境变量”，根据下表参数说明，填写变量信息。

须知

- 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。
- 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。

表 4-30 新增变量

参数	说明
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。在API定义中等于#Name值#部分（区分大小写），发布到环境里的API被变量值替换。 支持英文、数字、英文格式的下划线、中划线，必须以英文字母开头，长度为3-32个字符。
变量值	环境变量的值，支持英文、数字、英文格式的下划线、中划线、斜线、点、冒号，长度为1~255个字符。

步骤7 单击“确定”，创建完成。

----结束

后续操作

您可以将API**发布到环境**，以便API调用者调用。

4.9 发布 APIG 创建的 API

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。

约束与限制

- 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。

发布 API

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面，选择待发布的API，单击“发布最新版本”。

步骤6 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7 单击“确定”，API发布成功后，“发布最新版本”按钮左上角的红色感叹号消失。

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。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的用户后，选择待下线的API，单击“下线”即可。

----结束

查看 API 的发布历史

步骤1 在“API运行”页面，选择待查看发布历史的API。

步骤2 单击“更多 > 发布历史”。

步骤3 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4 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

发布 API 相关的 FAQ

对API的修改是否需要重新发布?

API发布到RELEASE环境可以正常访问，发布到非RELEASE环境无法访问?

API发布到不同环境后，会调用不同的后端服务吗?

后续操作

API发布完成后，您或API调用者就可以**调用API**了。如果您提供的是APP认证方式的API，还需要**配置API调用授权（可选）**才可调用API。

5 配置 API 调用授权（可选）

5.1 API 调用授权概述

API调用者在调用使用**APP认证**方式的API时，可以通过用凭据进行API认证或AppCode进行简易的API认证。您可以根据业务需求选择其中一种进行认证，下文介绍具体两种认证方式的配置。

- **配置APIG的API认证凭据**

  在API网关中创建一个凭据，生成密钥对（Key、Secret），在调用API时，API网关服务根据密钥对进行身份核对，完成鉴权。Key唯一且不可重置，支持**重置Secret**。

- **配置APIG的API简易认证AppCode**

  API配置简易认证模式后，在调用API时，API网关服务既可以根据AppCode进行简易认证，也可以根据密钥对进行鉴权。

5.2 配置 APIG 的 API 认证凭据

使用APP认证的API，需要在API网关中创建一个凭据，以生成凭据ID和密钥对（Key、Secret）。将创建的凭据绑定API后，才可以使用APP认证调用API。客户端（API调用者）在调用API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、华为IAM认证的API、自定义认证，无需创建凭据。

约束与限制

- 每个实例最多创建50个凭据，每个凭据最多绑定1000个API。
- 一个凭据可以绑定多个APP认证的API，一个APP认证的API可以绑定多个凭据。

创建凭据

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击“创建凭据”，根据下表参数说明，填写凭据信息。

表 5-1 凭据信息

参数	说明
凭据名称	凭据的名称。支持英文、中文、数字、下划线，且只能以英文或中文开头，长度为3~64个字符。
描述	对凭据的介绍。长度为1~255个字符。

说明

支持AppKey（Key）和AppSecret（Secret）自定义配置。AppKey是身份标识，需要保证全局唯一。如果没有特殊需求，不建议使用“自定义配置”，系统会默认生成全局标识，可在凭据详情中查看。

步骤5 单击“确定”，创建凭据。

- 创建凭据成功后，在凭据管理页面显示新建凭据和凭据ID。
- 单击凭据名称，进入详情页面，查看key和Secret。

----结束

绑定 API/授权 API

绑定API或授权API就是将API与凭据关联起来，APIG可以根据凭据的密钥对进行身份鉴权，调用关联的API。

绑定API

步骤1 在“凭据管理”页面，单击凭据名称，进入详情页面。

步骤2 在“关联API”区域，单击“绑定API”。

步骤3 选择授权环境、API分组和API。

步骤4 单击“确定”。

如需解绑API，在API所在行单击“解绑”即可。

授权API

步骤5 在左侧导航栏选择“API管理 > API分组”。

步骤6 单击分组名称，进入“分组信息”页面。

步骤7 在“API运行”页面，选择待授权的API，单击“更多 > 授权”。

步骤8 单击“添加授权”。

步骤9 选择API授权环境，查询并勾选凭据后，单击“确定”。在“授权历史”弹窗中展示已授权的凭据。

如果已授权的凭据需要解除授权，在凭据列表中凭据所在行单击“解除授权”。

----结束

重置 Secret

Key唯一且不可重置，Secret支持重置，将Secret的值重新改变。重置完成后，原先的Secret将失效，绑定此凭据的API将无法调用，请更新SDK中的密钥对，并重新调用API。

步骤1 在左侧导航栏选择“API管理 > 凭据管理”。

步骤2 单击凭据名称，进入凭据详情页面。

步骤3 单击“重置Secret”。

步骤4 在弹窗中单击“确定”。

----结束

5.3 配置 APIG 的 API 简易认证 AppCode

简易认证指在调用API时，HTTP请求头部消息增加一个参数X-Apig-AppCode（参数值填凭据详情中“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Key和Secret做签名和校验，也可以选择使用AppCode进行简易认证。

约束与限制

- 为了确保安全，简易认证仅支持HTTPS或GRPCS方式调用API，不支持HTTP。
- 每个凭据最多可创建5个AppCode。

生成 AppCode

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击凭据名称，进入凭据详情页面。

步骤5 在“AppCodes”区域，单击“添加AppCode”。

步骤6 根据下表参数说明，在弹窗中配置AppCode，完成后单击“确定”。

表 5-2 配置 AppCode

参数	说明
生成方式	选择AppCode的生成方式。 • 自动生成：由系统随机生成AppCode。 • 手动输入：自定义AppCode。

参数	说明
AppCode	仅手动输入方式需要填写AppCode的值。支持英文、数字、+_!@#$%-/=，且只能以英文、数字和+、/开头，长度为64~180个字符。

----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绑定到已创建的凭据。

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

6 调用 API

6.1 调用 APIG 开放的 API

API提供者在API网关开放自己的API后，API调用者从API网关中调用API。

约束与限制

- 如果您使用调试域名（创建API分组时系统分配的调试域名）访问API，该调试域名每天最多可以访问1000次。
- 如果在API网关控制台“API管理 > API策略 > SSL证书管理”界面的“创建SSL证书”窗口中设置了“CA”参数，那么在调用API时，请注意以下限制。
  - 使用HTTP/1.0协议调用API时，不允许请求头中存在 "Transfer-Encoding"参数。
  - 不允许使用CONNECT请求方法。
  - 不允许请求头中同时存在参数"Content-Length"和"Transfer-Encoding"。
  - 不允许请求行中存在空格或控制符。
  - 不允许header name中存在空格或控制符。
  - 不允许请求头"Host"中存在空格或控制符。
  - 不允许请求头中存在多个"Host"。

前提条件

在调用API前，确保您的业务系统所在网络与API的访问域名或地址互通。

- 如果业务系统与API网关在相同VPC内时，可直接访问API。
- 如果业务系统与API网关在同一区域的不同VPC内时，可通过创建VPC对等连接，将两个VPC的网络打通，实现同一区域跨VPC访问API。具体步骤请参考**VPC对等连接说明**。
- 如果业务系统与API网关在不同区域的不同VPC内时，可通过创建云连接实例并加载需要互通的VPC，将两个VPC的网络打通，实现跨区域跨VPC访问API。具体步骤请参考**跨区域VPC互通**。
- 如果业务系统与API网关通过公网互通，请确保API网关已绑定弹性IP。

获取 API 的调用信息

在调用API前，您需要向API提供者获取API的调用信息。

- 获取凭据的Key和Secret：

  在API网关控制台选择“API管理 > 凭据管理”，在凭据列表中单击API所授权凭据的名称，进入凭据详情页面，获取凭据的Key和Secret。

- 获取认证签名所使用SDK：

  在API网关控制台选择“帮助中心”，在“SDK使用指引”页签中下载对应语言所使用SDK。

- 获取AppCode：

  在API网关控制台选择“API管理 > 凭据管理”，在凭据列表中单击API所授权凭据的名称，进入凭据详情页面，在“AppCodes”区域中获取AppCode。

- 获取API的请求信息

  在API网关控制台选择“API管理 > API列表”，在“API列表”页签中可获取API的“域名”、“请求方法”和“请求路径”。单击API的名称进入“API运行”页面，在“前端配置”或“后端配置”区域获取API基本信息。

- 获取API的认证信息

  根据API使用的安全认证方式不同，还要获取相关的请求认证信息，请根据下表说明获取。

认证方式	认证信息
APP认证（签名认证）	向API提供者获取该API所授权凭据的Key和Secret，以及认证签名所使用的SDK。
APP认证（简易认证）	向API提供者获取该API所授权凭据的AppCode。
APP认证（双重认证）	同时获取APP认证以及自定义认证所需的认证信息。
APP认证（app_api_key认证）	向API提供者获取该API所授权凭据的Key和Secret。
APP认证（app_secret认证）	向API提供者获取该API所授权凭据的Key和Secret。
APP认证（app_basic认证）	向API提供者获取该API所授权凭据的Key和Secret。
APP认证（app_jwt认证）	向API提供者获取该API所授权凭据的Key和Secret。
IAM认证（Token认证）	获取云服务平台的用户账号密码。
IAM认证（AK/SK认证）	获取云服务平台的用户账号的AK/SK，以及认证签名所使用的SDK。

认证方式	认证信息
IAM认证（双重认证）	同时获取IAM认证以及自定义认证所需的认证信息。
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。
第三方认证（API策略）	向API提供者获取请求参数中要携带的第三方认证信息。

调用 API

本章节仅提供请求地址和认证参数的配置指导，客户端的其他参数配置需要用户自行调整，如超时配置、SSL配置等。如果客户端参数配置错误会导致业务受损，建议参考业界标准进行配置。

说明

API调用支持长连接。但是需要适当使用长连接，避免占用太多资源。

1. 构造API请求，示例如下：

```
POST https://{Address}/{Path}?{Query}
{Header}

{
 {Body}
}
```

   - **POST**：请求方法，需替换为**获取API的调用信息**中获取的请求方法。
   - **{Address}**：请求地址，需替换为**获取API的调用信息**中获取的域名地址。

API调用场景	API请求参数配置
使用域名调用API	使用服务分配的调试域名或服务绑定的域名调用API，无需另外配置。
使用IP调用DEFAULT分组的API	API允许使用IP地址调用DEFAULT分组下的API，无需另外配置。

API调用场景	API请求参数配置
使用IP调用非DEFAULT分组的API	• 使用IP地址直接调用非DEFAULT分组下的APP认证的API： 1. 将实例的**配置参数**“app_route”和“app_secret”设置为“on”。开启“app_route”之后，同一凭据不能授权给相同请求路径和方法的API。 2. 在请求消息中添加Header参数“X-HW-ID”和“X-HW-APPKEY”，参数值为API所授权凭据的Key和Secret。 **须知** 使用简易认证（APP认证）调用API时，仅需在请求消息中添加Header参数“X-Apig-AppCode”和“host”即可。 • 使用IP地址直接调用非DEFAULT分组下的非APP认证的API，需要在请求消息中添加Header参数“host”。

- **{Path}**：请求路径，需替换为**获取API的调用信息**中获取的请求路径。
- **{Query}**：查询参数，可选，格式为“参数名=参数取值”，例如limit=10，多个查询参数之间使用“**&**”隔开。需根据**获取API的调用信息**中获取的请求参数进行设置。
- **{Header}**：请求头参数，格式为“参数名: 参数取值”，例如Content-Type: application/json。需根据**获取API的调用信息**中获取的请求参数进行设置。
- **{Body}**：请求消息体，JSON格式。需根据**获取API的调用信息**中获取的请求体内容描述进行设置。

2. 为API请求添加认证信息。

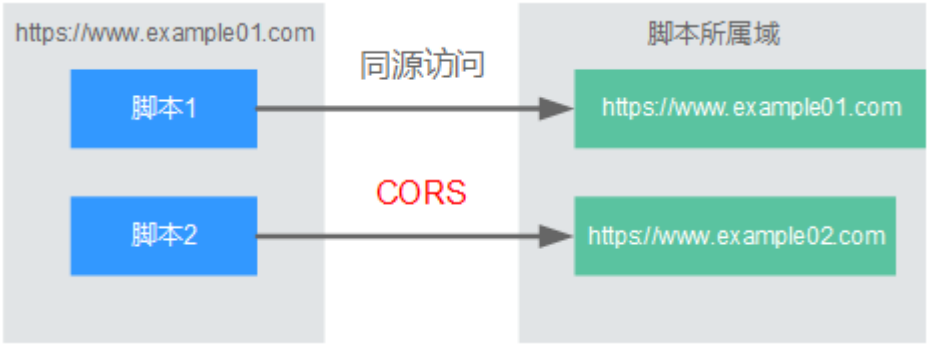
API认证方式	API请求参数配置
APP认证（签名认证）	使用获取的SDK对API请求进行签名，具体请参考**使用APP认证调用API**。
APP认证（简易认证）	在API请求中添加Header参数“X-Apig-AppCode”，参数值为**获取API的调用信息**中获取到的AppCode。具体请参考**快速入门**。
APP认证（app_api_key认证）	• 实例的**配置参数**“app_api_key”已设置为“on”，开启app_api_key认证。 • 在API请求中添加Header或Query参数“apikey”，参数值为**获取API的调用信息**中获取到的Key。
APP认证（app_secret认证）	• 实例的**配置参数**“app_secret”已设置为“on”，开启app_secret认证，且“app_api_key”已设置为“off”，关闭app_api_key认证。 • 在API请求中添加Header参数“X-HW-ID”，参数值为**获取API的调用信息**中获取到的Key。 • 在API请求中添加Header参数“X-HW-AppKey”，参数值为**获取API的调用信息**中获取到的Secret。

API认证方式	API请求参数配置
APP认证（app_basic认证）	• 实例的**配置参数**“app_basic”已设置为“on”，开启app_basic认证。 • 在API请求中添加Header参数“Authorization”，参数值为"Basic"+base64(appkey+":"+appsecret)，其中appkey和appsecret分别为**获取API的调用信息**中获取到的Key和Secret。
APP认证（app_jwt认证）	• 实例的**配置参数**“app_jwt”已设置为“on”，开启app_jwt认证。 • 在API请求中添加Header参数“Timestamp”，参数值为当前时间的Unix时间戳，单位为毫秒。 • 在API请求中添加Header参数“Authorization”，参数值为sha256(appkey+appsecret +timestamp)，且sha256加密后的字符串需为小写字母。其中appkey和appsecret分别为**获取API的调用信息**中获取到的Key和Secret，timestamp为当前时间的Unix时间戳，单位为毫秒。 • 在API请求中添加Header参数“X-HW-ID”，参数值为**获取API的调用信息**中获取到的Key。
APP认证（双重认证）	在API请求中同时携带APP认证和自定义认证的认证信息。
IAM认证（Token认证）	先获取云服务平台的认证Token，然后在API请求中添加Header参数“X-Auth-Token”，参数值为认证Token，具体请参考**Token认证**。
IAM认证（AK/SK认证）	使用获取的SDK对API请求进行签名，具体请参考**AK/SK认证**。
IAM认证（双重认证）	在API请求中同时携带IAM认证和自定义认证的认证信息。
自定义认证	根据自定义认证的定义，在API请求参数中携带相关认证信息进行认证。
无认证	无需认证，可直接调用API。
第三方认证（API策略）	向API提供者获取请求参数中要携带的第三方认证信息。

6.2 跨域调用 APIG 开放的 API

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 6-1 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。如需自定义跨域的请求头、跨域的请求方法和指定授权访问的域，请使用**配置API的跨域资源共享**。

- **简单请求的跨域访问**

  如果是创建新的API，在“安全配置”时，勾选“开启支持跨域（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**

  非简单请求的跨域访问可通过两种配置方式实现，选择其中一种配置即可。

  - 方式一：配置一个OPTIONS请求，作为预检请求。预检请求API的参数设置，操作详情请参考**非简单请求**。
  - 方式二：只需配置一个跨域资源共享策略并绑定API即可，配置详情请参考**配置API的跨域资源共享**。

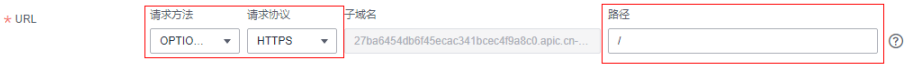
  a. 在“前端定义”中，参数填写说明如下：

  i. 请求方法：选择“OPTIONS”

  ii. 请求协议：选择与已开启CORS的API相同的请求协议

  iii. 路径：填斜杠/

  图 6-2 预检请求-定义 API 请求

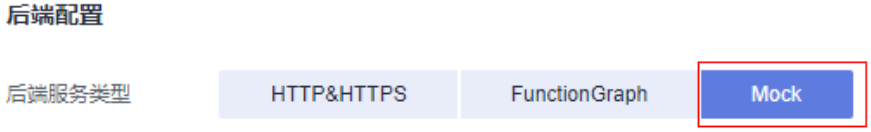


  b. 在“安全配置”中，安全认证选“无认证”，勾选“开启支持跨域CORS”。

  图 6-3 预检请求-使用无认证方式

  c. 后端配置选择“Mock”。

  图 6-4 预检请求-后端选 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
Origin: 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
Origin: 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“请求方法”为“OPTIONS”的API。

“请求方法”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。
- 请求方法：选择“OPTIONS”。
- 请求协议：选择与已开启CORS的API相同的请求协议。
- 路径：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。
- 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。
- 支持跨域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“请求方法”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
Origin: 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"}
```

6.3 APIG 的 API 响应消息头说明

调用API时，API网关增加下表中的响应消息头。

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
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。

响应消息头	描述
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	凭据流量限制信息。 示例：remain:9,limit:10,time:10 second 仅在请求消息头包含X-Apig-Mode: debug，且API配置了凭据流量限制时，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。
X-Apig-count	请求经过APIG的总次数。 经过APIG调用的合法请求都会返回此参数，当X-Apig-count请求头取值大于10时，会报错APIG.0612。

6.4 APIG 的 API 错误码说明

当调用API时，可能遇到下表中的错误码。如果遇到“APIGW”开头的错误码，请参见**API网关错误码**进行处理。

说明

- 通过APIG接口管理API，发生错误时，产生的错误码请参考**错误码**。
- 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 6-1 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	1. 检查调用API所使用的域名、请求方法、路径是否正确。 2. 检查API是否发布。 3. 检查域名解析是否正确。 4. 检查API是否使用OPTIONS跨域请求，如果使用OPTIONS跨域请求，请在API中开启CORS。 具体操作请参见**常见问题**。
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.0107	The custom lua script encountered an unexpected error	500	Lua脚本发生未知错误	联系技术支持。
APIG.0201	API request error.	400	请求格式不合法	检查请求格式是否合法。
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。

错误码	错误信息	HTTP状态码	语义	解决方案
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。
APIG.0201	Backend unavailable.	502	后端不可用	• 检查API配置的后端地址是否可用。 • 如果后端服务为ECS，ECS配置的安全组规则是否拦截了API请求。 • 请求协议是否正确。 • 后端服务链接链路是否可通。 具体操作请参见**常见问题**。
APIG.0201	Backend timeout.	504	后端超时	编辑API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与后端服务请求协议是否一致。
APIG.0203	Backend timeout	504	后端超时	编辑API增大超时时间，或缩小后端的处理时间。
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，当前支持TLS1.1和TLS1.2，推荐使用TLS1.2。
APIG.0205	Verify client certificate failed	400	客户端证书校验失败	检查客户端证书是否正确。

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0301	Incorrect IAM authentication information.	401	IAM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。请参见**常见问题**。
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。请参见**常见问题**。
APIG.0304	The app is not authorized to access the API.	403	APP不允许访问API	检查凭据是否绑定API，或API是否授权给凭据。
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。
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。如果触发调试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。

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.0312	Incorrect third-party authentication information,auth fail	401	第三方认证信息错误，认证失败	检查身份信息是否正确。
APIG.0313	Incorrect third-party authentication information,identities error	401	第三方认证信息错误，身份错误	检查请求中身份信息与第三方认证插件中身份来源设置是否一致。
APIG.0314	Incorrect third-party authentication information,access deny	403	第三方认证信息错误，访问拒绝	联系技术支持确认请求来源是否为业务请求，如果是，则提高第三方认证插件的防爆力拦截阈值以解决。
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API的访问控制限制。
APIG.0403	The IP address cannot be accessed.	403	IP地址不允许访问	检查IP地址是否被实例级访问控制限制。
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.0405	The app is not accessed from a trusted IP address.	403	未从受信任的IP地址访问应用程序	检查源IP是否在访问控制策略中配置了允许或者拒绝。
APIG.0501	The app quota has been used up.	405	APP已经超出配额	购买APP配额。
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。

错误码	错误信息	HTTP状态码	语义	解决方案
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	无法获取管理账户	联系技术支持。
APIG.0609	The VPC backend does not exist.	500	找不到负载后端	联系技术支持。
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.0615	Incorrect third-party authentication VPC information	500	获取第三方鉴权负载通道节点失败	检查第三方认证的负载通道配置是否正确。
APIG.0616	Incorrect third-party authentication request information	500	连接第三方鉴权服务失败	检查第三方认证服务是否正常。
APIG.0617	Incorrect third-party authentication response information	500	获取第三方鉴权服务响应失败	检查第三方认证服务是否正常。
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。

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.2102	PublicKey is null	400	签名密钥未找到	联系技术支持。
APIG.2201	Appkey or SecretKey is invalid	400	Appkey或SecretKey不合法	检查请求的Appkey或SecretKey是否正确。
APIG.2202	Refresh token is invalid	400	Refresh token不合法	检查Refresh token是否正确。
APIG.2203	Access token is invalid	400	Access token不合法	检查Access token是否正确。
APIG.2204	ContentType invalid	400	ContentType不合法	检查ContentType是否正确
APIG.2205	Auth parameter invalid	400	认证参数不合法	检查认证参数是否正确。
APIG.2206	Auth method invalid	400	认证方法不合法	检查认证方法是否正确。
APIG.2208	The length of through_data is out of range	400	through_data超长	through_data长度上限为300，根据实际情况调整through_data内容。
APIG.2209	The value of grant_type is not in enum List	400	grant_type的值不合法	grant_type只支持client_credentials、refresh_token，根据实际情况修改。
APIG.2210	Lack of grant_type	400	缺少授权类型	添加grant_type。
APIG.2211	Lack of client_id	400	缺少客户端ID	添加客户端ID。
APIG.2212	Lack of client_secret	400	缺少客户端密钥	添加客户端密钥。
APIG.2213	Lack of refresh_token	400	缺少refresh token	联系技术支持。
APIG.1001	Refresh token is expired	401	Refresh token过期	重新获取refresh token。
APIG.1002	Access token is expired	401	Access token过期	重新获取access token。

错误码	错误信息	HTTP状态码	语义	解决方案
APIG.1003	App not match refresh token	401	App与refresh token不匹配	检查client_id是否正确。
APIG.1004	App not exist	401	App不存在	检查access token是否正确。
APIG.1009	AppKey or AppSecret is invalid	400	AppKey或AppSecret不合法	检查请求的AppKey或AppSecret是否与凭据的Key或Secret相同。

7 管理 API

7.1 管理 API 概述

API创建完成后，您还可以进行以下相关操作管理API。

- **查看或编辑APIG的API信息**：您可以通过查看API的基本信息来确认API的调用信息，通过编辑API的基本信息来更改服务信息。
- **配置API的自定义认证**：您可以通过自定义认证来自定义认证系统。
- **配置API的参数编排规则**：您可以通过不同算法规则，将请求参数映射为新的请求参数。
- **自定义API的错误响应信息**：您可以通过网关响应功能，自定义响应状态码或网关响应内容。
- **克隆APIG的API**：您可以通过克隆API功能，快速创建基本信息相同的API。
- **下线APIG的API**：您可以通过下线API功能，将API从相关环境中下线，暂停对外提供的服务。**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。**
- **导入导出API**：您可以通过API设计文件、CCE工作负载、导入API到APIG。
- **APIG的API设计文件扩展定义**：导入API设计文件时，您可以参考apig支持的扩展定义，配置API设计文件。

7.2 查看或编辑 APIG 的 API 信息

API列表支持查看或编辑当前实例下所有的API，查看或编辑API的运行环境、请求方法、请求路径等信息。

查看或编辑 API 信息

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API列表”，您可以查看或编辑当前实例下的所有API，也可以进入API详情查看或编辑API。

步骤4 单击API名称，进入“API运行”页面。

- 支持查看API的监控视图、前端配置或后端配置信息。
- 支持编辑API、发布API、下线API、调试API、API授权、删除API或克隆API操作。

----结束

7.3 配置 API 的自定义认证

7.3.1 配置 API 的前端自定义认证

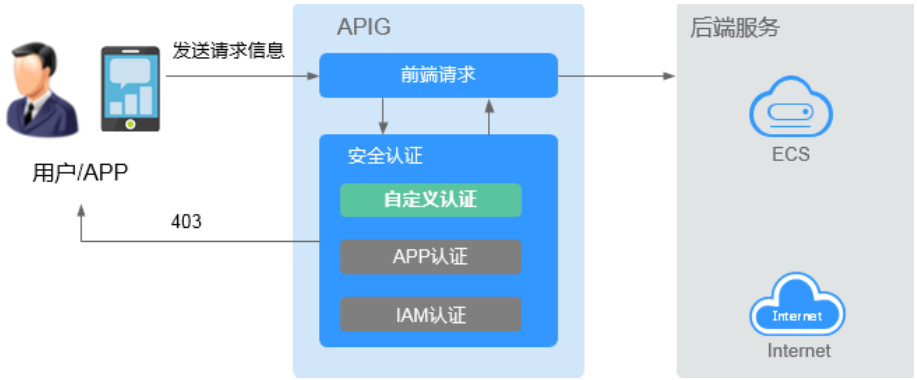
如果您需要把自己的认证系统用于API调用的认证鉴权，可以使用自定义认证来实现。

自定义认证包括前端和后端两种类型：

- 前端自定义认证：指APIG使用自定义的认证函数，对收到的API请求进行安全认证。
- 后端自定义认证：指API的后端服务使用自定义的认证函数，对来自APIG转发的后端服务请求进行安全认证。

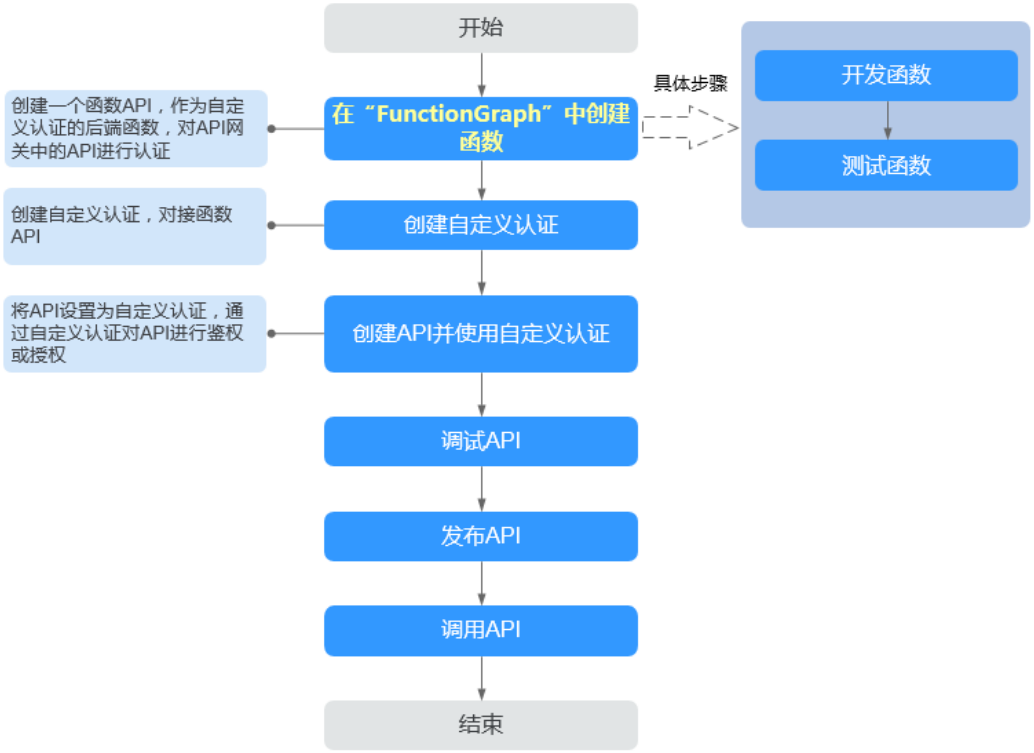
本章节主要介绍如何创建一个前端自定义认证。您需要先创建一个函数后端作为认证函数，并在自定义认证中使用该函数后端作为认证后端。

图 7-1 前端自定义认证示意图



使用自定义认证调用API的流程如下图所示：

图 7-2 自定义认证调用 API



约束与限制

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

创建用于前端自定义认证的函数

在使用前端自定义认证对前端请求进行认证鉴权前，您需要先在FunctionGraph创建一个函数，通过函数定义您所需的认证信息。

步骤1 进入FunctionGraph控制台。

步骤2 在左侧导航栏中选择“函数 > 函数列表”。

步骤3 单击“创建函数”，根据下表参数说明，创建一个函数。

表 7-1 配置函数

参数	说明
选择创建方式	默认“创建空白函数”。
函数类型	选择函数的类型，此处默认“事件函数”。
区域	选择与API网关相同区域。

参数	说明
项目	华为云的区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。此处默认为已选择的区域。
函数名称	根据规划自定义名称。建议您按照一定的命名规则填写名称，方便您快速识别和查找。
企业项目	企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。此处默认“default”。
委托名称	用户委托函数工作流去访问其他的云服务。此处选择“未使用任何委托”。
运行时	此处以python2.7语言为例。

步骤4 单击“创建函数”。

步骤5 函数创建完成后，进入函数详情。在“代码”页签中设置函数代码。

函数代码需要满足如下条件：

- 函数代码支持三种请求参数定义，格式为：
  - Header中的请求参数：event["headers"]["参数名"]
  - Query中的请求参数：event["queryStringParameters"]["参数名"]
  - 您自定义的用户数据：event["user_data"]
- 函数代码获取的三种请求参数与API网关自定义认证中的参数关系如下所示：
  - Header中的请求参数：对应自定义认证中参数位置为Header的身份来源，其参数值在您调用使用该前端自定义认证的API时传入
  - Query中的请求参数：对应自定义认证中参数位置为Query的身份来源，其参数值在您调用使用该前端自定义认证的API时传入
  - 您自定义的用户数据：对应自定义认证中的用户数据，其参数值在您创建自定义认证时输入
- 函数的返回值不能大于1M，必须满足如下格式：

```
{
    "statusCode":200,
    "body": "{\"status\": \"allow\", \"context\": {\"user\": \"abc\"}}"
}
```

其中，body字段的内容为字符串格式，json解码之后为：

```
{
    "status": "allow/deny",
    "context": {
        "user": "abc"
    }
}
```

  - “statusCode”字段为必选，函数服务正常且自定义认证函数代码符合规范时，statusCode的值则为自定义认证函数的响应码。
    - 调用自定义认证的API，当自定义认证函数的响应码为非200时，API网关认为函数服务异常，并返回错误码“500”，错误信息为“Internal server error”。

- 调用自定义认证的API，如果自定义认证开启宽松模式，当自定义认证函数连接失败、返回“500”或者“503”时，自定义认证不会校验body字段里面的status字段，直接返回调用成功，同时从函数代码中获取到的context字段也为空。

- “status”字段为必选，用于标识认证结果。只支持“allow”或“deny”，“allow”表示认证成功，“deny”表示认证失败。
- “context”字段为可选，支持字符串类型键值对，当实例支持authorizer_context_support_num_bool特性时，键值对的值支持number类型或boolean类型，键值不支持JSON对象或数组。

  context中的数据为您自定义的字段，认证通过后作为认证参数映射到API网关后端参数中，其中context中的参数名称与系统参数名称必须完全一致，且区分大小写，context中的参数名称必须以英文字母开头，支持英文大小写字母、数字、下划线和中划线，且长度为1~32个字符。

  前端认证通过后，context中的user的值abc映射到后端服务Header位置的test参数中。

Header中的请求参数定义代码示例：

```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
    if event["headers"].get("test")=='abc':
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"allow",
                "context":{
                    "user":"abcd"
                }
            })
        }
    else:
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"deny",
            })
        }
    return json.dumps(resp)
```

Query中的请求参数定义代码示例：

```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
    if event["queryStringParameters"].get("test")=='abc':
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"allow",
                "context":{
                    "user":"abcd"
                }
            })
        }
    else:
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"deny",
            })
        }
    return json.dumps(resp)
```


用户数据定义代码示例：

```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
    if event.get("user_data")=='abc':
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"allow",
                "context":{
                    "user":"abcd"
                }
            })
        }
    else:
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status":"deny",
            })
        }
    return json.dumps(resp)
```

步骤6 测试函数。在测试事件的“事件模板”中选择“apig-event-template”，根据实际情况修改后保存测试模板，单击“测试”。

执行结果为“成功”时，表示测试成功。

接下来您需要进入API网关界面创建前端自定义认证。

----结束

创建前端自定义认证

在创建前端自定义认证前，请确保已有用于前端自定义认证的函数后端，否则请提前**创建用于前端自定义认证的函数**。

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“自定义认证”页面，单击“创建自定义认证”。根据下表参数说明，配置自定义认证参数。

表 7-2 自定义认证参数说明

参数	说明
认证名称	填写自定义的认证名称，用于区分不同的自定义认证。支持中文、英文、数字、下划线，只能以中文或英文开头，长度为3~64个字符。
类型	创建前端自定义认证时，选择“前端”。
函数地址	选择用于前端自定义认证的函数后端，仅可以选择状态为“已部署”的函数后端。
版本或别名	选择函数的版本或别名，函数的版本或别名功能请参考**《函数工作流 FunctionGraph用户指南》**。

参数	说明
缓存时间(秒)	设置认证结果缓存的时间。 取值范围为0s~3600s，值为0时代表不缓存，最大支持3600s。
宽松模式	• 开关开启后，当函数服务不可用（与函数服务建立连接失败或者函数服务返回5*xx*）时，API网关仍然接受客户端请求。如果有重试请求，以最后一次返回结果为准。 • 开关开启后，如果API的后端认证使用了自定义认证，那么后端认证参数获取到的值为空。 **开启宽松模式存在安全风险，请谨慎操作。**
身份来源	设置用于认证的请求参数。 当“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。
是否发送body	指是否将API请求的body体内容传递给认证函数。body体内容传给函数的方式，与header、query内容传递一致。
用户数据	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。长度为1~2048个字符。

步骤5 单击“确定”，完成自定义认证的创建。

----结束

7.3.2 配置 API 的后端自定义认证

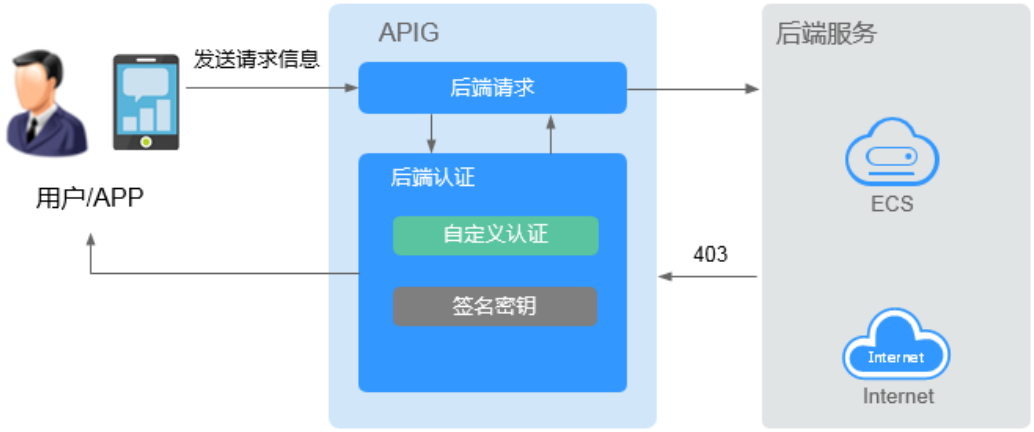
如果您需要把自己的认证系统用于API调用的认证鉴权，可以使用自定义认证来实现。

自定义认证包括前端和后端两种类型：

- 前端自定义认证：指APIG使用自定义的认证函数，对收到的API请求进行安全认证。
- 后端自定义认证：指API的后端服务使用自定义的认证函数，对来自APIG转发的后端服务请求进行安全认证。

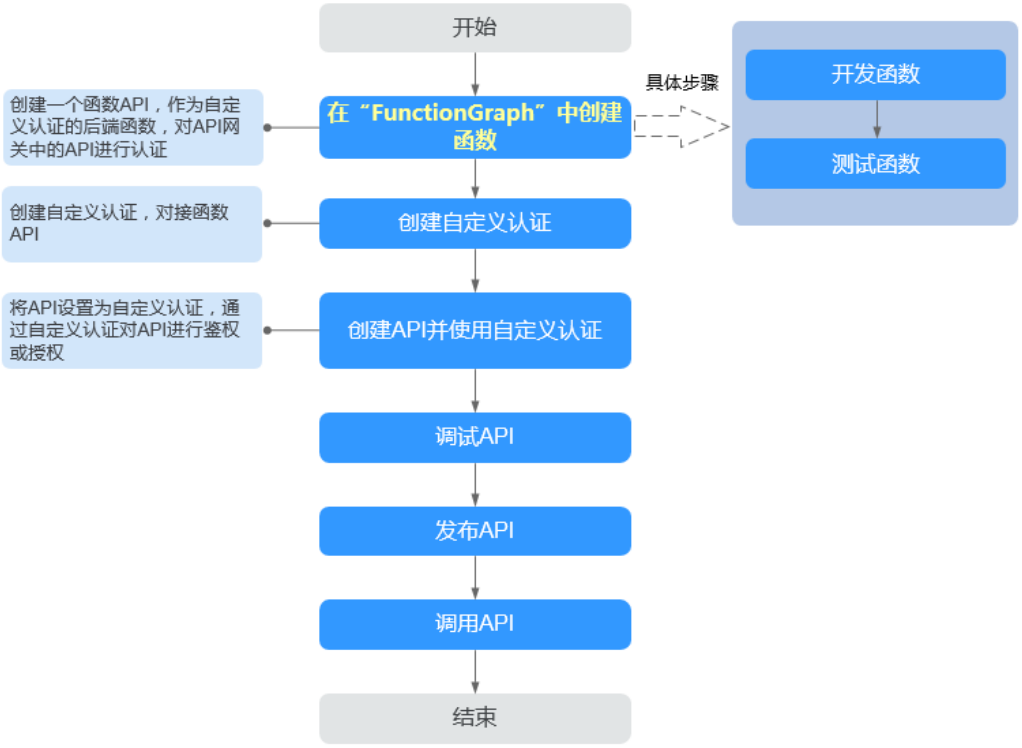
本章节主要介绍如何创建一个后端自定义认证。您需要先创建一个函数后端作为认证函数，并在自定义认证中使用该函数后端作为认证后端。

图 7-3 后端自定义认证示意图



使用自定义认证调用API的流程如下图所示：

图 7-4 使用自定义认证调用 API



约束与限制

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

创建用于后端自定义认证的函数

步骤1 进入FunctionGraph控制台。

步骤2 在左侧导航栏中选择“函数 > 函数列表”。

步骤3 单击“创建函数”，根据下表参数说明，创建一个函数。

表 7-3 配置函数

参数	说明
选择创建方式	默认“创建空白函数”。
函数类型	选择函数的类型，此处默认“事件函数”。
区域	选择与API网关相同区域。
项目	华为云的区域默认对应一个项目，这个项目由系统预置，用来隔离物理区域间的资源（计算资源、存储资源和网络资源），以默认项目为单位进行授权，用户可以访问您账号中该区域的所有资源。此处默认为已选择的区域。
函数名称	根据规划自定义名称。建议您按照一定的命名规则填写名称，方便您快速识别和查找。
企业项目	企业项目是项目的升级版，针对企业不同项目间资源的分组和管理，是逻辑隔离。此处默认“default”。
委托名称	用户委托函数工作流去访问其他的云服务。此处选择“未使用任何委托”。
运行时	此处以python2.7语言为例。

步骤4 单击“创建函数”。

步骤5 函数创建完成后，进入函数详情。

函数代码需要满足如下条件：

- 函数代码只支持您自定义的用户数据，且格式为：event["user_data"]。
- 函数代码获取的请求参数与API网关自定义认证中的参数关系为：函数请求参数中的自定义用户数据对应API网关自定义认证中的用户数据，参数值在您创建API网关自定义认证时输入，用户数据格式不限制，您可以自行指定。
- 函数的返回值不能大于1M，必须满足如下格式：

```
{
    "statusCode":200,
    "body": "{\"status\": \"allow\", \"context\": {\"user\": \"abc\"}}"
}
```

其中，body字段的内容为字符串格式，json解码之后为：

```
{
    "status": "allow/deny",
    "context": {
        "user": "abc"
    }
}
```

  - “statusCode”字段为必选，函数服务正常且自定义认证函数代码符合规范时，statusCode的值则为自定义认证函数的响应码。

- 调用自定义认证的API，当自定义认证函数的响应码为非200时，API网关认为函数服务异常，并返回错误码“500”，错误信息为“Internal server error”。
- 调用自定义认证的API，如果自定义认证开启宽松模式，当自定义认证函数连接失败、返回“500”或者“503”时，自定义认证不会校验body字段里面的status字段，直接返回调用成功，同时从函数代码中获取到的context字段也为空。

– “status”字段为必选，用于标识认证结果。只支持“allow”或“deny”，“allow”表示认证成功，“deny”表示认证失败。

– “context”字段为可选，支持字符串类型键值对，当实例支持authorizer_context_support_num_bool特性时，键值对的值支持number类型和boolean类型，键值不支持JSON对象或数组。

context中的数据为您自定义的字段，认证通过后作为认证参数映射到API网关后端参数中，其中context中的参数名称与系统参数名称必须完全一致，且区分大小写。context中的参数名称必须以英文字母开头，支持英文大小写字母、数字、下划线和中划线，且长度为1 ~ 32个字符。

后端认证通过后，context中的user的值abc映射到后端服务Header位置的test参数中，并将其传递给API的后端服务。

用户数据定义代码示例：

```
# -*- coding:utf-8 -*-
import json
import base64
def handler(event, context):
    exampleuserdata=base64.b64encode(event["user_data"])
    resp = {
        'statusCode': 200,
        'body': json.dumps({
            "status":"allow",
            "context":{
                "user":exampleuserdata
            }
        })
    }
    return json.dumps(resp)
```

步骤6 测试函数。在测试事件的“事件模板”中选择“空白模板”，内容为：

```
{"user_data": "123"}
```

根据实际情况修改后保存测试模板，单击“测试”。

执行结果为“成功”时，表示测试成功。

接下来您需要进入API网关界面创建后端自定义认证。

----结束

创建后端自定义认证

在创建后端自定义认证前，请确保已有用于后端自定义认证的函数后端，否则请提前**创建用于后端自定义认证的函数**。

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“自定义认证”页面，单击“创建自定义认证”。根据下表参数说明，配置自定义认证参数。

表 7-4 自定义认证参数说明

参数	说明
认证名称	填写您自定义的认证名称，用于区分不同的自定义认证。支持中文、英文、数字、下划线，只能以中文或英文开头，长度为3~64个字符。
类型	创建后端自定义认证时，选择“后端”。
函数地址	选择用于后端自定义认证的函数后端，仅可以选择状态为“已部署”的函数后端。
版本或别名	选择函数的版本或别名，函数的版本或别名功能请参考《函数工作流 FunctionGraph用户指南》。
缓存时间(秒)	设置认证结果缓存的时间。 取值范围为0s~3600s，值为0时代表不缓存，最大支持3600s。
宽松模式	• 开关开启后，当函数服务不可用（与函数服务建立连接失败或者函数服务返回5*xx*）时，API网关仍然接受客户端请求。如果有重试请求，以最后一次返回结果为准。 • 开关开启后，如果API的后端认证使用了自定义认证，那么后端认证参数获取到的值为空。 **开启宽松模式存在安全风险，请谨慎操作。**
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。
是否发送body	指是否将API请求的body体内容传递给认证函数。body体内容传给函数的方式，与header、query内容传递一致。
用户数据	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。长度为1-2048个字符。

步骤5 单击“确定”，完成自定义认证的创建。

----结束

7.4 配置 API 的参数编排规则

API网关支持对API进行参数编排，根据请求参数取值，配置不同算法规则，映射为新的请求参数和新的参数值。

创建编排规则

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 单击“编排规则管理”页签。

步骤5 单击“创建编排规则”，根据下表参数说明，配置编排规则。

表 7-5 编排规则配置

参数	说明
规则名称	填写编排规则的名称，根据规划自定义。支持英文、数字、下划线，且只能以英文开头，长度为3~64个字符。
编排策略	选择编排策略。 • list：列表中的值映射成另外的值。 • range：范围中的值映射成另外的值。 • hash：请求头的值经过哈希计算后直接映射为新的请求头。 • hash_range：先用请求参数生成hash值，再用hash值进行range编排。 • none_value：请求参数为空时将返回none_value策略的编排映射值。 • default：请求参数存在，但是没有编排规则可以匹配上请求参数时，将返回default策略的编排映射值。 • head_n：用于截取字符串前n项（如果n大于字符串长度，会返回完整的原始参数值），生成一个临时参数，后面的编排规则用这个临时参数值进行编排。 • tail_n：用于截取字符串后n项（如果n大于字符串长度，会返回完整的原始参数值），生成一个临时参数，后面的编排规则用这个临时参数值进行编排。
是否预处理策略	**当“编排策略”选择“list”、“range”、“hash”、“hash_range”、“head_n”、“tail_n”时可见。** 配置是否预处理策略。当编排规则为预处理时，将该编排规则生成的参数值作为临时参数，成为下一个编排规则的待编排参数。
参数名称	**当“是否预处理策略”开关关闭或者“编排策略”选择“none_value”或“default”时需要配置。** 填写编排后的参数名称。支持英文、数字、中划线，且只能以英文开头，长度为1~128个字符。

参数	说明
参数类型	**当“是否预处理策略”开关关闭或者“编排策略”选择“none_value”或“default”时需要配置。** 选择参数类型。 ● string ● number
参数位置	**当“是否预处理策略”开关关闭或者“编排策略”选择“none_value”或“default”时需要配置。** 选择参数位置。 ● header ● query
映射信息	**当“编排策略”选择“list”、“range”、“hash_range”、“none_value”、“default”时需要配置。** 填写参数映射信息。支持英文、数字、下划线、中划线，且只能以英文开头，长度为1~128个字符。多个参数值用英文逗号分隔，最多支持3000个参数。 单击“新增映射信息”，可添加新的映射信息。 ● 编排前的请求参数值 – 当“编排策略”选择“list”，输入编排前的请求参数值。 – 当“编排策略”选择“range”或“hash_range”，输入区间起始值和终止值。 ● 编排后的请求参数值：输入编排后的请求参数值。
截取长度	**当“编排策略”选择“head_n”或“tail_n”时需要配置。** 配置截取字符串的长度，取值范围为1~100。

步骤6 单击“确定”。

----结束

7.5 自定义 API 的错误响应信息

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。

约束与限制

- 每个分组最多可新增4个网关响应。
- 最多支持10个响应头自定义，响应头的key支持数字、英文字母和下划线（1到128位），value可以引用运行时变量（可以引用的变量见**API网关运行时可获取变量**），value不能包含“[[”和“]]”。
- 不论是默认网关响应“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。
- 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**。

自定义网关响应

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“网关响应”区域，您可以新增或编辑网关响应。

如果修改完默认网关响应后，需要恢复默认配置，单击“恢复默认配置”即可。

----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下表，其中响应状态码可以按实际需要做自定义修改。

表 7-6 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
第三方认证配置错误	500	第三方认证方异常，通信失败、返回异常响应等错误
第三方认证失败	401	第三方认证方返回认证失败

错误说明	默认的响应状态码	详细说明
第三方认证身份来源错误	401	第三方认证的身份来源信息缺失
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	404	未匹配到API
请求参数错误	400	请求参数校验失败、不支持的HTTP方法
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
凭据未授权	401	使用的凭据未被授权访问该API

API 网关运行时可获取变量

表 7-7 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.apiName	API名称
$context.appId	API调用者的凭据对象ID
$context.appName	API调用者的凭据对象名称
$context.requestId	当次API调用生成请求ID
$context.stage	API调用的部署环境
$context.sourceIp	API调用者的源地址
$context.reqPath	API请求路径，不包含query参数
$context.reqUri	API请求路径，包含query参数
$context.reqMethod	API请求方法
$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

运行时变量名称	描述
$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

7.6 克隆 APIG 的 API

API网关支持克隆已创建的API，提高API创建效率。您在克隆API时需要自定义API名称和API前端路径。

克隆API暂不支持克隆绑定策略，如果需要绑定策略请手动操作。

前提条件

已创建API，如果未创建API，请**通过APIG创建REST API**。

克隆 API

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面，单击“更多 > 克隆”。

步骤6 根据下表参数说明，自定义API名称和API前端路径，单击“确定”。

表 7-8 克隆 API 配置

参数	说明
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。 支持中文、英文、数字、中划线、下划线、点、斜杠、中英文格式下的小括号和冒号、中文格式下的顿号，且只能以英文、中文或数字开头，长度为3~255个字符。
API路径	API的请求路径。请求路径可以包含请求参数，请求参数使用{}标识，例如/a/{b}，也可以通过配置“+”号做前缀匹配，例如：/a/{b+}。注意，请求路径中的字母区分大小写。

----结束

后续操作

API克隆完成后，通过**调试API**，验证服务是否正常。

7.7 下线 APIG 的 API

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 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击*API分组名称*，进入API分组详情页面。

- 单个下线API。在左侧选择API，然后在右上角单击“下线”，弹出“下线API”对话框。
- 批量下线API，最多同时下线1000个API。单击“批量操作”，选择API，然后单击下线按钮，弹出“下线API”对话框。

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。

7.8 导入导出 API

7.8.1 导入导出 API 的限制与兼容性说明

在API网关中导入或者导出API时，限制与兼容性如下所示：

约束与限制

- API网关参数限制，如下所示。

  - API网关暂不支持formData和body位置的请求参数定义。
  - API网关暂不支持consumes和produces定义。
  - API网关中，header位置的参数名称，不区分大小写。
- 后端策略限制，如下所示。
  - 默认后端类型为HTTP，策略后端支持HTTP、HTTP-VPC。
  - 默认后端类型为HTTP-VPC，策略后端支持HTTP、HTTP-VPC。
  - 默认后端类型为function，策略后端支持function。
  - 默认后端类型为mock，策略后端支持mock。

兼容性说明

- 支持OpenAPI规范。

  OpenAPI规范（OAS），是定义一个标准的、与具体编程语言无关的RESTful API的规范。OpenAPI规范的前身是Swagger规范，API网关目前支持两种OpenAPI规范：Swagger 2.0或OpenAPI 3.0。**为了方便区分，下文中OAS表示OpenAPI规范（包含Swagger 2.0或OpenAPI 3.0），Swagger表示Swagger 2.0规范，OpenAPI表示OpenAPI 3.0规范。**
- API网关导入或导出的OAS对象，与API网关对象定义的**映射关系**。
- **请求参数类型与API网关参数类型差异**。
- **API请求路径模板语法差异**。
- 导入API时支持的API网关**扩展字段**。

表 7-9 OAS 对象与 API 网关对象定义的映射关系

Swagger对象	OpenAPI对象（以3.0.0为例）	API网关对象	导入时行为	导出时行为
info.title	info.title	API分组名称	导入到新的分组：新的分组名称 导入到已有分组：未使用 支持汉字、英文、数字、下划线，且只能以英文或汉字开头，3 ~ 64字符	填充为分组名称
info.description	info.description	API分组描述	导入到新的分组：新的分组描述 导入到已有分组：未使用	填充为分组描述信息
info.version	info.version	版本	未使用	用户指定 未指定则使用当前时间

Swagger对象	OpenAPI对象（以3.0.0为例）	API网关对象	导入时行为	导出时行为
host	server.url	API分组域名	未使用	优先使用API分组的第一个自定义域名 如果分组未绑定自定义域名则使用分组的独立域名
basePath	-	-	将与每条API的请求路径拼接起来使用	未填充
paths.path	paths.path	API请求路径	与basePath拼接起来作为API请求路径	填充为API请求路径
operation.operationId	operation.operationId	API名称	作为API名称	填充为API名称
operation.description	operation.description	API描述	作为API描述	填充为API描述
operation.parameters	operation.parameters	API前端请求参数	作为API请求参数	填充为API请求参数
operation.schemes	-	API前端请求协议	作为API请求协议	填充为API请求协议
operation.responses	operation.responses	-	未使用	固定填充default响应定义
operation.security	operation.security	API认证方式	API认证方式 结合x-apigateway-auth-type	填充为API认证方式 结合x-apigateway-auth-type

表 7-10 请求参数类型和 API 网关参数类型差异

OAS类型Swagger类型	API网关类型	支持的参数属性字段
integer long float double	number	maximum minimum default enum required description

OAS类型Swagger类型	API网关类型	支持的参数属性字段
string	string	maxLength minLength default enum required description
其它类型	不支持	不支持

表 7-11 API 请求路径模板语法差异

语法	OAS类型Swagger类型	API网关
/users/{userName}	支持	支持
/users/prefix-{userName} /users/{userName}-suffix /users/prefix-{userName} -suffix	支持	前端请求定义不支持 后端请求定义支持
/users/{proxy+}	不支持	前端请求定义支持 后端请求定义不支持

7.8.2 通过 API 设计文件导入 API

将Swagger或OpenAPI定义的API导入到API网关，支持**导入到新分组**和**导入到已有分组**两种方式。导入前您需要在API定义中补全API网关的**扩展定义**。

注意事项

- API网关中API分组和API的**配额**满足需求。
- 如果使用Swagger info或OpenAPI info的title作为API分组名称，新创建的API分组名称不能与已有的API分组名称重名。
- 导入的API定义中，如果存在冲突，那么根据系统导入的先后顺序，先导入的API会显示导入成功，后导入的API会显示导入失败。例如导入的API定义中存在2个名称相同或请求路径相同的API，那么先导入的API会显示导入成功，后导入的会显示导入失败。
- 导入的API定义与已有的API定义冲突时，您可以选择使用导入的API定义覆盖已有的API定义，或者保留已有的API定义，此时导入的API定义会显示导入失败。
- 如果选择扩展覆盖，当导入API的扩展定义项名称与已有策略（ACL，流量控制等）名称相同时，则会覆盖已有策略（ACL，流量控制等）。
- 导入的API不会自动发布到环境，导入时可以选择“立即发布”或者“稍后发布”，您可以自行选择策略。

- 暂不支持导入API的负载通道。

导入 API 设计文件

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 支持通过以下路径导入API。

- 在左侧导航栏选择“API管理 > API分组”。单击“创建API分组 > 导入API设计文件”。
- 在左侧导航栏选择“API管理 > API列表”。单击“导入API”。

步骤4 在弹窗中选择本地路径下的API文件，然后单击“打开”导入文件。

步骤5 根据下表参数说明，填写导入信息。

表 7-12 导入 API

参数名称	说明
导入方式	导入方式包含以下2种： • 生成新的分组：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。 • 选择已有分组：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“选择已有分组”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名称相同时，导入的API会覆盖已有的API。 仅在选择“选择已有分组”时，需要选择是否覆盖。
扩展覆盖	勾选后，当导入API扩展定义项名称（ACL，流控等）与已有的策略（ACL，流控等）名称相同时，会覆盖已有的策略（ACL，流控等）。

步骤6 （可选）单击“全局配置(可选)”。

1. 安全配置。请参考**5.2**。
2. 后端请求配置。请参考**步骤1**。
3. 单击“下一步”，支持通过“表单”、“JSON”、“YAML”样式查看配置详情。
4. 确认无误后，单击“提交”，完成配置。

步骤7 单击“立即导入”，在弹窗中选择是否现在发布API到环境。

- 如果选择“现在发布”，还需要选择API要发布的环境，将API分组下的所有API发布到环境上。
- 如果选择“稍后发布”，请参考**发布API**。

步骤8 单击“确定”，跳转到“API运行”页面，可查看分组下的API。

您也可以参考以下示例导入API到API网关：

- **导入HTTP类型后端服务API示例**
- **导入HTTP VPC类型后端服务API示例**
- **导入FUNCTION类型后端服务API示例**
- **导入MOCK类型后端服务API示例**

----结束

导入 HTTP 类型后端服务 API 示例

包含IAM认证和请求参数编排的GET方法API定义，后端服务类型为HTTP。

Swagger示例：

```
swagger: "2.0"
info:
  title: "importHttpEndpoint10"
  description: "import apis"
  version: "1.0"
host: "api.account.com"
paths:
  '/http/{userId}':
    get:
      operationId: "getUser3"
      description: "get user by userId"
      security:
      - apig-auth-iam: []
      schemes:
      - https
      parameters:
      - name: "test"
        description: "authorization token"
        type: "string"
        in: "header"
        required: true
      - name: "userId"
        description: "user id"
        type: "string"
        in: "path"
        required: true
      responses:
        "200":
          description: "user information"
      x-apigateway-request-type: "public"
      x-apigateway-cors: true
      x-apigateway-is-send-fg-body-base64: true
      x-apigateway-match-mode: "NORMAL"
      x-apigateway-backend:
        type: "HTTP"
        parameters:
        - name: "userId"
          value: "userId"
          in: "query"
          origin: "REQUEST"
          description: "user id"
        - name: "X-Invoke-User"
          value: "apigateway"
          in: "header"
          origin: "CONSTANT"
          description: "invoke user"
        httpEndpoints:
          address: "example.com"
          scheme: "http"
          method: "GET"
          path: "/users"
```

```
        timeout: 30000
securityDefinitions:
  apig-auth-app:
    in: header
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
openapi: 3.0.0
info:
  title: importHttpEndpoint10
  version: '1.0'
servers:
  - url: >-
      http://abc.com
  - url: >-
      https://abc.com
paths:
  '/http/{userId}':
    get:
      description: get user by userId
      operationId: getUser3
      parameters:
        - description: authorization token
          example: ''
          in: header
          name: test
          required: true
          schema:
            maxLength: 0
            maximum: 0
            minimum: 0
            type: string
          x-apigateway-pass-through: always
        - description: user id
          example: ''
          in: path
          name: userId
          required: true
          schema:
            maxLength: 0
            maximum: 0
            minimum: 0
            type: string
          x-apigateway-pass-through: always
      responses:
        default-cors:
          description: response example
          x-apigateway-result-failure-sample: ''
          x-apigateway-result-normal-sample: ''
      security:
        - apig-auth-iam: []
      servers:
        - url: >-
            https://abc.com
      x-apigateway-backend:
        httpEndpoints:
          address: example.com
          description: ''
          enableClientSsl: false
          method: GET
          path: /users
          retryCount: '-1'
```

```
        scheme: http
        timeout: 30000
      parameters:
        - description: invoke user
          in: HEADER
          name: X-Invoke-User
          origin: CONSTANT
          value: apigateway
        - description: user id
          in: QUERY
          name: userId
          origin: REQUEST
          value: userId
      type: HTTP
    x-apigateway-cors: true
    x-apigateway-is-send-fg-body-base64: true
    x-apigateway-match-mode: NORMAL
    x-apigateway-request-type: public
    x-apigateway-response: default
components:
  responses:
    default-cors:
      description: response example
      headers:
        Access-Control-Allow-Origin:
          schema:
            default: '*'
            type: string
  securitySchemes:
    apig-auth-app:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-type: AppSigv1
    apig-auth-app-header:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-opt:
        appcode-auth-type: header
      x-apigateway-auth-type: AppSigv1
    apig-auth-iam:
      in: header
      name: unused
      type: apiKey
      x-apigateway-auth-type: IAM
  x-apigateway-responses:
    default: {}
```

导入 HTTP VPC 类型后端服务 API 示例

包含APP认证和请求参数编排的ANY方法API定义，后端服务使用VPC通道。

Swagger示例：

```
swagger: "2.0"
info:
  title: "importHttpVpcEndpoint"
  description: "import apis"
  version: "1.0"
host: "api.account.com"
paths:
  '/http-vpc':
    x-apigateway-any-method:
      operationId: "userOperation"
      description: "user operation resource"
      security:
      - apig-auth-app: []
      schemes:
```

```
    - https
    parameters:
    - name: "Authorization"
      description: "authorization signature"
      type: "string"
      in: "header"
      required: true
    responses:
      "default":
        description: "endpoint response"
    x-apigateway-request-type: "public"
    x-apigateway-cors: true
    x-apigateway-is-send-fg-body-base64: true
    x-apigateway-match-mode: "SWA"
    x-apigateway-backend:
      type: "HTTP-VPC"
      parameters:
      - name: "X-Invoke-User"
        value: "apigateway"
        in: "header"
        origin: "CONSTANT"
        description: "invoke user"
      httpVpcEndpoints:
        name: "userVpc"
        scheme: "http"
        method: "GET"
        path: "/users"
        timeout: 30000
securityDefinitions:
  apig-auth-app:
    in: header
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
openapi: 3.0.0
info:
  description: import apis
  title: importHttpVpcEndpoint
  version: '1.0'
servers:
  - url: >-
      http://abc.com
  - url: >-
      https://abc.com
paths:
  /http-vpc:
    x-apigateway-any-method:
      description: user operation resource
      operationId: userOperation
      parameters:
        - description: authorization signature
          example: ''
          in: header
          name: Authorization
          required: true
          schema:
            maxLength: 0
            maximum: 0
            minimum: 0
            type: string
          x-apigateway-pass-through: always
      responses:
```

```
      default-cors:
        description: response example
        x-apigateway-result-failure-sample: ''
        x-apigateway-result-normal-sample: ''
    security:
      - apig-auth-app: []
    servers:
      - url: >-
          https://abc.com
    x-apigateway-backend:
      httpVpcEndpoints:
        cascade_flag: false
        description: ''
        enableClientSsl: false
        method: GET
        name: userVpc
        path: /users
        retryCount: '-1'
        scheme: http
        timeout: 30000
      parameters:
        - description: invoke user
          in: HEADER
          name: X-Invoke-User
          origin: CONSTANT
          value: apigateway
      type: HTTP-VPC
    x-apigateway-cors: true
    x-apigateway-is-send-fg-body-base64: true
    x-apigateway-match-mode: SWA
    x-apigateway-request-type: public
components:
  responses:
    default-cors:
      description: response example
      headers:
        Access-Control-Allow-Origin:
          schema:
            default: '*'
            type: string
  securitySchemes:
    apig-auth-app:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-type: AppSigv1
    apig-auth-app-header:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-opt:
        appcode-auth-type: header
      x-apigateway-auth-type: AppSigv1
    apig-auth-iam:
      in: header
      name: unused
      type: apiKey
      x-apigateway-auth-type: IAM
  x-apigateway-responses: {}
```

导入 FUNCTION 类型后端服务 API 示例

包含IAM认证和请求参数编排的GET方法API定义，后端服务类型为FunctionGraph。

Swagger示例：

```
swagger: "2.0"
info:
  title: "importFunctionEndpoint"
```

```
  description: "import apis"
  version: "1.0"
host: "api.account.com"
paths:
  '/function/{name}':
    get:
      operationId: "invokeFunction"
      description: "invoke function by name"
      security:
      - apig-auth-iam: []
      schemes:
      - https
      parameters:
      - name: "test"
        description: "authorization token"
        type: "string"
        in: "header"
        required: true
      - name: "name"
        description: "function name"
        type: "string"
        in: "path"
        required: true
      responses:
        "200":
          description: "function result"
      x-apigateway-request-type: "public"
      x-apigateway-cors: true
      x-apigateway-is-send-fg-body-base64: true
      x-apigateway-match-mode: "NORMAL"
      x-apigateway-backend:
        type: "FUNCTION"
        parameters:
        - name: "functionName"
          value: "name"
          in: "query"
          origin: "REQUEST"
          description: "function name"
        - name: "X-Invoke-User"
          value: "apigateway"
          in: "header"
          origin: "CONSTANT"
          description: "invoke user"
        functionEndpoints:
          function-urn: "your function urn address"
          version: "your function version"
          invocation-type: "async"
          timeout: 30000
securityDefinitions:
  apig-auth-app:
    in: header
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
openapi: 3.0.0
info:
  description: import apis
  title: importHttpEndpoint
  version: '1.0'
servers:
  - url: >-
      http://api.account.com
```

```
  - url: >-
      https://api.account.com
paths:
  /function/{name}:
    get:
      description: invoke function by name
      operationId: invokeFunction
      parameters:
        - description: function name
          in: path
          name: name
          required: true
          schema:
            maxLength: 0
            maximum: 0
            minimum: 0
            type: string
          x-apigateway-pass-through: always
          example: ''
        - description: authorization token
          in: header
          name: test
          required: true
          schema:
            maxLength: 0
            maximum: 0
            minimum: 0
            type: string
          x-apigateway-pass-through: always
          example: ''
      responses:
        default-cors:
          description: response example
          x-apigateway-result-failure-sample: ''
          x-apigateway-result-normal-sample: ''
      security:
        - apig-auth-iam: []
      servers:
        - url: >-
            https://api.account.com
      x-apigateway-backend:
        functionEndpoints:
          alias-urn: ''
          description: ''
          function-urn: "your function urn address"
          invocation-type: async
          network-type: V1
          timeout: 30000
          version: "your function version"
        parameters:
          - description: invoke user
            in: HEADER
            name: X-Invoke-User
            origin: CONSTANT
            value: apigateway
          - description: function name
            in: QUERY
            name: functionName
            origin: REQUEST
            value: name
        type: FUNCTION
      x-apigateway-cors: true
      x-apigateway-is-send-fg-body-base64: true
      x-apigateway-match-mode: NORMAL
      x-apigateway-request-type: public
      x-apigateway-response: default
components:
  responses:
    default-cors:
```

```
    description: response example
    headers:
      Access-Control-Allow-Origin:
        schema:
          default: '*'
          type: string
securitySchemes:
  apig-auth-app:
    in: header
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
x-apigateway-responses:
  default: {}
```

导入 MOCK 类型后端服务 API 示例

包含无认证的GET方法API定义，后端服务类型为MOCK。

Swagger示例：

```
swagger: "2.0"
info:
  title: "importMockEndpoint"
  description: "import apis"
  version: "1.0"
host: "api.account.com"
paths:
  '/mock':
    get:
      operationId: "mock"
      description: "mock test"
      schemes:
      - http
      responses:
        "200":
          description: "mock result"
      x-apigateway-request-type: "private"
      x-apigateway-cors: true
      x-apigateway-is-send-fg-body-base64: true
      x-apigateway-match-mode: "NORMAL"
      x-apigateway-backend:
        type: "MOCK"
        mockEndpoints:
          result-content: "{\"message\": \"mocked\"}"
securityDefinitions:
  apig-auth-app:
    in: header
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
openapi: 3.0.0
info:
  description: import apis
  title: importHttpVpcEndpoint
  version: '1.0'
```



```
servers:
  - url: >-
      http://abc.com
  - url: >-
      https://abc.com
paths:
  /mock:
    get:
      description: mock test
      operationId: mock
      responses:
        default-cors:
          description: response example
          x-apigateway-result-failure-sample: ''
          x-apigateway-result-normal-sample: ''
      servers:
        - url: >-
            http://abc.com
      x-apigateway-backend:
        mockEndpoints:
          description: ''
          result-content: '{"message": "mocked"}'
        type: MOCK
      x-apigateway-cors: true
      x-apigateway-is-send-fg-body-base64: true
      x-apigateway-match-mode: NORMAL
      x-apigateway-request-type: private
      x-apigateway-response: default
components:
  responses:
    default-cors:
      description: response example
      headers:
        Access-Control-Allow-Origin:
          schema:
            default: '*'
            type: string
  securitySchemes:
    apig-auth-app:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-type: AppSigv1
    apig-auth-app-header:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-opt:
        appcode-auth-type: header
      x-apigateway-auth-type: AppSigv1
    apig-auth-iam:
      in: header
      name: unused
      type: apiKey
      x-apigateway-auth-type: IAM
  x-apigateway-responses:
    default: {}
```

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。

7.8.3 通过 CCE 工作负载导入 API

API网关支持导入云容器引擎（Cloud Container Engine，简称CCE）的工作负载，将工作负载作为后端服务，在API网关中开放API，提供给API调用者使用。

说明

如果当前实例不支持“导入CCE工作负载”，请联系客服。

注意事项

- 仅支持华为云CCE Turbo集群、VPC网络模型的CCE集群。
- 您需要确保当前实例与CCE集群所属同一个VPC中，或通过其他方式保证两者网络可达，否则导入后调用API会出现失败场景。
- 选择VPC网络模型的CCE集群时，您需要在实例详情界面的路由配置中添加CCE集群的容器网段，否则导入后调用API会出现失败场景。
- 导入后会生成相应的API以及微服务类型的负载通道，负载通道会监测工作负载下所有实例的地址变化，并更新到负载通道中。

前提条件

已创建**CCE工作负载**。

导入 CCE 工作负载

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击“创建API分组 > 导入CCE工作负载”。根据下表参数说明，配置信息。

表 7-13 配置信息

参数	说明
所属分组	CCE工作负载所属分组。支持同步创建新的分组或选择已有分组。
集群	选择集群，可单击“查看云容器引擎CCE”查看。
命名空间	选择工作负载的命名空间。命名空间是对一组资源和对象的抽象整合。
工作负载类型	选择工作负载类型。 • 无状态负载 Deployment：在运行中始终不保存任何数据或状态的工作负载称为无状态负载 。 • 有状态工作负载 Statefulset：在运行过程中会保存数据或状态的工作负载称为有状态工作负载。 • 守护进程集 DaemonSet：守护进程集可以确保全部（或者某些）节点上仅运行一个Pod实例，当有节点加入集群时，也会为其新增一个 Pod 。 当有节点从集群移除时，这些Pod会被回收。删除DaemonSet将会删除它创建的所有Pod。 工作负载类型的介绍请参考**工作负载概述**。
服务标识名	选择工作负载的Pod标签，通过Pod标签指定某个工作负载。服务标识名为Pod标签的键，服务标识值为Pod标签的值。 Pod标签相关内容指导，请参考**设置标签与注解**。
服务标识值	

参数	说明
标签	选择工作负载的Pod标签。如果服务标识名和服务标识值不唯一，且不能指定某个工作负载时，还可以通过选择其他Pod标签指定某个工作负载。
请求协议	支持HTTP、HTTPS，传输重要或敏感数据时推荐使用HTTPS。
请求路径前缀	请求路径通过配置“+”做前缀匹配。例如，请求路径为/a/{b+}。
端口	填写CCE工作负载的监测端口号。
安全认证	支持APP认证、华为IAM认证和无认证。 • APP认证：表示由API网关服务负责接口请求的安全认证。推荐使用APP认证方式。 • 华为IAM认证：表示借助IAM服务进行安全认证。 • 无认证：表示不需要认证。
支持跨域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“请求方法”为“OPTIONS”的API，具体操作请参考**开启跨域访问**。
后端超时(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms。 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。 **说明** 在实例**配置参数**中修改超时时间上限，可修改范围为1ms~600000ms。

步骤5 单击“完成”。

----结束

相关文档

使用专享版API网关开放云容器引擎CCE工作负载

7.8.4 导出 APIG 的 API

APIG支持把创建的API以JSON、YAML、YML文件的格式导出，支持导出单个API和批量导出API。

导出 API

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。单击分组名称然后单击“导出”。

或在左侧导航栏选择“API管理 > API列表”，单击“导出API”。

步骤4 根据下表参数说明，设置导出参数。

表 7-14 导出 API

参数	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。
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。适用于生成Swagger或OpenAPI格式的API文档定义。 • 全量定义：包括API前端请求定义、后端服务定义和响应定义。适用于将API定义备份为Swagger或OpenAPI文件。 • 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、YAML或YML。
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。
OpenAPI版本	选择导出Swagger 2.0或OpenAPI 3.0定义的API。

步骤5 单击“导出”，右侧显示导出结果，并自动下载文件。

----结束

7.9 APIG 的 API 设计文件扩展定义

7.9.1 x-apigateway-auth-type

含义：基于Swagger的apiKey认证格式，定义API网关支持的特有认证方式。

作用域：Security Scheme Object(2.0)/Security Scheme Object(3.0)

Swagger：

```
securityDefinitions:
  apig-auth-app:
    in: header
```

```
    name: Authorization
    type: apiKey
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    in: header
    name: unused
    type: apiKey
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
securitySchemes:
    apig-auth-app:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-type: AppSigv1
    apig-auth-iam:
      in: header
      name: unused
      type: apiKey
      x-apigateway-auth-type: IAM
```

表 7-15 参数说明

参数	是否必选	类型	说明
x-apigateway-auth-type	是	String	API网关认证方式，支持AppSigv1、IAM。
type	是	String	认证类型，仅支持apiKey。
name	是	String	用于认证的参数名称。
in	是	String	仅支持header。
description	否	String	描述信息。

7.9.2 x-apigateway-request-type

含义：API网关定义的API请求类型，支持public和private。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-request-type: 'public'
```

表 7-16 参数说明

参数	是否必选	类型	说明
x-apigateway-request-type	是	String	API类型，支持public和private。 • public：公开类型API，可以上架。 • private：私有类型API，不会被上架。

7.9.3 x-apigateway-match-mode

含义：API网关定义的API请求URL的匹配模式，支持NORMAL和SWA。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-match-mode: 'SWA'
```

表 7-17 参数说明

参数	是否必选	类型	说明
x-apigateway-match-mode	是	String	API匹配模式，支持SWA和NORMAL。 • SWA：前缀匹配，如“/prefix/foo”和“/prefix/bar”都会被“/prefix ”匹配，但“/prefixpart”却不会被匹配。 • NORMAL：绝对匹配，如“/prefix/foo”只能被“/prefix/foo”匹配。

7.9.4 x-apigateway-cors

含义：API网关定义的API请求是否支持跨域。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-cors: true
```

表 7-18 参数说明

参数	是否必选	类型	说明
x-apigateway-cors	是	boolean	是否支持开启跨域请求的标识。 • true：支持。 • false：不支持。

开启跨域访问的API请求，响应会增加如下头域：

头域名称	头域值	描述
Access-Control-Max-Age	172800	预检响应最大缓存时间。 单位：s。
Access-Control-Allow-Origin	*	允许任何域。
Access-Control-Allow-Headers	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	正式请求允许的头域。
Access-Control-Allow-Methods	GET，POST，PUT，DELETE，HEAD，OPTIONS，PATCH	正式请求允许的方法。

7.9.5 x-apigateway-is-send-fg-body-base64

含义：是否对与FunctionGraph交互场景的请求体进行Base64编码，boolean类型。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      "x-apigateway-is-send-fg-body-base64": true
```

表 7-19 参数说明

参数	是否必选	类型	说明
x-apigateway-is-send-fg-body-base64	否	boolean	是否对与FunctionGraph交互场景的请求体进行Base64编码。 • true：编码。 • false：不编码。

7.9.6 x-apigateway-any-method

含义：API网关定义的API请求方法，用以匹配未指定定义的HTTP方法。

作用域：Path Item Object(2.0)/Path Item Object(3.0)

示例：

```
paths:
  '/path':
    get:
      produces:
        - application/json
      responses:
        "200":
          description: "get response"
    x-apigateway-any-method:
      produces:
        - application/json
      responses:
        "200":
          description: "any response"
```

表 7-20 参数说明

参数	是否必选	类型	说明
x-apigateway-any-method	否	String	API请求方法。

7.9.7 x-apigateway-backend

含义：API网关定义的API后端服务定义。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      responses:
        default:
```

```
      description: "default response"
    x-apigateway-request-type: "public"
    x-apigateway-backend:
      type: "backend endpoint type"
```

表 7-21 参数说明

参数	是否必选	类型	说明
x-apigateway-backend	是	String	API后端服务定义。
type	是	String	后端服务类型，支持HTTP、HTTP-VPC、FUNCTION、MOCK。
parameters	否	**x-apigateway-backend.parameters**	后端参数定义。
httpEndpoints	否	**x-apigateway-backend.httpEndpoints**	HTTP类型后端服务定义。
httpVpcEndpoints	否	**x-apigateway-backend.httpVpcEndpoints**	HTTP-VPC类型后端服务定义。
functionEndpoints	否	**x-apigateway-backend.functionEndpoints**	FUNCTION类型后端服务定义。
mockEndpoints	否	**x-apigateway-backend.mockEndpoints**	MOCK类型后端服务定义。

7.9.8 x-apigateway-backend.parameters

含义：API网关定义的API后端参数定义。

作用域：**x-apigateway-backend**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      parameters:
```

```
    - name: "X-Auth-Token"
      description: "认证token"
      type: "string"
      in: "header"
      required: true
    - name: "userId"
      description: "用户名"
      type: "string"
      in: "path"
      required: true
  responses:
    default:
      description: "default response"
  x-apigateway-request-type: "public"
  x-apigateway-backend:
    type: "HTTP"
    parameters:
      - name: "userId"
        value: "userId"
        in: "query"
        origin: "REQUEST"
        description: "用户名"
      - name: "X-Invoke-User"
        value: "apigateway"
        in: "header"
        origin: "CONSTANT"
        description: "调用者"
```

表 7-22 参数说明

参数	是否必选	类型	说明
name	是	String	参数名称，长度不能超过32个字节，由字母、数字、下划线、连线或点组成，且必须以字母开头。 header位置的参数名称不区分大小写。
value	是	String	参数值，当参数来源为REQUEST时，值为请求参数名称。
in	是	String	参数位置，支持header、query、path。
origin	是	String	参数映射来源，支持REQUEST、CONSTANT。
description	否	String	参数含义描述。

7.9.9 x-apigateway-backend.httpEndpoints

含义：API网关定义的HTTP类型API后端服务定义。

作用域：**x-apigateway-backend**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
```

```
  parameters:
    - name: "X-Auth-Token"
      description: "认证token"
      type: "string"
      in: "header"
      required: true
  responses:
    default:
      description: "default response"
  x-apigateway-request-type: "public"
  x-apigateway-backend:
    type: "HTTP"
    httpEndpoints:
      address: "example.com"
      scheme: "http"
      method: "GET"
      path: "/users"
      timeout: 30000
```

表 7-23 参数说明

参数	是否必选	类型	说明
address	是	Array	后端服务地址，格式为：<域名或IP>:[port]。
scheme	是	String	后端请求协议定义，支持http、https。
method	是	String	后端请求方法，支持GET、POST、PUT、DELETE、HEAD、OPTIONS、PATCH、ANY。
path	是	String	后端请求路径，支持路径变量。
timeout	否	Number	后端请求超时时间，单位毫秒，缺省值为5000，取值范围为1~60000。

7.9.10 x-apigateway-backend.httpVpcEndpoints

含义：API网关定义的HTTP VPC类型API后端服务定义。

作用域：**x-apigateway-backend**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      parameters:
        - name: "X-Auth-Token"
          description: "认证token"
          type: "string"
          in: "header"
          required: true
      responses:
        default:
          description: "default response"
      x-apigateway-request-type: "public"
      x-apigateway-backend:
```

```
    type: "HTTP-VPC"
    httpVpcEndpoints:
      name: "vpc-test-1"
      scheme: "http"
      method: "GET"
      path: "/users"
      timeout: 30000
```

表 7-24 参数说明

参数	是否必选	类型	说明
name	是	Array	VPC通道名称。
scheme	是	String	后端请求协议定义，支持http、https。
method	是	String	后端请求方法，支持GET、POST、PUT、DELETE、HEAD、OPTIONS、PATCH、ANY。
path	是	String	后端请求路径，支持路径变量。
timeout	否	Number	后端请求超时时间，单位毫秒，缺省值为5000，取值范围为1 ~ 60000。

7.9.11 x-apigateway-backend.functionEndpoints

含义：API网关定义的FUNCTION类型API后端服务定义。

作用域：**x-apigateway-backend**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      parameters:
        - name: "X-Auth-Token"
          description: "认证token"
          type: "string"
          in: "header"
          required: true
      responses:
        default:
          description: "default response"
      x-apigateway-request-type: "public"
      x-apigateway-backend:
        type: "FUNCTION"
        functionEndpoints:
          version: "v1"
          function-urn: ""
          invocation-type: "synchronous"
          timeout: 30000
```

表 7-25 参数说明

参数	是否必选	类型	说明
function-urn	是	String	函数URN地址。
version	是	String	函数版本。
invocation-type	是	String	函数调用类型，支持异步或同步。
timeout	否	Number	函数超时时间，单位毫秒，缺省值为5000，取值范围为1~60000。

7.9.12 x-apigateway-backend.mockEndpoints

含义：API网关定义的MOCK类型API后端服务定义。

作用域：**x-apigateway-backend**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      parameters:
        - name: "X-Auth-Token"
          description: "认证token"
          type: "string"
          in: "header"
          required: true
      responses:
        default:
          description: "default response"
      x-apigateway-request-type: "public"
      x-apigateway-backend:
        type: "MOCK"
        mockEndpoints:
          result-content: "mocked"
```

表 7-26 参数说明

参数	是否必选	类型	说明
result-content	是	String	MOCK返回结果。

7.9.13 x-apigateway-backend-policies

含义：API网关定义的API后端策略。

作用域：**Operation Object(2.0)**/**Operation Object(3.0)**

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      responses:
        default:
          description: "default response"
      x-apigateway-request-type: "public"
      x-apigateway-backend:
        type: "backend endpoint type"
      x-apigateway-backend-policies:
        - type: "backend endpoint type"
          name: "backend policy name"
          conditions:
            - type: "equal/enum/pattern",
              value: "string",
              origin: "source/request_parameter",
              parameter_name: "string"
```

表 7-27 参数说明

参数	是否必选	类型	说明
x-apigateway-backend-policies	否	x-apigateway-backend-policies	策略后端。
type	是	String	后端服务类型，支持HTTP、HTTP-VPC、FUNCTION、MOCK。
name	是	String	后端策略名称。
parameters	否	**x-apigateway-backend.parameters**	后端参数定义。
httpEndpoints	否	**x-apigateway-backend.httpEndpoints**	HTTP类型服务定义。
httpVpcEndpoints	否	**x-apigateway-backend.httpVpcEndpoints**	HTTP-VPC类型服务定义。
functionEndpoints	否	**x-apigateway-backend.functionEndpoints**	FUNCTION类型服务定义。
mockEndpoints	否	**x-apigateway-backend.mockEndpoints**	MOCK类型服务定义。

参数	是否必选	类型	说明
conditions	是	x-apigateway-backend-policies.conditions	策略条件数组。

7.9.14 x-apigateway-backend-policies.conditions

含义：API网关定义的API后端策略条件。

作用域：x-apigateway-backend-policies

示例：

```
paths:
  '/users/{userId}':
    get:
      produces:
        - "application/json"
      responses:
        default:
          description: "default response"
      x-apigateway-request-type: "public"
      x-apigateway-backend:
        type: "backend endpoint type"
      x-apigateway-backend-policies:
        - type: "backend endpoint type"
          name: "backend policy name"
          conditions:
            - type: "equal/enum/pattern",
              value: "string",
              origin: "source/request_parameter",
              parameter_name: "string"
```

表 7-28 参数说明

参数	是否必选	类型	说明
type	是	String	策略条件类型，支持equal、enum、pattern。
value	是	String	策略条件值。
origin	是	String	策略条件输入来源，支持source、request。
parameter	否	String	策略条件输入来源为request时，请求入参的名称。

7.9.15 x-apigateway-ratelimit

含义：引用流控策略。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-ratelimit: 'customRatelimitName'
```

表 7-29 参数说明

参数	是否必选	类型	说明
x-apigateway-ratelimit	否	String	流控策略。

7.9.16 x-apigateway-ratelimits

含义：流控策略名称与关联策略映射。

作用域：Swagger Object

示例：

```
x-apigateway-ratelimits:
  customRatelimitName:
    api-limit: 200
    app-limit: 200
    user-limit: 200
    ip-limit: 200
    interval: 1
    unit: second/minute/hour
    shared: true
    special:
      - type: APP
        limit: 100
        instance: xxxxxxxxx
```

表 7-30 参数说明

参数	是否必选	类型	说明
customRatelimitName	否	x-apigateway-ratelimits.policy	指定名称的流控策略。 要使用该策略，将x-apigateway-ratelimit属性值引用为该策略名称。

7.9.17 x-apigateway-ratelimits.policy

含义：流控策略定义。

作用域：x-apigateway-ratelimits

示例：

```
x-apigateway-ratelimits:
  customRatelimitName:
    api-limit: 200
    app-limit: 200
    user-limit: 200
    ip-limit: 200
    interval: 1
    unit: MINUTE
    shared: false
    special:
      - type: USER
        limit: 100
        instance: xxxxxxx
```

表 7-31 参数说明

参数	是否必选	类型	说明
api-limit	是	Number	API访问次数限制。
user-limit	否	Number	用户访问次数限制。
app-limit	否	Number	应用访问次数限制。
ip-limit	否	Number	源IP访问次数限制。
interval	是	Number	流控策略时间周期。
unit	是	String	流控策略时间周期单位，支持SECOND、MINUTE、HOUR、DAY。
shared	否	Boolean	是否共享流控策略。
special	否	**x-apigateway-ratelimits.policy.special** 对象数组	特殊流控策略。

7.9.18 x-apigateway-ratelimits.policy.special

含义：特殊流控策略定义。

作用域：**x-apigateway-ratelimits.policy**

示例：

```
x-apigateway-ratelimits:
  customRatelimitName:
    api-limit: 200
    app-limit: 200
    user-limit: 200
    ip-limit: 200
    interval: 1
    unit: MINUTE
    shared: false
    special:
      - type: USER
        limit: 100
        instance: xxxxxxxx
```

表 7-32 参数说明

参数	是否必选	类型	说明
type	是	String	特殊流控策略类型，支持APP、USER。
limit	是	Number	API的访问次数。
instance	是	String	特殊APP或USER的对象标识。

7.9.19 x-apigateway-access-control

含义：引用访问控制策略。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-access-control: 'customAccessControlName'
```

表 7-33 参数说明

参数	是否必选	类型	说明
x-apigateway-access-control	否	String	访问控制策略。

7.9.20 x-apigateway-access-controls

含义：访问控制策略名称与关联策略映射。

作用域：Swagger Object

示例：

```
x-apigateway-access-controls:
  customAccessControlName:
    acl-type: "DENY"
    entity-type: "IP"
    value: 127.0.0.1,192.168.0.1/16
```

表 7-34 参数说明

参数	是否必选	类型	说明
customAccessControlName	否	x-apigateway-access-controls.policy	指定名称的访问控制策略。 如果使用该策略，需要将x-apigateway-access-control属性值引用为该策略名称。

7.9.21 x-apigateway-access-controls.policy

含义：访问控制策略定义。

作用域：x-apigateway-access-controls

示例：

```
x-apigateway-access-controls:
  customAccessControlName:
    acl-type: "DENY"
    entity-type: "IP"
    value: 127.0.0.1,192.168.0.1/16
```

表 7-35 参数说明

参数	是否必选	类型	说明
acl-type	是	String	访问控制行为，支持PERMIT、DENY。
entity-type	是	String	访问控制对象，仅支持IP。
value	是	String	访问控制策略值，多个值以“,”间隔。

7.9.22 x-apigateway-plugins

含义：API网关定义的API插件服务。

作用域：Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  '/path':
    get:
      x-apigateway-plugins: ['Plugin_mock']
```

表 7-36 参数说明

参数	是否必选	类型	说明
x-apigateway-plugins	否	Array	API所绑定的插件名列表。

7.9.23 x-apigateway-auth-opt

含义：APP简易认证方式参数。

作用域：Security Scheme Object(2.0)/Security Scheme Object(3.0)

Swagger示例：

```
securityDefinitions:
  apig-auth-app:
    type: apiKey
    name: Authorization
    in: header
    x-apigateway-auth-type: AppSigv1
  apig-auth-app-header:
    type: apiKey
    name: Authorization
    in: header
    x-apigateway-auth-opt:
      appcode-auth-type: header
    x-apigateway-auth-type: AppSigv1
  apig-auth-iam:
    type: apiKey
    name: unused
    in: header
    x-apigateway-auth-type: IAM
```

OpenAPI示例：

```
securitySchemes:
    apig-auth-app:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-type: AppSigv1
    apig-auth-app-header:
      in: header
      name: Authorization
      type: apiKey
      x-apigateway-auth-opt:
        appcode-auth-type: header
      x-apigateway-auth-type: AppSigv1
    apig-auth-iam:
      in: header
      name: unused
      type: apiKey
      x-apigateway-auth-type: IAM
```

表 7-37 参数说明

参数	是否必选	类型	说明
appcode-auth-type	否	String	AppCode简易认证类型，默认为disable。 • disable：不开启简易认证 • header：开启简易认证且AppCode位置在HEADER。

7.9.24 x-apigateway-result-normal-sample

含义：成功响应示例。

作用域： Operation Responses

示例：

```
paths:
  /:
    get:
      responses:
        default:
          x-apigateway-result-normal-sample: success
```

7.9.25 x-apigateway-result-failure-sample

含义：失败响应示例。

作用域： Operation Responses

示例：

```
paths:
  /:
    get:
      responses:
        default:
          x-apigateway-result-failure-sample: fail
```

7.9.26 x-apigateway-authorizer

含义：自定义认证对象。

作用域： Security Scheme Object

示例：

```
x-apigateway-authorizer:
    auth_downgrade_enabled: false
    authorizer_alias_uri: ''
    authorizer_type: FUNC
    authorizer_uri: >-
      urn:fss:region:73d69ae0cfcf460190522d**********:function:default:DSFA
    authorizer_version: latest
    identities:
      - location: HEADER
        name: test
        validation: ''
    need_body: false
```

```
network_type: V2
retry_attempts: 0
timeout: 5000
ttl: 0
type: FRONTEND
```

表 7-38 参数说明

参数	是否必选	类型	说明
authorizer_type	是	String	只能为：FUNC。
authorizer_uri	是	String	函数地址。
auth_downgrade_enabled	否	Boolean	宽松模式开关，默认为false。
authorizer_alias_uri	否	String	函数别名地址。 当函数别名URN和函数版本同时传入时，函数版本将被忽略，只会使用函数别名URN。
authorizer_version	否	String	函数版本。 当函数别名URN和函数版本同时传入时，函数版本将被忽略，只会使用函数别名URN。 最大长度：64。
need_body	否	Boolean	是否发送body。
identities	否	Array of Identity objects	认证来源。
network_type	否	String	对接函数的网络架构类型。 ● V1：非VPC网络架构 ● V2：VPC网络架构 缺省值：V1。
retry_attempts	否	Number	重试次数。
timeout	否	Number	超时时间。
ttl	否	Number	缓存时间。
type	是	String	自定义认证类型。 ● FRONTEND：前端 ● BACKEND：后端

表 7-39 Identity

参数	是否必选	类型	说明
name	是	String	参数名称。
location	是	String	参数位置。
validation	否	String	参数校验表达式，默认为null，不做校验。

7.9.27 x-apigateway-response

含义：API的网关响应名称。

作用域： Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  /:
    get:
      x-apigateway-response: test
```

7.9.28 x-apigateway-responses

含义：自定义网关响应类型。

作用域： Operation Object(2.0)/Operation Object(3.0)

示例：

```
x-apigateway-responses:
  default:
    ACCESS_DENIED:
      status: 403
      body:
        application/json: >-
          {"error_code":"$context.error.code","error_msg":"Access
          denied","request_id":"$context.requestId"}
```

7.9.29 x-apigateway-pass-through

含义：API的请求参数是否透传。always为是，never为否。

作用域： Operation Object(2.0)/Operation Object(3.0)

示例：

```
paths:
  /:
    get:
      parameters:
        - maximum: 0
          minimum: 0
          maxLength: 0
          minLength: 0
          type: string
          x-apigateway-orchestrations: []
          x-apigateway-pass-through: always
```

```
      x-apigateway-sample: ''
      name: test
      in: query
      required: true
```

7.9.30 x-apigateway-sample

含义： API的请求参数示例值。

作用域： **Operation Object(2.0)**/**Operation Object(3.0)**

示例：

```
paths:
  /:
    get:
      parameters:
        - maximum: 0
          minimum: 0
          maxLength: 0
          minLength: 0
          type: string
          x-apigateway-orchestrations: []
          x-apigateway-pass-through: always
          x-apigateway-sample: 'test-sample'
          name: test
          in: query
          required: true
```

7.9.31 x-apigateway-content-type

含义： API的请求内容类型。

作用域： **Operation Object(2.0)**

示例：

```
paths:
  /:
    get:
      x-apigateway-content-type: application/json
```

7.9.32 x-apigateway-orchestrations

含义： API请求参数的编排规则列表。

作用域： **Operation Object(2.0)**/**Operation Object(3.0)**

示例：

```
paths:
  /:
    get:
      parameters:
        - maximum: 0
          minimum: 0
          maxLength: 0
          minLength: 0
          type: string
          x-apigateway-orchestrations:
            - Orchestration_114w
          x-apigateway-pass-through: always
          x-apigateway-sample: ''
          name: test
```

```
      in: query
      required: true`
```


8 配置 API 策略

8.1 配置 API 的传统策略

8.1.1 配置 API 的流量控制

流量控制支持从用户、凭据和时间段等不同的维度限制对API的调用次数，保护后端服务。支持按分/秒粒度级别的流量控制。为了提供持续稳定的服务，您可以通过配置流控策略，针对部分API进行流量控制。

约束与限制

- API配置流控策略相当于流控策略同步绑定了API。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。
- 如果API未绑定流控策略，流控限制值为实例“配置参数”中“ratelimit_api_limits”的参数运行值。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建流量控制策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“传统策略 > 流量控制”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-1 流量控制参数说明

参数	说明
策略名称	API流控策略名称。支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3-64个字符。
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，单位可选秒、分钟、小时、天。 ● 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“凭据流量限制”配合使用，表示单位时间内的单个凭据请求次数上限。 ● 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，**仅在API的安全认证方式为APP认证或IAM认证时适用**。 ● 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。 ● 如果主账号下有多个子用户访问API，按主账号累计的调用次数进行限制。
凭据流量限制	单个凭据调用API次数上限，**仅在API的安全认证方式为APP认证时适用**。 ● 不超过“用户流量限制”和“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的凭据请求次数上限。
源IP流量限制	单个IP地址（客户端IP地址）调用API次数上限。您可以选择配置实例的“real_ip_from_xff”参数，使用X-Forwarded-For头中的IP作为流控的判断依据。 ● 不超过“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的IP地址请求次数上限。
描述	关于控制策略的描述。长度为1~255个字符。

步骤7 单击“确定”。

- 如果需要对某个凭据进行流量控制，可以在“流量控制策略”中**为流量控制策略配置特殊凭据**。
- 如果需要对某个租户进行流量控制，可以在“流量控制策略”中**为流量控制策略配置特殊租户**。

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

为流量控制策略配置特殊凭据

如果希望对某个凭据进行流量控制，可以通过在流控策略中添加特殊凭据实现。把凭据添加到流控策略中后，该凭据的凭据流量限制受特殊凭据的阈值限制，API流量限制和用户流量限制受流控策略限制。

步骤1 在流控策略详情页面，单击“特殊凭据”页签，进入特殊凭据页面。

步骤2 单击“添加特殊凭据”，弹出“添加特殊凭据”对话框。

步骤3 通过以下两种方式，添加特殊凭据。

- 添加已有凭据：单击“已有凭据”，选择已有凭据，输入阈值。
- 添加其他凭据：单击“其他”，输入其他用户的凭据ID和阈值。

说明

特殊凭据流控值和凭据流量限制值共同作用时，以特殊凭据流控值为准。

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

为流量控制策略配置特殊租户

如果希望对某个租户进行流量控制，可以通过在流控策略中添加特殊租户实现。把租户添加到流控策略中后，该租户的用户流量限制受特殊租户的阈值限制，API流量限制和应用流量限制受流控策略限制。

步骤1 在流控策略详情页面，单击“特殊租户”，进入特殊租户页面。

步骤2 单击“添加特殊租户”，弹出“添加特殊租户”对话框。

步骤3 根据下表参数说明，输入租户信息。

表 8-2 特殊租户信息

参数	说明
租户ID	租户ID为账号ID或项目ID。 ● 绑定APP认证的API时，租户ID为项目ID，**获取项目ID**。 ● 绑定华为IAM认证的API时，租户ID为账号ID，不支持细分到IAM用户维度，**获取账号名和账号ID**。
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4 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

8.1.2 配置 API 的访问控制

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地址和账户，您可以通过设置IP地址或账户的黑白名单来禁止/允许某个IP地址/账号名/账号ID访问API。实例级访问控制策略请参考**表10-1**。

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。

约束与限制

- 同一个API在同一个环境中只能绑定一个相同限制类型的访问控制策略，一个访问控制策略可以绑定多个API。
- 2022年12月31日后创建的实例支持限制调用API的**账号ID**，在这之前创建的专享版实例不支持，如需使用，请联系客服。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建访问控制策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“传统策略 > 访问控制”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-3 访问控制参数说明

参数	说明
策略名称	访问控制策略的名称。支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~64个字符。
类型	控制访问API的类型。 ● IP地址：限制调用API的IP地址。 ● 账号名：仅适用**IAM认证**类型的API，限制调用API的账号名。仅支持配置账号名，对账号名及账号名下的IAM用户名做限制，不支持配置IAM用户名。 可以配置单账号名或多账号名，多账号名以英文格式下的逗号“,”隔开，账号名支持除英文格式下“,”以外的任意ASCII字符，账号名长度限制在1~64个字符，不支持纯数字。多账号名字符的总长度不超过1024。 ● 账号ID：仅适用**IAM认证**类型的API，限制调用API的账号ID。仅支持配置账号ID，对账号ID及账号ID下的IAM用户ID做限制，不支持配置IAM用户ID。 可以配置单账号ID或多账号ID，多账号ID以英文格式下的逗号“,”隔开。账号ID为英文字母、数字组成的32位字符；多账号ID字符的总长度不超过1024。 **说明** ● **一个API同时绑定两种类型的访问控制策略：**账户维度的账户名类型和账号ID类型。访问API时，如果同时有黑白名单，只校验白名单，校验通过则访问成功；如果只有黑名单或白名单，校验通过的结果为“且”逻辑。 ● **一个API同时绑定三种类型的访问控制策略：**IP维度的IP类型、账户维度的账号名类型和账号ID类型。访问API时，IP维度和账户维度为“且”的关系，其中一方校验失败则访问失败。（一个API同时绑定IP类型和账号名/账号ID类型的访问控制策略，这两种类型的判断逻辑与三种类型的判断逻辑相同）。
动作	包括“允许”和“禁止”。 和“类型”配合使用，允许/禁止指定的IP地址/账号名/账号ID访问API。

参数	说明
IP地址	**仅当“类型”为“IP地址”时需要配置。** 输入允许或者禁止访问API的IP地址，或IP地址范围。 **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。
账号名	**仅当“类型”为“账号名”时需要配置。** 输入允许或者禁止访问API的账号名，多个账号名之间使用英文逗号“,”隔开。 您可以单击控制台右上角的用户名，选择“我的凭证”，在“我的凭证”页面获取用户的账号名。
账号ID	**仅当“类型”为“账号ID”时需要配置。** 输入允许或者禁止访问API的账号ID，多个账号ID之间使用英文逗号“,”隔开。 您可以单击控制台右上角的用户名，选择“我的凭证”，在“我的凭证”页面获取用户的账号ID。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

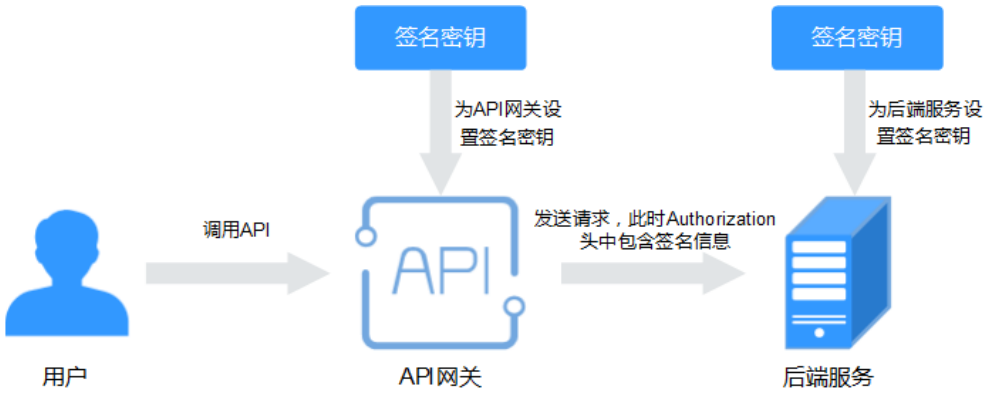
----结束

8.1.3 配置 API 的后端服务签名校验

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。

图 8-1 签名密钥流程图



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等）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。

约束与限制

- 同一个环境中一个API只能绑定一个签名密钥，一个签名密钥可以绑定多个API。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建签名密钥策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中选择“传统策略 > 签名密钥”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-4 签名密钥参数说明

参数	说明
密钥名称	自定义名称，用于识别不同的密钥。支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~64个字符。

参数	说明
类型	选择签名密钥的认证类型，可选择“HMAC”、“Basic Auth”、“AES”和“Public Key”。 在实例的**配置参数**中开启“public_key_enable”功能后，才支持选择“Public Key”类型。
签名算法	选择AES的签名算法，包含以下两种： • aes-128-cfb • aes-256-cfb
Key	根据选择的密钥类型，填写不同的密钥信息。 • HMAC：填写APP认证所使用密钥对的Key。 • Basic Auth：填写basic认证所使用的用户名。 • AES：填写AES认证所使用的密钥key。 • Public Key：填写public_key认证所使用的公钥。
Secret	根据选择的密钥类型，填写不同的密钥信息。 • HMAC：填写APP认证所使用密钥对的Secret。 • Basic Auth：填写basic认证所使用的密码。 • aes：填写aes认证所使用的向量。 • Public Key：填写Public Key认证所使用的私钥。
确认Secret	填写与Secret一致的值。

步骤7 单击“确定”。

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

验证签名结果

参考**签名算法**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。

8.2 配置 API 的插件策略

8.2.1 配置 API 的跨域资源共享

出于安全性考虑，浏览器会限制从页面脚本内发起的跨域请求，此时页面只能访问当前域的资源。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。更多跨域访问的说明请参见**跨域调用APIG开放的API**。

跨域资源共享策略为跨域访问提供指定预检请求头和响应头、自动创建跨域预检请求API的扩展能力，可快速、灵活的实现API的跨域访问。

说明

- 如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。
- 策略参数会明文展示，为防止信息泄露，请谨慎配置。

约束与限制

- 同一个环境中，一个API只能被一个跨域共享策略绑定，但一个跨域共享策略可以绑定多个API。
- 同一API分组下，相同请求路径的所有API，只能绑定同一个跨域资源共享策略。
- 如果API开启了“支持CORS”功能的同时，也绑定了跨域资源共享策略，则以绑定的策略为准。
- 如果某个请求路径下有OPTIONS方法的API，则该请求路径下的所有API均不允许绑定跨域资源共享策略。
- **为策略绑定API**时，API的请求方法必须为allow_methods中允许的请求方法。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建跨域资源共享策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 跨域资源共享”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-5 跨域资源共享策略配置

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“跨域资源共享”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
Allowed Origins	Access-Control-Allow-Origin响应头，指定允许访问API的外域URI，多个URI之间使用英文逗号隔开。 对于未携带身份凭证的请求，可以把参数值设置为“*”，表示允许来自所有域的访问请求。
Allowed Methods	Access-Control-Allow-Methods响应头，指定允许使用的HTTP请求方法，多个请求方法之间使用英文逗号隔开。
Allowed Headers	Access-Control-Allow-Headers响应头，指定XMLHttpRequest请求中允许携带的请求头字段，多个请求头之间使用英文逗号隔开。 其中，简单请求头Accept、Accept-Language、Content-Language、Content-Type（取值仅限为application/x-www-form-urlencoded、multipart/form-data、text/plain时）默认允许在请求中携带，无需在该参数中设置。 **说明** • 创建跨域资源共享策略时，默认不配置Allowed Headers，不允许跨域请求携带任何自定义请求头。 • 配置Allowed Headers为“*”，表示允许跨域请求头携带所有请求头。
Exposed Headers	Access-Control-Expose-Headers响应头，指定XMLHttpRequest请求响应中允许携带的响应头字段，多个响应头之间使用英文逗号隔开。 其中，基本响应头Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma默认允许在响应中携带，无需在该参数中设置。 **说明** • 创建跨域资源共享策略时，默认不配置Exposed Headers，不允许浏览器的JavaScript代码解析跨域访问获得的响应头内容（除XMLHttpRequest对象的getResponseHeader()方法获得的基本响应头，Cache-Control、Content-Language、Content-Type、Expires、Last-Modified、Pragma）。 • 配置Exposed Headers为“*”，表示允许浏览器的JavaScript代码解析跨域访问获得的所有响应头内容。

参数	说明
Maximum Age	Access-Control-Max-Age响应头，指定本次预检请求的有效期，单位为秒。在有效期内，无需再次发出预检请求。
Allowed Credentials	Access-Control-Allow-Credentials响应头，定XMLHttpRequest请求中是否允许携带Cookie。 • 开关开启表示允许。 • 开关关闭表示不允许。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "allow_origin": "*",
  "allow_methods": "GET,POST,PUT",
  "allow_headers": "Content-Type,Accept,Accept-Ranges,Cache-Control",
  "expose_headers": "X-Request-Id,X-Apig-Latency",
  "max_age": 86400,
  "allow_credentials": true
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

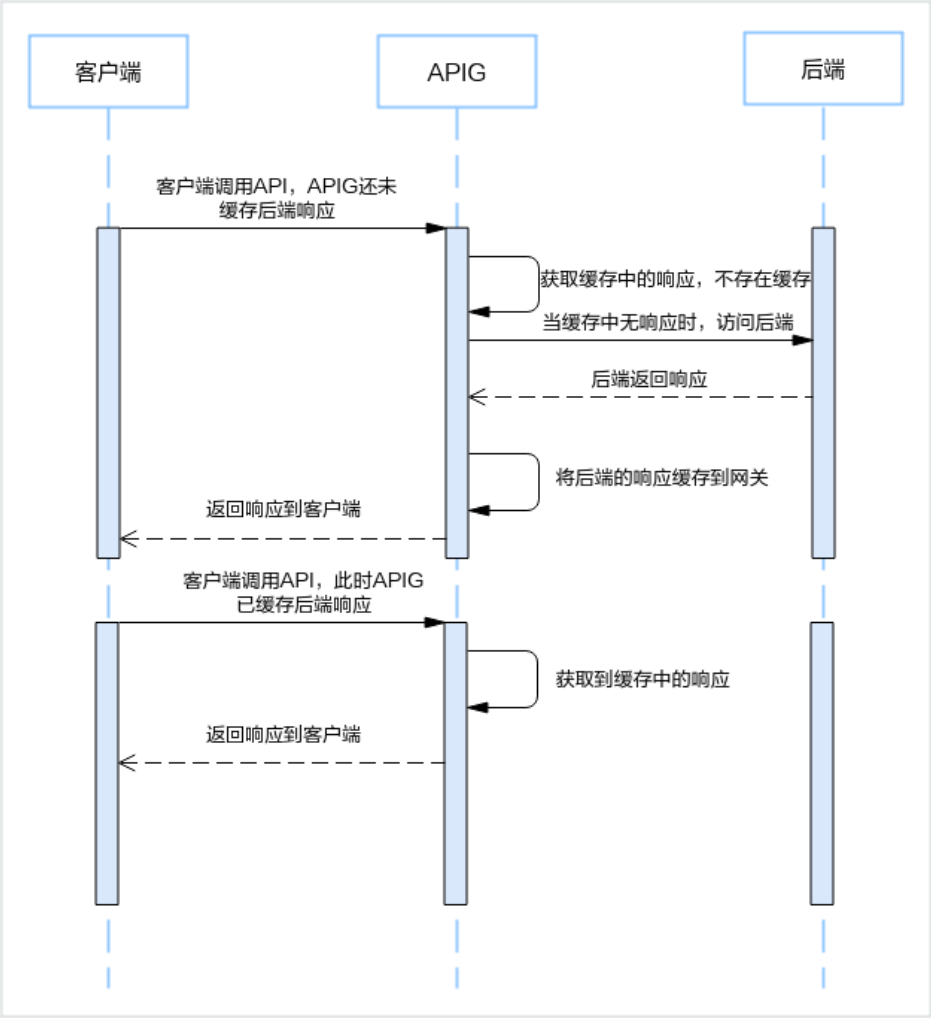
8.2.2 配置 API 的响应缓存

您可以通过配置响应缓存策略将后端服务（服务端）返回的应答缓存在API网关中，当客户端发送相同的请求时，网关不用向后端传递请求，直接返回缓存的应答。有效降低后端的负荷，同时减少API调用的延迟。

须知

- 当使用响应缓存策略时，后端的响应内容会缓存到API网关中，此时API网关不支持缓存数据加密，对于响应中的敏感数据存在安全风险，请谨慎配置策略。
- 策略参数会明文展示，为防止信息泄露，请谨慎配置。

响应缓存策略原理图如下：



约束与限制

- 同一个环境中，一个API只能被一个响应缓存策略绑定，但一个响应缓存策略可以绑定多个API。
- 响应缓存策略仅支持使用GET、HEAD方法的API。
- 超过1M的响应体不会被缓存。
- 用于后端响应内容的缓存大小为128m。
- API网关遵守后端应答中的Cache-Control头的约定来处理缓存，如果后端不返回Cache-Control头，则默认缓存，使用策略中配置的ttl字段作为缓存超期时间。
- API网关默认不处理客户端的Cache-Control头，可以通过策略中的client_cache_control来进行配置。

- Cache-Control拓展缓存指令不是核心HTTP缓存标准文档的一部分，本策略不支持拓展缓存指令。
  ```
  Cache-control: immutable
  Cache-control: stale-while-revalidate=<seconds>
  Cache-control: stale-if-error=<seconds>
  ```
- API网关仅支持缓存**Content-Type**、**Content-Encoding**、**Content-Language**头，如需要缓存更多的Headers，请在策略的“允许缓存的后端响应头”参数处添加，但是无法添加API网关增加的系统响应头（x-apig-*，x-request-id等）。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建响应缓存策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 响应缓存”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-6 响应缓存参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“响应缓存”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
响应缓存键	配置参数作为响应缓存键，用于区分不同的缓存。 • system_params类型：配置不同的网关内置系统参数作为响应缓存键来区分缓存。配置参数请参考**网关内置参数**。 • parameters类型：配置不同的请求query参数作为响应缓存键来区分缓存。 • headers类型：配置不同的请求头作为响应缓存键来区分缓存。

参数	说明
HTTP参数	根据HTTP响应码和缓存时长来决定是否缓存，以及缓存的有效时间。 如果不配置HTTP参数，那么HTTP响应码默认值为200，取值范围：200~599。缓存时长默认值为300s，取值范围：1s~720000s。
缓存策略模式	网关通过客户端请求中的**Cache-Control**请求头来处理缓存，默认拒绝所有客户端带**Cache-Control**头的请求。 ● all：允许所有客户端带**Cache-Control**头的请求。 ● off：拒绝所有客户端带**Cache-Control**头的请求。 ● apps：允许appId（凭据ID）取值在datas列表中的客户端。
允许缓存的后端响应头	对于后端的响应Headers，默认仅支持缓存**Content-Type**，**Content-Encoding**，**Content-Language**头。如果需要缓存更多的Headers，请在“允许缓存的后端响应头”处添加，但是无法添加API网关增加的系统响应头（x-apig-*，x-request-id等）。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "cache_key": {
    "system_params": [
      "$context.sourceIp",
      "$context.requestId"
    ],
    "parameters": [
      "demo_parameters"
    ],
    "headers": [
      "demo_header"
    ]
  },
  "cache_http_status_and_ttl": [
    {
      "http_status": [
        200
      ],
      "ttl": 300
    }
  ],
  "client_cache_control": {
    "mode": "apps",
    "datas": [
      "demo_app_id_1,demo_app_id_2"
    ]
  },
```



```
 "cacheable_headers": [
   "demo_cacheable_headers_1,demo_cacheable_headers_2"
 ]
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

8.2.3 配置 API 的 HTTP 响应头

API响应是指API网关向客户端返回的响应，HTTP响应头是API响应中的一部分。您可以自定义HTTP响应头，在返回的API响应中指定您配置的响应头。

说明

- 如果此策略在当前实例中不支持，请联系技术支持升级实例到最新版本。
- 策略参数会明文展示，为防止信息泄露，请谨慎配置。

约束与限制

- 同一个环境中，一个API只能被一个HTTP响应头策略绑定，但一个HTTP响应头策略可以绑定多个API。
- 无法修改API网关增加的系统响应头（x-apig-*，x-request-id等），包括API网关提供的CORS功能增加的响应头。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建 HTTP 响应头策略

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > HTTP响应头管理”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-7 HTTP 响应头参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“HTTP响应头”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
Name	响应头名称。每个策略中不能添加重复名称的响应头（不区分大小写），且最多添加10条响应头。 支持英文，数字，点，中划线，且只能以英文开头，长度为1~32个字符，不区分大小写。注意，name不能以 x-apig- 和 access-control- 开头，且不能为x-request-id，Transfer-Encoding，Connection，Date或server。
Value_type	响应头的类型。 system_parameter：使用系统参数作为响应头的value。 custom_value：自定义内容作为响应头的value。 字符串：
Value	响应头的值。当“Action”为“Delete”时响应头的值不生效，可为空。长度为1-255字符。

参数	说明
Action	响应头操作，您可以覆盖、添加、删除、跳过或新增指定的响应头。 **Override**：覆盖 ● 当API响应中存在指定的响应头时，使用当前响应头的值覆盖已有响应头的值。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，该操作只会按当前响应头的值返回一条响应头记录。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Append**：添加 ● 当API响应中存在指定的响应头时，将当前响应头的值添加到已有响应头值之后，用逗号分隔。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，会将多个响应头的值用“，”拼接后，再添加当前响应头的值。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Delete**：删除 ● 当API响应中存在指定的响应头时，删除当前响应头。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，删除所有相同名称的响应头。 **Skip**：跳过 ● 当API响应中存在指定的响应头时，跳过当前响应头。 ● 当API响应中存在多个与指定响应头相同名称的响应头时，均不作处理直接返回。 ● 当API响应中不存在指定的响应头时，添加当前响应头。 **Add**：新增 无论API响应中是否存在指定的响应头，都添加当前响应头。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "response_headers": [
    {
```



```
        "name": "test",
        "value": "test",
        "action": "append"
      },
      {
        "name": "test1",
        "value": "test1",
        "action": "override"
      }
   ]
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

8.2.4 配置 API 的流量控制 2.0

流量控制2.0策略可以限制单位时间内API的被调用次数，支持参数流控、基础流控和基于基础流控的特殊流控。

- 基础流控

  可以对API、用户、凭据、源IP进行多维度流控，与已有的**配置API的流量控制**功能一致但不兼容。
- 参数流控

  支持根据Header、Path、Method、Query以及系统变量中的参数值进行自定义流控。
- 基于基础流控的特殊流控

  对某个凭据或租户进行特定的流控。

说明

如果此策略在当前实例中不支持，可**提交工单**升级实例到最新版本。

约束与限制

- 同一个环境中，一个API只能被一个流量控制2.0策略绑定，但一个流量控制2.0策略可以绑定多个API。
- 如果一个API绑定流量控制策略后，继续绑定流量控制2.0策略，流量控制策略会失效。
- 参数流控的参数支持1~32个字符；参数流控的规则最多可定义100个。
- 策略内容最大长度65535。

- 策略参数会明文展示，为防止信息泄露，请谨慎配置。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建流量控制 2.0 策略

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 流量控制2.0”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-8 流量控制 2.0 参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“流量控制2.0”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
流控类型	推荐使用高性能流控。 • 高精度流控：高并发场景下实例内部会有一定的性能损耗，适用于并发量较小的场景。 • 高性能流控：高并发场景下实例内部性能损耗较小，单位时间内会偶现较小的误差值，适用于并发量较大的场景。 • 单机流控：实例的每个节点各自进行流控，高并发场景下实例内部性能损耗最小，单位时间内会存在一定的误差值，适用于并发量更大的场景。
策略生效范围	• 单个API生效 对单个API进行流量统计和控制。 • API共享生效 对绑定了该策略的所有API进行总流量统计和控制。

参数	说明
时长	流量限制的时长，单位可选秒、分钟、小时、天。 ● 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“凭据流量限制”配合使用，表示单位时间内的单个凭据请求次数上限。 ● 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，如果API认证方式为IAM认证，用户流量根据项目ID来限制；如果API认证方式为APP认证，用户流量根据账号ID来限制。账号ID和项目ID请参考下文“特殊租户”配置说明。 ● 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。 ● 如果主账号下有多个子用户访问API，按主账号累计的调用次数进行限制。
凭据流量限制	单个凭据调用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“API流量限制”。 ● 与“时长”配合使用，表示单位时间内的单个凭据请求次数上限。
源IP流量限制	单个IP地址调用API次数上限。您可以选择配置实例的“real_ip_from_xff”参数使用X-Forwarded-For头中的IP作为流控的判断依据。 ● 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。
参数流控配置	参数流控配置开关。开启后，以参数维度进行流控限制。

参数	说明
定义参数	定义用于规则匹配的参数。 ● 参数位置：用于规则匹配的参数位置。 – path：API请求的URI，系统默认配置。 – method：API请求方法，系统默认配置。 – Header：请求头的key值。**建议不要设置敏感信息，以防泄露。** – Query：QueryString的key值。 – System：系统参数。 ● 参数：用于判断与规则匹配中的参数值是否匹配。
定义规则	定义规则的匹配条件，以及API流量限制和时长。 单击“添加规则”，可添加多个规则。 ● 规则 单击  ，可添加多个条件表达式，选择“定义参数”中的参数名和判断条件，以及输入参数值。 – =为等于 – !=为不等于 – pattern为正则表达式 – enum为枚举值，多个参数值之间用英文逗号分隔 ● API流量限制 API调用次数的最大值。 ● 时长 定义规则的流量控制时长，如果此处不配置时长，规则的流量控制时长以“策略基本信息”的时长为准。 例如，在“定义参数”中添加参数“Host”，参数位置选择“Header”；在“定义规则”中添加一条规则，匹配条件设置成“Host = www.abc.com”，API流量限制为10，时长为60s。表示在60s内，对于请求头域中Host参数等于“www.abc.com”的API，且API调用次数达到10，参数流控生效。
特殊流控配置	特殊流控配置开关。开启后，“基础流控”的用户流量限制/凭据流量限制与“特殊流控”的特殊租户/特殊凭据共同作用时，以特殊流控值为准。
特殊租户	租户ID为账号ID或项目ID。 ● 绑定APP认证的API时，租户ID为项目ID，**获取项目ID**。 ● 绑定华为IAM认证的API时，租户ID为账号ID，不支持细分到IAM用户维度，**获取账号名和账号ID**。 阈值为单位时间内，此租户访问API的最大值，不超过“基础流控”的API流量限制值。

参数	说明
特殊凭据	选择已有凭据，阈值为单位时间内，此凭据访问API的最大值，不超过“基础流控”的API流量限制值。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "scope": "basic",
  "default_interval": 60,
  "default_time_unit": "second",
  "api_limit": 100,
  "app_limit": 50,
  "user_limit": 50,
  "ip_limit": 20,
  "specials": [
    {
      "type": "app",
      "policies": [
        {
          "key": "e9230d70c749408eb3d1e838850cdd23",
          "limit": 10
        }
      ]
    },
    {
      "type": "user",
      "policies": [
        {
          "key": "878f1b87f71c40a7a15db0998f358bb9",
          "limit": 10
        }
      ]
    }
  ],
  "algorithm": "counter",
  "parameters": [
    {
      "id": "3wuj354lpptv0toe0",
      "value": "reqPath",
      "type": "path",
      "name": "reqPath"
    },
    {
      "id": "53h7e7j11u38l3ocp",
      "value": "method",
      "type": "method",
      "name": "method"
    },
    {
      "id": "vv502bnb6g40td8u0",
      "value": "Host",
      "type": "header",
      "name": "Host"
    }
  ],
```



```
 "rules": [
  {
    "match_regex": "[\"Host\",\"==\",\"www.abc.com\"]",
    "rule_name": "u8mb",
    "time_unit": "second",
    "interval": 2,
    "limit": 5
  }
 ]
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

8.2.5 配置 API 的 Kafka 日志推送

Kafka日志推送策略提供了把API的详细调用日志推送到Kafka的能力，方便用户获取API的调用日志信息。

说明

如果此策略在当前实例中不支持，可**提交工单**升级实例到最新版本。

约束与限制

- 同一个环境中，一个API只能被一个Kafka日志推送策略绑定，但一个Kafka日志推送策略可以绑定多个API。
- 同一个APIG实例内最多可创建5个Kafka日志推送策略。
- API绑定Kafka日志推送策略后，性能将损耗30%。性能数据请参考**产品规格差异**。
- 日志支持最大推送大小为4K，请求体/响应体支持最大推送大小为1K，超出部分会被截断。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建 Kafka 日志推送策略

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > Kafka日志推送”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-9 Kafka 日志推送参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“Kafka日志推送”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
策略基本信息	
Broker地址	填写目标Kafka的连接地址，建立连接关系。多个地址间以英文逗号（,）隔开。
Topic主题	填写目标Kafka上报日志的主题。
Key	填写日志的Key值，表示日志存储在Kafka的指定分区，可以当成有序消息队列使用。如果Key为空，则日志分布式存储在不同的消息分区。
失败重试分配	日志推送到Kafka失败后的重试配置。 • 重试次数：失败后的重试次数，范围为0~5次。 • 重试间隔时间：失败后的重试时间间隔，范围为1~10秒。
SASL配置信息	
安全协议	连接目标Kafka所使用的安全协议。 • PLAINTEXT：默认接入点的用户认证协议。 • SASL_PLAINTEXT：SASL用户认证协议。 • SASL_SSL：SSL用户认证协议。
消息收发机制	目标Kafka的消息收发机制，默认为PLAIN。

参数	说明
SASL用户名	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户名。
SASL用户密码	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** SASL或SSL认证所使用的用户密码。
确认SASL用户密码	**仅当“安全协议”选择“SASL_PLAINTEXT”或“SASL_SSL”时需配置。** 填写与SASL用户密码一样的值。
证书内容	**仅当“安全协议”选择“SASL_SSL”时需配置。** SSL认证所使用的CA证书内容。
元数据配置信息	
系统元数据	推送的日志中，需要携带的系统字段信息。 其中，start_time、request_id、client_ip、request_time、http_status、scheme、request_method、host、uri、upstream_addr、upstream_status、upstream_response_time、http_x_forwarded_for、http_user_agent和error_type字段信息默认在日志中携带，其他系统字段需勾选后才携带。
请求数据	推送的日志中，需要携带的API请求信息。 ● 日志包含请求头域信息：勾选后，需填写日志中要携带的请求Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含请求QueryString信息：勾选后，需填写日志中要携带的请求Query参数信息。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含请求Body体信息：勾选后，日志中会携带API请求的Body体信息。
响应数据	推送的日志中，需要携带的API响应信息。 ● 日志包含响应头域信息：勾选后，需填写日志中要携带的响应Header参数。多个字段间使用英文逗号（,）分隔，支持使用*进行通配设置。 ● 日志包含响应Body体信息：勾选后，日志中会携带响应Body体信息。
自定义认证配置	推送的日志中，需要携带的自定义认证信息。 ● 前端：填写日志中要携带的前端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。 ● 后端：填写日志中要携带的后端自定义认证的响应字段信息，多个字段间使用英文逗号（,）分隔。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

8.2.6 配置 API 的断路器

断路器是API网关在后端服务出现性能问题时保护系统的内置机制。当API的后端服务出现连续N次超时或者时延较高的情况下，会触发断路器的降级机制，向API调用方返回固定错误或者将请求转发到指定的降级后端。当后端服务恢复正常后，断路器关闭，请求恢复正常。

说明

如果此策略在当前实例中不支持，可**提交工单**升级实例到最新版本。

约束与限制

- 同一个环境中，一个API只能被一个断路器策略绑定，但一个断路器策略可以绑定多个API。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建断路器策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 断路器”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-10 断路器参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“断路器”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
策略生效范围	● 单个API生效 对单个API进行控制。 ● API共享生效 对绑定了该策略的所有API进行控制。
断路器类型	选择断路器的触发类型。 ● 超时降级：断路器以后端服务超时作为触发条件。 ● 匹配条件降级：断路器以“匹配条件”中的设置作为触发条件。
条件模式	选择断路器的触发模式。 ● 计数器：在时间窗内满足触发条件的请求次数达到设定阈值，则立即触发断路器。 ● 百分比：在时间窗内满足触发条件的请求率达到设定阈值，时间窗结束后触发断路器。
匹配条件	**仅当“断路器类型”选择“匹配条件降级”时需配置。** 配置断路器的触发条件。 ● 响应错误码：后端响应状态码符合设定值，则该后端请求满足触发条件。 ● 触发降级响应时延：后端响应时延超过设定值，则该后端请求满足触发条件。
时间窗（秒）	断路器的触发次数统计时间窗，与“阈值”或“最小百分比”参数配合使用，当时间窗内的触发次数达到设定阈值或百分比，则触发断路器。

参数	说明
阈值（次）	**仅当“条件模式”选择“计数器”时需配置。** 断路器的触发阈值，与“时间窗”参数配合使用。在时间窗内，满足触发条件的后端请求次数达到阈值，则触发断路器。 如果某个网关组件在时间窗内的触发次数超过阈值，则发送到该网关组件上的请求会触发断路器，其他未超过阈值的网关组件依然正常转发请求。 **说明** 断路器策略是按单个网关组件分开触发，如果API网关存在多个网关组件，则各个网关组件的触发统计分开计数。 您可以在API网关实例控制台的“实例信息”页面，在“出私网IP”下查看网关组件的IP个数，一个IP表示为一个网关组件。
最小调用次数	**仅当“条件模式”选择“百分比”时需配置。** 时间窗内触发断路器的API最小调用次数。如果时间窗内API的总调用次数小于该值，则不触发断路器。
最小百分比（%）	**仅当“条件模式”选择“百分比”时需配置。** 断路器的触发阈值，与“时间窗”参数配合使用。当时间窗内的满足触发条件的后端请求百分比达到阈值，则触发断路器。
开启时长（秒）	断路器开启的持续时间，断路器开启时间达到该值后将关闭。
后端降级策略	后端降级策略开关。 ● 开启：触发降级的API将把请求转发到指定后端服务。 ● 关闭：触发降级的API不会把请求转发到任何后端服务，直接返回服务不可用的错误信息，返回的HTTP状态码为“503”。

参数	说明
后端策略类型	**仅当“后端降级策略”开启时需配置。** 断路器开启后，后端请求的转发策略类型。**建议不要设置敏感信息，以防泄露。** ● Mock：把配置的响应结果作为后端服务响应固定返回。 – Mock自定义返回码：后端服务响应的状态码。 – Mock返回结果：后端服务响应的Body信息，JSON格式。 – 响应头参数：后端服务响应的Header参数。 ● HTTP&HTTPS：把后端服务请求转发给指定HTTP&HTTPS后端服务。 – 负载通道：是否使用负载通道访问后端服务。如果选择“使用”，您需要提前**创建负载通道**。 – 后端URL：配置要转发的后端服务请求地址。 – 后端超时(ms)：后端服务请求的超时时间，默认为5000ms。 ● FunctionGraph：把后端服务请求转发给指定函数。 – 函数URN：函数请求的唯一标识。单击“添加”，添加作为后端服务的函数URN。 – 函数名：选择函数URN后自动配置。 – 版本或别名：选择要使用的函数版本。 – 调用类型：选择函数的调用类型。 Synchronous：表示同步调用，后端函数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：表示异步调用，后端函数服务收到调用请求后将请求排队，执行成功后返回调用结果，服务端在空闲的情况下会逐个处理排队的请求，客户端不关注请求调用的结果。 – 后端超时(ms)：后端服务请求的超时时间，默认为5000ms。 ● Passthrough：把后端服务请求转发给API的原后端服务。 单击“添加参数”，可为转发给后端服务的请求添加请求头参数。

参数	说明
降级参数配置	降级参数配置开关。开启后可为断路器自定义规则，API请求优先匹配自定义规则中的触发条件和降级策略，仅当未匹配到自定义规则时才执行上方配置的默认触发条件和降级策略。 ● 如果匹配到自定义规则，则执行规则内配置的触发条件和降级策略。如果匹配到的自定义规则内未配置触发条件或降级策略，则执行上方配置的默认触发条件或降级策略。 ● 如果未匹配到自定义规则，则执行上方配置的默认触发条件和降级策略。
定义参数	定义用于规则匹配的参数。**建议不要设置敏感信息，以防泄露。** ● 参数位置：参数在API请求中的位置。 ● 参数：用于做规则匹配的参数名。 系统默认包含reqPath（请求路径）和method（请求方法）参数。单击“添加参数”，可添加其他匹配参数。
定义规则	自定义断路器的匹配规则。单击“添加规则”，可添加规则，系统根据从上到下的顺序匹配规则，可通过上下移动调整规则优先级。 ● 匹配条件：单击“”编辑匹配条件表达式。如果表达式数量大于等于3个，可通过“转子层级”对表达式进行分层设置。 – =为等于 – !=为不等于 – pattern为正则表达式 – enum为枚举值，多个参数值之间用英文逗号分隔 ● 触发条件和后端降级策略配置可参考上方的默认触发条件和降级策略配置。 例如，开启“降级参数配置”，按顺序添加“rule01”和“rule02”规则，“rule01”关闭“触发条件配置”并且开启“后端降级策略”，“rule02”两者都开启。断路器优先判断“rule01”匹配条件，如果匹配则会按照上方配置的默认触发条件开启断路器（rule01内未配置触发条件），并执行rule01内的后端降级策略。如果不匹配则会继续判断“rule02”，以此类推。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "breaker_condition":{
    "breaker_type":"timeout",
    "breaker_mode":"counter",
    "unhealthy_threshold":30,
    "time_window":15,
    "open_breaker_time":15,
    "unhealthy_percentage":51,
    "min_call_threshold":20
  },
  "scope":"share",
  "downgrade_default":{
    "type":"http",
    "passthrough_infos":null,
    "func_info":null,
    "mock_info":null,
    "http_info":{
      "isVpc":false,
      "vpc_channel_id":"",
      "address":"10.10.10.10",
      "scheme":"HTTP",
      "method":"GET",
      "path":"/demo",
      "timeout":5000
    },
    "http_vpc_info":null
  },
  "downgrade_parameters":[
  {
    "name":"reqPath",
    "type":"path",
    "value":"path",
    "disabled":true,
    "focused":true,
    "id":"92002eqbpilg6g"
  },
  {
    "name":"method",
    "type":"method",
    "value":"method",
    "disabled":true,
    "focused":true,
    "id":"tuvxetsdqvcos8"
  }],
  "downgrade_rules":[
  {
    "rule_name":"rule-test1",
    "parameters":[
      "reqPath",
      "method"
    ],
    "match_regex":"[\"reqPath\",\"==\",\"/test\"]",
    "downgrade_backend":{
      "type":"mock",
      "passthrough_infos":null,
      "func_info":null,
      "mock_info":{
        "status_code":200,
        "result_content":"{status: ok}",
        "headers":[]
      },
      "http_info":null,
      "http_vpc_info":null
    },
    "breaker_condition":{
      "breaker_type":"timeout",
      "breaker_mode":"percentage",
      "unhealthy_threshold":30,
```



```
    "time_window":15,
    "open_breaker_time":15,
    "unhealthy_percentage":51,
    "min_call_threshold":20
  }
 }]
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

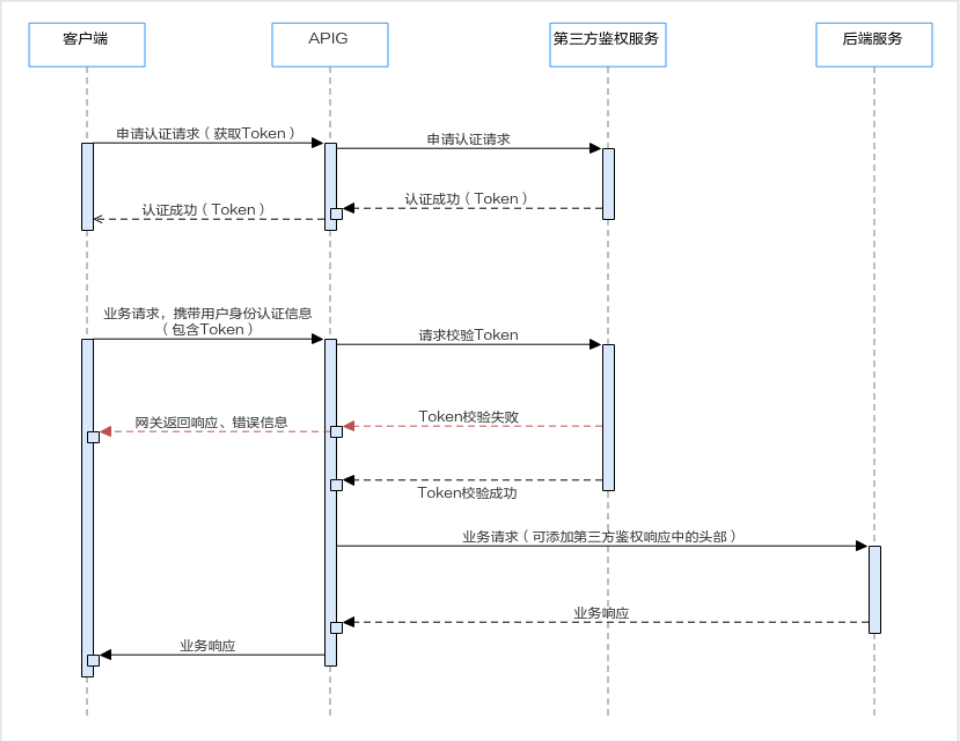
8.2.7 配置 API 的第三方认证

您可以通过第三方认证策略配置自己的鉴权服务为API的访问进行认证。API网关先调用用户的鉴权服务，收到鉴权服务的鉴权成功响应后再继续调用后端服务。

说明

如果此策略在当前实例中不支持，可**提交工单**升级实例到最新版本。

第三方认证原理图如下，第三方认证策略绑定API后，您可以参考**调用APIG开放的API**调用。



前提条件

- 同一个环境中，一个API只能被一个第三方认证策略绑定，但一个第三方认证策略可以绑定多个API。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建第三方认证策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 第三方认证”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-11 第三方认证参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“第三方认证”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
负载通道	是否使用负载通道作为第三方接口的鉴权服务。 ● 选择“使用”时，配置鉴权服务的**负载通道**。 ● 选择“不使用”时，配置鉴权服务的访问地址。
后端URL	● 请求方法 支持GET、POST、PUT、HEAD请求方法。 ● 请求协议 HTTP或HTTPS，传输重要或敏感数据时推荐使用HTTPS。 ● 负载通道（可选） **仅在“使用”负载通道时，需要设置**。选择已创建的负载通道名称，如果没有可选的负载通道，您也可以单击“新建负载通道”创建。 ● 后端服务地址（可选） **仅在不使用负载通道时，需要设置**。 填写鉴权服务的访问地址，格式：“主机:端口”。主机为鉴权服务的访问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。 **目前仅支持IPv4地址。** ● 路径 鉴权服务的路径，即服务的url。
后端超时（ms）	鉴权服务请求的超时时间。超时时间不超过后端响应超时时间上限，超时时间上限可在API网关控制台的“配置参数”中查看。
自定义host头域	**仅在使用负载通道时配置**。 自定义后端服务请求中的Host头域，默认使用请求中原始的host头域。
防暴力拦截阈值	当源IP访问在5分钟内进行第三方认证失败的次数达到此处配置的阈值时，将触发源IP请求拦截，在这5分钟后解除请求拦截。 例如，5分钟内，源IP访问在第三分钟进行第三方认证失败的次数达到此处配置的阈值，触发源IP请求拦截，再过2分钟解除请求拦截。

参数	说明
身份来源	将从API原始请求中获取此处配置的参数进行第三方鉴权接口鉴权（最大支持10个header参数和10个query参数）。身份来源信息为空时，携带API原始请求的请求参数（header参数和query参数）调用第三方鉴权接口进行鉴权。
宽松模式	开关开启后，当鉴权服务不可用（与鉴权服务建立连接失败或者鉴权服务返回5*xx*）时，API网关仍然接受客户端请求。
允许携带原始请求体	开关开启后，将携带API原始请求体调用鉴权接口鉴权。
请求体大小（字节）	**仅在开启“允许携带原始请求体”时配置**。 请求体大小不能超过实例允许的最大请求体大小。实例的最大请求体大小可在API网关控制台“配置参数”中查看。
允许携带原始请求路径	开关开启后，将API原始请求路径拼接到鉴权接口路径之后调用鉴权接口鉴权。
直接返回鉴权响应	开关开启后，鉴权失败时，将直接返回鉴权服务的响应。
允许携带的响应头部	鉴权成功时，原始请求将从鉴权服务返回的响应头中获取此处配置的头部，传到业务后端。 最大支持配置10个头部。
简易鉴权模式	开关开启后，鉴权服务返回状态码“2*xx*”时，表示认证通过。
鉴权结果匹配	**仅在“简易鉴权模式”关闭后可配置**。 根据鉴权服务返回的响应头中的参数名和参数值进行校验，响应头中存在此处配置的参数名，并且参数值相等则认证通过。
黑白名单配置	开关开启后，原始API请求匹配黑/白名单规则将进行/不进行第三方认证鉴权。
规则类型	• 白名单规则 如果原始API请求匹配白名单规则，将不进行第三方认证鉴权。 • 黑名单规则 如果原始API请求匹配黑名单规则，将进行第三方认证鉴权。

参数	说明
定义参数	定义用于规则的参数。**建议不要设置敏感信息，以防泄露。** ● 参数位置：用于规则匹配的参数位置。 – path：API请求的URI，系统默认配置。 – method：API请求方法，系统默认配置。 – header：请求头的key值。 – query：QueryString的key值。 – system：系统参数。 ● 参数：用于判断与规则中的参数值是否匹配。
定义规则	定义用于规则的判断条件。 单击“添加规则”，编辑规则名称和规则条件。在“条件表达式”弹窗中，选择“定义参数”中的参数名和判断条件，以及输入参数值。**建议不要设置敏感信息，以防泄露。** ● =为等于 ● !=为不等于 ● pattern为正则表达式 ● enum为枚举值，多个参数值之间用英文逗号分隔

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "auth_request": {
    "method": "GET",
    "protocol": "HTTPS",
    "url_domain": "192.168.10.10",
    "timeout": 5000,
    "path": "/",
    "vpc_channel_enabled": false,
    "vpc_channel_info": null
  },
  "custom_forbid_limit": 100,
  "carry_body": {
    "enabled": true,
    "max_body_size": 1000
  },
  "auth_downgrade_enabled": true,
  "carry_path_enabled": true,
  "return_resp_body_enabled": false,
  "carry_resp_headers": [],
  "simple_auth_mode_enabled": true,
  "match_auth": null,
  "rule_enabled": false,
```



```
  "rule_type": "allow"
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

8.2.8 配置 API 的流量镜像

API网关提供了镜像客户端请求的能力，将发送到源后端的流量复制一份到镜像服务中，在不影响业务后端的情况下，便于对请求内容进行具体的分析和统计。

约束与限制

- 同一个环境中，一个API只能被一个流量镜像策略绑定，但一个流量镜像策略可以绑定多个API。
- 镜像请求返回的响应会被忽略。
- 镜像请求的请求体大小受**实例参数“request_body_size”**控制，默认请求体大小为12MB，可通过“request_body_size”参数调整请求体大小，**请求体大小调整越大性能损耗越大**，请谨慎操作。
- API的后端服务类型为Mock时，不支持绑定流量镜像策略。
- 策略和API本身相互独立，只有为API绑定策略后，策略才对API生效。为API绑定策略时需指定发布环境，策略只对指定环境上的API生效。
- 策略的绑定、解绑、更新会实时生效，不需要重新发布API。
- API的下线操作不影响策略的绑定关系，再次发布后仍然会带有下线前绑定的策略。
- 如果策略与API有绑定关系，则策略无法执行删除操作。

创建流量镜像策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API策略”。

步骤4 在“策略管理”页面，单击“创建策略”。

步骤5 在“选择策略类型”弹窗中，选择“插件策略 > 流量镜像”。

步骤6 在“创建策略”弹窗中，根据下表参数说明，配置策略信息。

表 8-12 流量镜像参数说明

参数	说明
策略名称	填写策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。
策略类型	固定为“流量镜像”。
描述	填写策略的描述信息。长度为1~255个字符。
策略内容	策略的配置内容，支持表单配置和脚本配置两种方式。
镜像协议	镜像请求协议。指定的镜像服务协议须与用户的镜像业务协议保持一致。
镜像地址	镜像服务的地址。由IP/域名和端口号组成，总长度不超过255。格式为主机:端口（如：xxx.xxx.xxx:7443）。如果不写端口号，那么HTTPS默认端口号为443，HTTP默认端口号为80。
镜像请求路径	当“镜像协议”为HTTP/HTTPS时设置。 镜像请求的路径，支持* % - _ .等特殊字符，总长度不超过512，且满足URI规范。如果不指定镜像请求路径，那么默认使用绑定的API的请求路径。
拼接模式	当指定镜像请求的路径后，可以设置请求路径的拼接模式。 • replace模式：表示使用指定的“镜像请求路径”作为镜像请求的路径。 • prefix模式：表示使用指定的“镜像请求路径”+API的请求路径作为镜像请求的路径。
采样率	镜像请求的采样率，取值范围：0.00001~1。当设置为1时为全采样，默认为1。 例如，API请求流量为1000，采样率为0.1，那么采样的线上请求流量为100。
超时时间(ms)	镜像请求的超时时间，单位ms。默认超时时间为5000ms。
客户端请求体	镜像客户端的请求体，默认开启镜像客户端请求体。

步骤7 单击“确定”。

如果您需要复制已创建的策略，请在已创建策略的“操作”列中单击“克隆”配置参数即可。**克隆策略的名称不能与已创建的策略名称重复。**

步骤8 策略创建后，您还需要**为策略绑定API**，才能使策略对API生效。

----结束

脚本配置示例

```
{
  "protocol": "HTTPS",
  "host": "X.X.X.X",
  "sample_ratio": 1,
  "timeout": 5000,
  "mirror_request_body_enabled": true,
  "path": "/ab",
  "path_concat_mode": "replace"
}
```

为策略绑定 API

步骤1 单击策略名称，进入策略详情。

步骤2 在API列表区域选择环境后，单击“绑定API”。

步骤3 筛选API分组以及发布环境，勾选所需的API。

支持通过API名称或标签筛选API，标签为创建API时定义的标签。

步骤4 单击“确定”，绑定完成。

- 如果单个API不需要绑定此策略，单击API所在行的“解绑”。
- 如果批量API不需要绑定此策略，则勾选待解绑的API，单击列表上方“解绑”。最多同时解绑1000个API。

----结束

9 配置凭据策略

9.1 配置 API 认证凭据的配额控制

凭据配额可限制单位时间内凭据调用API的总次数，保护后端服务。您可以创建凭据配额策略，对绑定策略的凭据进行调用次数限制。

凭据配额策略和凭据本身是相互独立的，只有将凭据绑定凭据配额策略后，凭据配额策略才对凭据生效。

操作步骤

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击凭据名称，进入凭据详情页面。

步骤5 在“凭据配额策略”区域，单击“绑定”。

步骤6 在弹窗中选择已有策略或单击“创建新策略”。

- 选择已有策略：单击“选择已有策略”后，选择策略。
- 创建新策略：请参考**表9-1**所示配置策略。

表 9-1 配置凭据配额策略

参数	说明
策略名称	填写客户端配额策略的名称，根据业务规划自定义。建议您按照一定的命名规则填写配额策略名称，方便您快速识别和查找。 支持中文、英文、数字、下划线，且只能以英文或中文开头，长度为3~255个字符。

参数	说明
首次生效时间点	设置配额策略的生效起始时间点。例如，时长为1小时，首次生效时间点为2020/08/08 05:05:00，则表示客户端配额策略从2020/08/08 05:05:00开始生效，每个小时的05分开始到下一个小时的05分之间为一个单位时间，即05:05:00-06:05:00为一个单位时间，以此类推。
时长	填写配额限制的时长，单位可选择“秒”、“分”、“时”和“天”。需与“API访问限制”配合使用，表示单位时间内客户端可调用API的总次数上限。
API访问限制	填写客户端可调用API的次数上限，与“时长”配合使用。
描述	填写客户端配额策略的描述信息。长度为1~255个字符。

步骤7 策略配置完成后，单击“确定”。

----结束

9.2 配置 API 认证的凭据访问控制

凭据访问控制可控制访问API的凭据IP地址，保护后端服务。您可以为凭据设置访问控制策略，允许/禁止某个IP地址的凭据访问API。

配置凭据的访问控制策略

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > 凭据管理”。

步骤4 单击凭据名称，进入凭据详情页面。

步骤5 在“访问控制策略”区域，单击“绑定”。

步骤6 根据下表参数说明，在弹窗中配置策略信息。

表 9-2 绑定访问控制策略

参数	说明
动作	选择访问控制的动作。 ● 允许：表示仅允许指定IP地址的客户端调用API。 ● 禁止：表示禁止指定IP地址的客户端调用API。
IP地址	单击“增加IP地址”，添加允许或禁止调用API的客户端IP地址或IP地址段。

步骤7 策略配置完成后，单击“确定”。

----结束

10 管理 APIG 实例

10.1 查看或编辑 APIG 实例信息

实例创建完成后，可在控制台查看和编辑实例的配置信息。

查看或编辑实例信息

步骤1 进入API网关控制台页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待查看或编辑的实例上，单击“查看控制台”或实例名称。

步骤4 在“实例信息”页签，根据下表参数说明，查看或编辑实例的配置信息。

表 10-1 实例信息

可编辑项	说明
基本信息	实例的基本信息，包括实例名称、实例ID、实例规格、可用区、描述、企业项目和时间窗。 • 用户可以根据实际需要修改基本信息。 • 用户可以单击“实例ID”右侧的 复制实例ID信息。
计费信息	实例的计费模式和创建实例的时间。

可编辑项	说明
网络配置	• 虚拟私有云 实例所关联的VPC，用户可以单击VPC名称跳转查看VPC的具体配置信息。 • 子网 实例所关联的子网，用户可以单击子网名称跳转查看子网的具体配置信息。 • 安全组 实例所关联的安全组，用户可以单击安全组名称跳转查看安全组的具体配置信息，也可以单击，绑定新的安全组。 • 访问控制 API网关提供实例级的访问控制策略，您可以通过设置IP地址的黑白名单来禁止/允许某个IP地址访问实例。IP地址说明如下： – 常规IP格式，如：127.0.0.1 – IP加掩码，如：192.145.0.0/16 – IP段范围，如：127.0.0.1-192.145.0.1 访问控制策略最多支持设置100个IP地址或网段，且最大长度为5120。 如果使用IPv6地址，请先确保对应实例支持IPv6协议。 如果不开启访问控制策略，默认允许所有IP访问；如果开启访问控制策略，设置“白名单”类型，但是没有配置任何IP地址，则禁止任何IP访问；如果开启访问控制策略，设置“黑名单”类型，但是没有配置任何IP地址，则允许任何IP访问。 **安全组策略**、实例级访问控制策略和**API级访问控制策略**遵循Deny优先原则。
入口地址	• 虚拟私有云访问地址 • 弹性IP地址 – 如果实例未绑定弹性IP地址，您可以单击地址右侧的“立即启用”，绑定弹性IP地址。 – 如果实例已绑定弹性IP地址，您可以单击地址右侧的复制地址信息。 – 如果实例已绑定弹性IP地址，您可以编辑公网带宽。公网带宽费用按小时计算，以弹性公网IP服务的价格为准。 – 如果实例已绑定弹性IP地址，您可以单击地址右侧的“解绑EIP”，解绑弹性IP地址。
出口地址	指允许实例API的后端服务部署在外部网络，API网关为实例开启公网出口。公网出口可随时关闭或开启。 开启公网出口后，您可以单击“查看带宽监控”查看数据，也可编辑出公网带宽。

可编辑项	说明
路由	配置私有网段。实例创建完成后，默认能够与创建时指定的VPC子网网段进行互通。如果有额外的私有网段需要与实例互通，可通过该配置项进行路由配置。 如果本地数据中心的子网不在以下三个大子网段内，暂时不支持配置本地路由。 ● 10.0.0.0/8-24 ● 172.16.0.0/12-24 ● 192.168.0.0/16-24

----结束

10.2 配置 APIG 实例参数

配置参数提供了实例内组件的公共参数配置，通过修改配置参数，可以调整组件的相关功能。

约束与限制

修改实例配置参数会引起APIG业务中断，建议在无业务运行或业务低峰时修改配置参数。

配置实例参数

步骤1 进入**API网关控制台**页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待配置参数的实例上，单击“查看控制台”或实例名称。

步骤4 单击“配置参数”页签，找到您需要调整的配置项，根据下表参数说明，进行修改。不同的实例规格展示的配置参数会存在不同，具体以界面为准。

表 10-2 实例配置参数说明

参数	说明
ratelimit_api_limits	API全局默认流控值，默认值为200次/秒。API未绑定流控策略时，执行此默认流控；API绑定流控策略时，则执行绑定的流控策略。流控策略的API流量限制值不能超过API全局默认流控值。
request_body_size	API请求中允许携带的Body大小上限，默认值为12MB，可修改范围为1MB~9536MB。 支持通过POST方法上传文件，目前仅支持对请求体透传。
backend_timeout	后端响应超时时间上限，默认值为60000ms，可修改范围为1ms~600000ms。

参数	说明
app_token	app_token认证方式开关，默认关闭。启用后，可在API请求中使用获取的access_token进行API的调用认证。 ● app_token_expire_time：access_token的有效时间，在access_token到期前，请及时获取新的access_token并更新，避免影响正常使用。 ● refresh_token_expire_time：refresh_token的有效时间。refresh_token用于获取新的access_token。 ● app_token_uri：获取access_token的uri。 ● app_token_key：access_token的加密key。
app_api_key	app_api_key认证方式开关，默认关闭。启用后，可在API请求中添加“apikey”参数，携带凭据的Key进行API的调用认证。
app_basic	app_basic认证方式开关，默认关闭。启用后，在API请求中添加Header参数“Authorization”，参数值为"Basic"+base64(*appkey*:*appsecret*)，其中appkey和appsecret分别为凭据的Key和Secret。
app_secret	app_secret认证方式开关，默认关闭。启用后，可在API请求中添加“X-HW-ID”和“X-HW-AppKey”参数，携带凭据的Key和Secret进行API的调用认证。
app_route	支持IP访问开关，默认关闭。启用后，非DEFAULT分组下的APP认证的API可以使用IP地址调用。
backend_client_certificate	后端双向认证开关，默认关闭。启用后，创建API配置后端服务时，可配置后端双向认证。
ssl_ciphers	支持配置https加密套件，默认所有的加密套件全部支持。当您绑定独立域名后，可根据需要选择支持的加密套件。
real_ip_from_xff	是否使用X-Forwarded-For头中的IP作为ACL、流控的判断依据，默认不使用。 xff_index：X-Forwarded-For头中IP的排序序号，值允许为正数、负数、0。 ● xff_index值为0或正数时，获取X-Forwarded-For头中对应索引的IP。 ● xff_index值为负数时，按倒序方式从X-Forwarded-For头中获取IP。 例如到达API网关的X-Forwarded-For头中依次有IP1，IP2，IP3三个IP地址，xff_index取0时获取IP1，xff_index取1时获取IP2，xff_index取-1时获取IP3，xff_index取-2时获取IP2。
vpc_name_modifiable	负载通道名称是否可修改，默认可修改。 **须知** 负载通道名称可修改时，当前实例的负载通道无法通过项目级负载通道管理接口操作。

参数	说明
app_jwt_enable	app_jwt认证方式开关，默认关闭。启用后，可在API请求中添加如下参数，携带凭据的Key和Secret以及时间戳进行API的调用认证。 ● 在API请求中添加Header参数“Timestamp”，参数值为当前时间的Unix时间戳，单位为毫秒。 ● 在API请求中添加Header参数“Authorization”，这一参数可以通过修改“app_jwt_auth_header”项进行配置，默认值为“Authorization”，参数值为sha256(appkey+appsecret+timestamp)，且sha256加密后的字符串需为小写字母。其中appkey和appsecret分别为凭据的Key和Secret，timestamp为当前时间的Unix时间戳，单位为毫秒。 ● 在API请求中添加Header参数“X-HW-ID”，参数值为凭据的Key。
public_key_enable	public_key类型签名密钥开关，默认关闭。启用后，可在签名密钥认证中使用public_key类型签名。 public_key_uri_prefix：获取public_key对应secret的uri前缀。具体uri格式为：https://{虚拟私有云访问地址}{public_key_uri_prefix}{public_key签名密钥名称}。
custom_auth_header	认证头域自定义配置开关，默认关闭。启用后，参数“app_auth_header”和“backend_sign_header”的初始值为空，与不启用效果一致。 如果配置“app_auth_header”的“参数运行值”，那么对于APP认证的API，请求header中携带APP认证信息的参数为此处“app_auth_header”的值；如果配置“backend_sign_header”的“参数运行值”，那么对于绑定HMAC或者Basic Auth类型签名密钥策略的API，API网关到后端服务的请求header中携带签名信息的参数为此处“backend_sign_header”的值。 **须知** 配置后会影响当前实例下所有APP认证或签名密钥策略（HMAC/Basic Auth类型），请谨慎配置。
gzip	对响应请求使用gzip压缩，用于减少公网流量。默认未配置gzip压缩，配置后1分钟生效，请谨慎修改。 启用后，可配置comp_level参数，comp_level表示压缩级别，值越大表示性能消耗越大，一般默认为6。 **须知** ● 响应请求体大于1KB时，您可以使用gzip压缩文件（即1KB以下的文件不做压缩）。 ● gzip压缩支持的文件类型有text/xml、text/plain、text/css、application/javascript、application/x-javascript、application/rss+xml、text/javascript、image/tiff、image/svg+xml、application/json、application/xml ● 启用gzip压缩后，须在请求中添加请求头“Accept-Encoding: gzip”。 ● gzip配置完成后，如需修改，至少需要1分钟后。

参数	说明
custom_log	自定义日志功能开关，默认关闭。开启自定义日志功能后，实例下所有API的**调用日志**中会在指定位置打印指定参数的值。 启用后，需单击“编辑”，添加需在调用日志中打印的参数。 **须知** • 自定义日志只支持打印由客户端发起的请求信息，不支持打印在APIG中定义的常量参数和系统参数。 • 自定义日志最多可配置10个字段，且字段大小总和不得超过2KB。 • 参数值中的部分特殊字符会进行编码，例如：加号（+）会被编码为空格“ ”，双引号（"）会被编码为“\x22”，反斜杠（\）会被编码为“\x5C”。
sse_strategy	SSE传输策略开关，默认关闭。启用后，支持通过使用Server-Sent Events（SSE）按照流式输出API的响应内容，可以实现逐字符渲染。 **须知** sse_strategy配置完成后，如需修改，至少需要1分钟后。
vpc_name_modifiable	负载通道名称支持修改开关。开启后可修改负载通道名称，但当前实例的负载通道无法通过项目级VPC通道管理API接口操作。
vpc_health_status	负载通道后端实例健康状态显示开关，默认关闭。开关开启且负载通道的健康检查开启时，将在负载通道详情页面展示后端实例的健康状态。
request_custom_config	支持自定义配置客户端请求相关参数。 • HTTP/2：HTTP/2协议的开关，默认为开启状态。更多详情请参考**什么是API网关**。 • request_body_timeout：客户端请求体超时时间的修改，默认为8s。网络状况差或请求体过大的情况下可适当调整该参数。 **须知** 客户端请求自定义配置修改完成后，如需修改，至少需要1分钟后。
api_uri_no_escape	API的URL中的Path转义处理开关。默认关闭，表示URL中的Path会进行转义处理。 开启“api_uri_no_escape”开关后，使用Path不转义的功能请参见**表10-3**。

表 10-3 Path 不转义影响的功能

功能	描述	API前端定义的Path	请求发送时使用的Path	api_uri_no_escape开关关闭	api_uri_no_escape开关开启
API定义	APIG进行匹配路由的Path	/{path}	/aa%2Faa	/aa/aa	/aa%2Faa
参数编排	后端服务参数使用的Path	-	-	/aa/aa	/aa%2Faa
http到https重定向	重定向使用的Path	-	-	/aa/aa	/aa%2Faa
策略后端	策略条件为请求入参的Path	-	-	/aa/aa	/aa%2Faa
第三方认证策略	API绑定第三方认证策略后，传递到第三方的Path	-	-	/aa/aa	/aa%2Faa
kafka日志推送策略	API绑定kafka日志推送策略后，使用的请求Path	-	-	/aa/aa	/aa%2Faa
负载通道	使用URI哈希分发算法的负载通道时，APIG用来转发的Path	-	-	/aa/aa	/aa%2Faa
FunctionGraph后端	API的后端类型为FunctionGraph时，发送到函数请求Path	-	-	/aa/aa	/aa%2Faa
自定义认证	API认证方式选择自定义认证时，发送到函数请求Path	-	-	/aa/aa	/aa%2Faa

----结束

10.3 配置 APIG 实例标签

通过标签功能对实例资源进行标记，批量分类实例资源，实现对实例资源进行分组查询、分析及管理。

用户可在**标签管理服务（Tag Management Service，简称TMS）**中过滤查询资源、分析资源及管理资源。

配置实例标签

步骤1 进入API网关控制台页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待添加标签的实例上，单击“查看控制台”或实例名称。

步骤4 在“标签”页签中，单击“添加标签”。

标签由键和值组成，值可以为空。

- 标签键：支持可用UTF-8格式表示的字母(包含中文)、数字和空格，以及： _ . : = + - @字符； _sys_开头属于系统标签，租户不能输入。
- 标签值：支持可用UTF-8格式表示的字母(包含中文)、数字和空格，以及： _ . : = + - @字符。

说明

如您的组织已经设定API网关服务的相关标签策略，则需按照标签策略规则为实例添加标签。标签如果不符合标签策略的规则，则可能会导致添加标签失败，请联系组织管理员了解标签策略详情。

步骤5 单击“确定”。

----结束

相关操作

进入标签管理服务控制台，通过已添加标签过滤实例，查看、分析及管理实例资源。

步骤1 将鼠标移至左侧 图标展开服务列表，输入“标签管理服务”搜索。

步骤2 进入标签管理服务控制台，填写搜索信息搜索，过滤实例资源。

1. 区域：选择API网关所在区域。
2. 资源类型：选择“APIG”。
3. 资源标签：选择已添加的标签键。

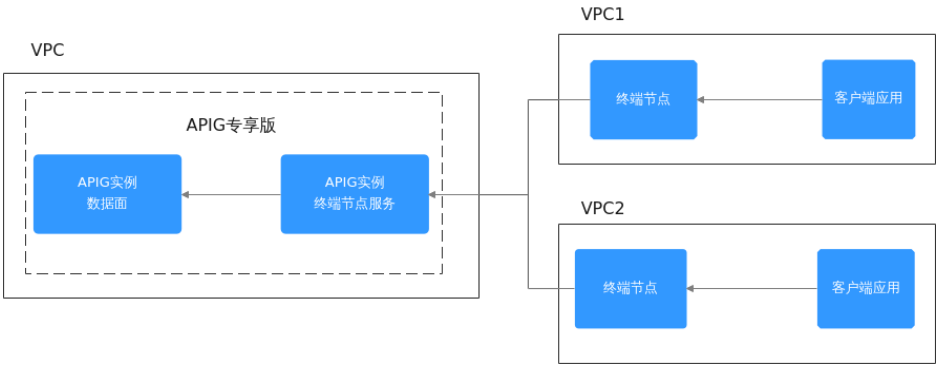
----结束

10.4 配置 APIG 的终端节点信息

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。

在同一区域中，可实现云内跨VPC访问/开放API。

图 10-1 同一区域跨 VPC 访问



约束与限制

目前除墨西哥城一、北京一区域外，其他区域都支持终端节点管理功能。

配置终端节点信息

步骤1 进入**API网关控制台**页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在已创建的实例上，单击“查看控制台”或实例名称。

步骤4 单击“终端节点管理”页签，根据下表参数说明，查看终端节点信息，详细信息可参考**终端节点管理**。

表 10-4 终端节点信息

参数	说明
服务信息	展示的名称由{region}.{终端节点服务名称}.{终端节点服务ID}组成。您在**购买实例**时，会同步创建VPC终端节点服务，可以设置终端节点服务名称，也可以在此处修改终端节点服务名称。

参数	说明
连接管理	展示连接到网关实例的终端节点信息。如果需要新建终端节点，请单击“创建终端节点”创建。 ● 终端节点ID：终端节点的ID。 ● 报文标识：终端节点ID的标识，用来识别是哪个终端节点。 ● 状态：终端节点的状态。 关于终端节点的各个状态，请查看**终端节点服务和终端节点有哪些状态?** 。 ● 拥有者：终端节点创建者的**账号ID**。 ● 创建时间：终端节点的创建时间。 ● 操作：终端节点服务对终端节点的连接审批，可选择“接受”或“拒绝”。 **须知** 如您仍有业务通过该连接进行访问，拒绝已建立的连接可能导致业务受损，请谨慎操作。
权限管理	权限管理用于控制是否允许跨租户的终端节点进行访问。可以设置允许连接该终端节点服务的授权账号ID，将授权账号ID添加至终端节点服务的白名单中。 单击“添加白名单记录”，填写**账号ID**。 ● 授权账号ID：连接访问终端节点的授权账号ID。 ● 创建时间：白名单的创建时间。 ● 操作：对连接访问终端节点的授权账号进行操作，支持将授权账号从白名单中删除。

----结束

10.5 自定义 APIG 的客户端访问端口

API网关提供自定义实例入端口功能，支持客户端通过不同的端口来访问不同的后端服务。

约束与限制

- 新增端口时，一个端口仅允许配置一种协议。当前仅支持HTTP和HTTPS协议。
- 独立域名与端口相关约束与限制内容，请参考**约束与限制**。

自定义客户端访问端口

步骤1 进入**API网关控制台**页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 在待自定义入方向端口的实例上，单击“查看控制台”或实例名称。

步骤4 在“自定义入方向端口”页签中，单击“新增入方向端口”。

根据实际业务，选择请求协议，并填写入方向端口。

步骤5 单击“确定”。

----结束

后续操作

在“分组信息”页面的“**域名管理**”区域，将已绑定独立域名的端口修改为新增的入端口或在绑定独立域名时选择新增的入端口，用户才可以通过不同的端口访问不同的后端服务。

10.6 变更 APIG 的实例规格

当实例规格无法满足您的业务需求时，您可以进行规格变更操作升配到更高规格版本。

约束与限制

- 规格变更过程中，长连接会发生闪断，需要重新建链，建议业务低峰期进行规格变更。
- 只能升配到更高规格，无法降配规格。
- 规格变更时，出私网IP会发生变化，如有相关防火墙配置或者白名单配置需要完全放通，防止网络问题导致业务受损！变更期间请勿对实例进行任何操作！变更完成后，请根据业务需要重新调整相关防火墙配置或者白名单配置。
- 如果当前实例不支持规格变更，请联系技术支持升级实例到最新版本。

变更实例规格

步骤1 进入**API网关控制台**页面。

步骤2 在左侧导航栏选择“实例管理”。

步骤3 单击待变更实例右侧的“更多 > 规格变更”。

步骤4 实例参数信息请参考**表10-2**，选择升级规格，单击“下一步”。

步骤5 确认信息无误后，勾选服务协议，单击“去支付”后开始变更，变更时长15~30分钟左右。

说明

- “按需计费”模式的实例变更规格时不需要补齐差额。

----结束

11 查看监控指标与配置告警

11.1 APIG 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

SYS.APIC

监控指标

表 11-1 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）
requests	接口调用次数	统计测量api接口被调用的次数。	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
error_4xx	4xx异常次数	统计测量api接口返回4xx错误的次数。	≥0	测量对象：专享版API网关实例 测量维度：instance_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）
error_5xx	5xx异常次数	统计测量api接口返回5xx错误的次数	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
throttled_calls	被流控的调用次数	统计测量api被流控的调用次数	≥0	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
avg_latency	平均延迟毫秒数	统计测量api接口平均响应延时时间	≥0 单位：毫秒	测量对象：专享版API网关实例 测量维度：instance_id	1分钟
max_latency	最大延迟毫秒数	统计测量api接口最大响应延时时间	≥0 单位：毫秒	测量对象：专享版API网关实例 测量维度：instance_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
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

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
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
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
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
node_system_load	网关节点系统负载	该指标用于统计当前数据面网关节点负载详情，1表示低水位，2表示中水位，3表示高水位	1，2，3， 单位：count	测量对象：单个网关节点 测量维度：node_ip	1分钟
node_cpu_usage	网关节点cpu使用率	该指标用于统计当前数据面网关节点cpu使用率	≥0，单位：%	测量对象：单个网关节点 测量维度：node_ip	1分钟
node_memory_usage	网关节点内存使用率	该指标用于统计当前数据面网关节点内存使用率	≥0，单位：%	测量对象：单个网关节点 测量维度：node_ip	1分钟

维度

表 11-2 API 网关监控指标测量维度

Key	Value
instance_id	专享版API网关
instance_id,node_ip	专享版API网关节点
instance_id,api_id	API

11.2 配置 APIG 的监控告警

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。

操作步骤

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面的“监控视图”区域，单击“查看更多监控”，返回“云服务监控”界面，参考**创建告警规则**为API网关创建告警规则。

----结束

11.3 查看 APIG 的监控指标

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。

查看单个 API 的监控指标

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“API管理 > API分组”。

步骤4 单击分组名称，进入“分组信息”页面。

步骤5 在“API运行”页面左侧选择API。

步骤6 在“监控视图”区域，查看API的各项监控指标。

查看某个API的调用统计，包括“请求次数”、“调用延时”、“数据流量”和“出错统计”，同时可以选择要查看数据的时间段范围。

- 近1小时数据每2分钟刷新一次。
- 近6小时数据每2小时刷新一次。
- 近一天数据每2小时刷新一次。
- 近一周和近一月数据每天刷新一次。

步骤7 如果需要查看实例、实例节点的监控信息，请单击“查看更多监控”，查看更多的监控数据。

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

查看 API 分组的监控指标

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“监控分析 > API监控”。

步骤4 选择待查看的API分组，查看分组下API的调用统计，包括“请求次数”、“调用延时”、“数据流量”和“出错统计”。

----结束

11.4 查看 APIG 的带宽监控

API网关支持查看出入口带宽各项指标的监控数据，了解带宽的网络情况和使用率。

前提条件

已启用入口地址或出口地址。入口地址或出口地址可在**实例信息**中查看。

查看带宽监控

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“监控分析 > 带宽监控”。

步骤4 根据下表参数说明，配置监控信息。

表 11-3 监控信息

参数	配置项
带宽IP	带宽IP为实例的入口或出口IP，可在**实例信息**中查看。

参数	配置项
时间段	支持查看“近1小时”、“近3小时”、“近12小时”、“近24小时”或“近7天”的数据监控时间段，也可以单击  自定义时间段。同时，监控指标视图右上角会动态显示对应时段内监控指标的最大值与最小值。
自动刷新	打开“自动刷新”开关，可每分钟自动刷新一次数据。
周期	数据聚合周期，即原始采样指标数据以最大、最小、平均、求合或方差形式进行聚合的计算周期。

----结束

11.5 查看 APIG 的 API 调用日志

APIG提供了API的可视化分析和统计能力，支持查看API的调用日志。

前提条件

已调用API。

查看 API 的调用日志

步骤1 进入**API网关控制台**页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 在左侧导航栏选择“监控分析 > 日志分析”。

步骤4 单击“配置访问日志”，将“启动日志记录”修改为  ，即启用日志记录能力。

步骤5 “日志组”和“日志流”设置请参见**日志管理**，完成后单击“确定”。

步骤6 查看日志分析可单击页面右上角“日志字段说明”，根据日志字段说明分析日志。

步骤7 如需导出日志，具体步骤请参见**日志转储**。

访问日志的字段采用空格作为分隔符，按照顺序，每个字段的含义如下表：

表 11-4 日志字段说明

序号	字段	说明
1	remote_addr	客户端地址。
2	request_id	请求ID。
3	api_id	API ID。
4	user_id	当使用IAM认证访问时，请求方提供的项目ID。

序号	字段	说明
5	app_id	当使用APP认证访问时，请求方提供的APP ID。
6	time_local	请求完成时间。
7	request_time	请求延迟（单位：秒）。
8	request_method	HTTP请求方法。
9	scheme	请求协议。
10	host	请求域名。
11	router_uri	请求URI。
12	server_protocol	请求协议。
13	status	响应状态码。
14	bytes_sent	响应大小（单位：字节，包含状态行、响应头、响应体）。
15	request_length	请求长度（单位：字节，包含起始行、请求头、请求体）。
16	http_user_agent	用户代理标识。
17	http_x_forwarded_for	X-Forwarded-For头。
18	upstream_addr	请求的后端地址。
19	upstream_uri	请求后端的URI。
20	upstream_status	后端响应状态码。
21	upstream_connect_time	与后端建立连接所用时间（单位：秒）。
22	upstream_header_time	从开始与后端建立连接到从后端获取到首字节所用时间（单位：秒）。
23	upstream_response_time	从开始与后端建立连接到从后端获取到最后一个字节所用时间（单位：秒）。
24	region_id	云服务区ID。
25	all_upstream_response_time	从开始与后端建立连接到从后端获取到最后一个字节所用时间（单位：秒）。发生重试时，为所用时间总和。
26	errorType	API请求的错误类型。 ● 0：非流控错误 ● 1：流控错误
27	auth_type	API认证类型。
28	access_model1	认证模式1。

序号	字段	说明
29	access_model2	认证模式2，开启双重认证时，为自定义认证编号。
30	inner_time	apig的内部处理时长，单位秒。
31	proxy_protocol_vni	VPC终端节点的虚拟网络标识。
32	proxy_protocol_vpce_id	VPC终端节点的ID。
33	proxy_protocol_addr	客户端源IP地址。
34	body_bytes_sent	API请求的Body体大小，单位字节。
35	api_name	API名称。
36	app_name	当使用APP认证访问时，请求方使用的APP名称。
37	provider_app_id	API所属的APP ID。
38	provider_app_name	API所属的APP名称。
39	custom_data_log1	用户自定义日志字段值1。
40	custom_data_log2	用户自定义日志字段值2。
41	custom_data_log3	用户自定义日志字段值3。
42	custom_data_log4	用户自定义日志字段值4。
43	custom_data_log5	用户自定义日志字段值5。
44	custom_data_log6	用户自定义日志字段值6。
45	custom_data_log7	用户自定义日志字段值7。
46	custom_data_log8	用户自定义日志字段值8。
47	custom_data_log9	用户自定义日志字段值9。
48	custom_data_log10	用户自定义日志字段值10。
49	response_source	请求响应来源。 ● local：APIG ● remote：后端服务
50	gzip_ratio	原始响应body体大小与压缩后大小的比率。
51	upstream_scheme	后端协议类型。
52	group_id	分组ID。
53	apig_err_code	网关错误码。

序号	字段	说明
54	function_urn	函数URN。

----结束

12 查看 APIG 审计日志

12.1 云审计服务支持的 APIG 操作列表

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、审计、问题定位等常见应用场景时，则需要先**开通云审计服务**。

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

查看关键操作列表

通过云审计服务，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。API Gateway操作列表见下表：

表 12-1 云审计服务支持的 API Gateway 操作列表

操作名称	资源类型	事件名称
创建API分组	ApiGroup	createApiGroup
修改API分组	ApiGroup	updateApiGroup
删除API分组	ApiGroup	deleteApiGroup
校验API分组名称是否存在	Swagger	CheckApiGroups
创建环境	Environment	createEnvironment
修改环境	Environment	updateEnvironment

操作名称	资源类型	事件名称
删除环境	Environment	deleteEnvironment
新建变量	EnvVariable	CreateEnvironmentVariable
删除变量	EnvVariable	DeleteEnvironmentVariable
修改变量	EnvVariable	UpdateEnvironmentVariable
创建流控策略	Throttle	CreateRequestThrottlingPolicy
修改流控策略	Throttle	UpdateRequestThrottlingPolicy
删除流控策略	Throttle	DeleteRequestThrottlingPolicy
创建API	Api	CreateApi
修改API	Api	UpdateApi
删除API	Api	DeleteApi
发布或下线API	Api	CreateOrDeletePublishRecordForApi
校验API定义	Api	CheckApis
调试API	Api	DebugApi
批量发布/下线API	Api	BatchPublishOrOfflineApi
切换API版本	Api	ChangeApiVersion
根据版本号下线API	Api	DeleteApiByVersionId
创建签名密钥	Signature	CreateSignatureKey
修改签名密钥	Signature	UpdateSignatureKey
删除签名密钥	Signature	DeleteSignatureKey
绑定签名密钥	SignatureBinding	AssociateSignatureKey
解除API与签名密钥的绑定关系	SignatureBinding	DisassociateSignatureKey
绑定流控策略	ThrottleBinding	AssociateRequestThrottlingPolicy
解除API与流控策略的绑定关系	ThrottleBinding	DisassociateRequestThrottlingPolicy

操作名称	资源类型	事件名称
批量解绑流控策略	ThrottleBinding	BatchDisassociateThrottlingPolicy
创建特殊设置	ThrottleSpecial	CreateSpecialThrottlingConfiguration
修改特殊流控	ThrottleSpecial	UpdateSpecialThrottlingConfiguration
删除特殊流控	ThrottleSpecial	DeleteSpecialThrottlingConfiguration
APP授权	AppAuth	CreateAuthorizingApps
解除授权	AppAuth	CancelingAuthorization
绑定域名	ApiGroup	AssociateDomain
绑定域名证书	ApiGroup	AssociateCertificate
修改域名	ApiGroup	UpdateDomain
解绑域名	ApiGroup	DisassociateDomain
删除域名证书	ApiGroup	DisassociateCertificate
创建ACL策略	Acl	CreateAclStrategy
修改ACL策略	Acl	UpdateAclStrategy
删除ACL策略	Acl	DeleteAcl
批量删除ACL策略	Acl	BatchDeleteAclV2
将API与ACL策略进行绑定	AclBinding	CreateApiAclBinding
解除API与ACL策略的绑定	AclBinding	DeleteApiAclBinding
批量解除API与ACL策略的绑定	AclBinding	BatchDeleteApiAclBinding
创建自定义认证	Authorizer	CreateCustomAuthorizer
修改自定义认证	Authorizer	UpdateCustomAuthorizer
删除自定义认证	Authorizer	DeleteCustomAuthorizer
导出API	Swagger	swaggerExportApiToGroup
导入API	Swagger	ImportApiDefinitions
创建VPC通道	Vpc	CreateVpcChannel
更新VPC通道	Vpc	UpdateVpcChannel
删除VPC通道	Vpc	DeleteVpcChannel

操作名称	资源类型	事件名称
添加或更新后端实例	Vpc	AddingBackendInstances
更新后端实例	Vpc	UpdateBackendInstances
删除后端实例	Vpc	DeleteBackendInstance
批量修改后端服务器状态可用	Vpc	BatchEnableMembers
批量修改后端服务器状态不可用	Vpc	BatchDisableMembers
修改VPC通道健康检查	Vpc	UpdateHealthCheck
添加或更新VPC通道后端服务器组	Vpc	CreateMemberGroup
删除VPC通道后端服务器组	Vpc	DeleteMemberGroup
更新VPC通道后端服务器组	Vpc	UpdateMemberGroup
创建分组自定义响应	ApiGroup	CreateGatewayResponse
修改分组自定义响应	ApiGroup	UpdateGatewayResponse
删除分组自定义响应	ApiGroup	DeleteGatewayResponse
修改分组下指定错误类型的自定义响应	ApiGroup	UpdateGatewayResponseType
删除分组指定错误类型的自定义响应配置	ApiGroup	DeleteGatewayResponseType
实例配置特性	Feature	CreateFeatureV2
创建专享版实例（按需）	Instance	CreateInstance
更新专享版实例	Instance	UpdateInstance
实例更新或绑定EIP	Instance	AddEip
实例解绑EIP	Instance	RemoveEip
开启实例公网出口	Instance	AddEngressEip
更新实例出公网带宽	Instance	UpdateEngressEip
关闭实例公网出口	Instance	RemoveEngressEip
开启实例公网入口	Instance	AddIngressEip
更新实例入公网带宽	Instance	UpdateIngressEip
关闭实例公网入口	Instance	RemoveIngressEip
删除专享版实例	Instance	DeleteInstances

操作名称	资源类型	事件名称
按需规格变更	Instance	CreatePostPayResizeOrder
接受或拒绝终端节点连接	vpc-endpoint	AcceptOrRejectEndpointConnections
批量添加实例终端节点连接白名单	vpc-endpoint	AddEndpointPermissions
批量删除实例终端节点连接白名单	vpc-endpoint	DeleteEndpointPermissions
批量添加或删除单个实例的标签	Instance	BatchCreateOrDeleteInstanceTags
导入微服务	Microservice	ImportMicroservice
创建SSL证书	SslCertificate	CreateCertificate
域名绑定SSL证书	ApiGroup	BatchAssociateCerts
域名解绑SSL证书	ApiGroup	BatchDisassociateCerts
删除SSL证书	SslCertificate	DeleteCertificate
修改SSL证书	SslCertificate	UpdateCertificate
SSL证书绑定域名	Certificate	BatchAssociateDomains
SSL证书解绑域名	Certificate	BatchDisassociateDomains
创建插件	Plugin	CreatePlugin
修改插件	Plugin	UpdatePlugin
删除插件	Plugin	DeletePlugin
插件绑定API	Plugin	AttachApiToPlugin
API绑定插件	Plugin	AttachPluginToApi
解除绑定插件的API	Plugin	DetachApiFromPlugin
解除绑定API的插件	Plugin	DetachPluginFromApi
创建APP	App	CreateAnApp
修改APP	App	UpdateApp
删除APP	App	DeleteAppV2
重置密钥	App	ResettingAppSecret
校验APP	App	CheckApp
创建APP Code	AppCode	CreateAppCode

操作名称	资源类型	事件名称
自动生成APP Code	AppCode	CreateAppCodeAuto
删除APP Code	AppCode	DeleteAppCode
设置APP的访问控制	AppAcl	UpdateAppAcl
删除APP的访问控制	AppAcl	DeleteAppAcl
创建凭据配额	AppQuota	CreateAppQuota
修改凭据配额	AppQuota	UpdateAppQuota
删除凭据配额	AppQuota	DeleteAppQuota
凭据配额绑定凭据列表	AppQuotaBinding	AssociateAppsForAppQuota
解除凭据配额和凭据的绑定	AppQuotaBinding	DisassociateAppQuotaWithApp

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**删除追踪器**。

12.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。
- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

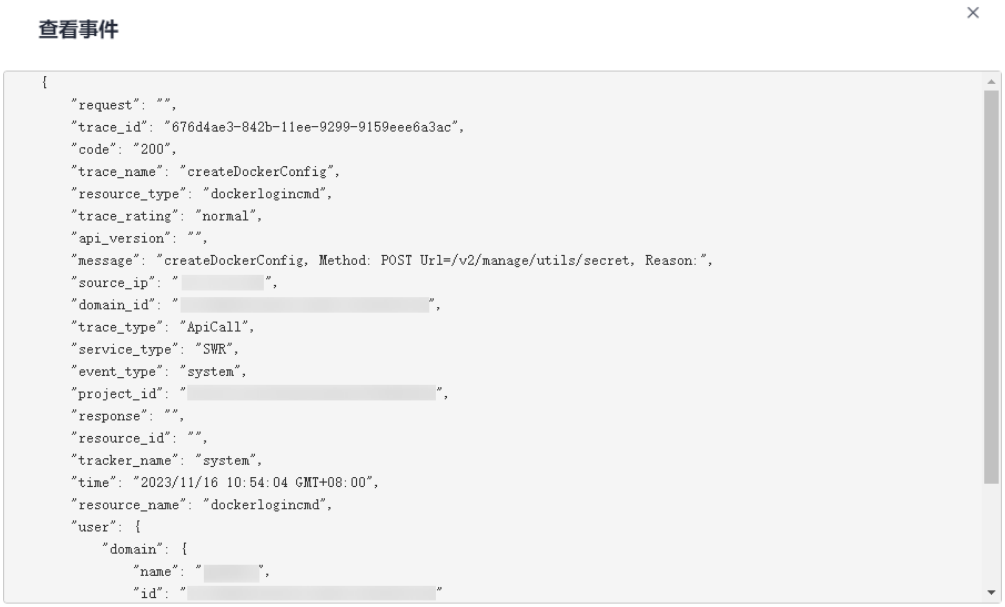
在新版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 企业项目ID：输入企业项目ID。
   - 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
   - 单击 按钮，可以自定义事件列表的展示信息。启用表格内容折行开关 ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。
7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

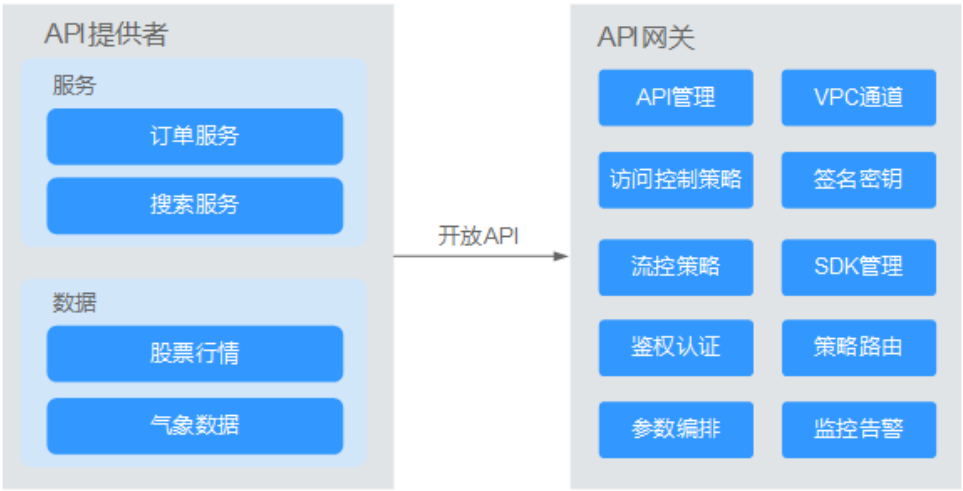
13 共享版操作指导（仅存量用户使用）

13.1 APIG 使用流程

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网关的**开放API**和**调用API**功能，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。

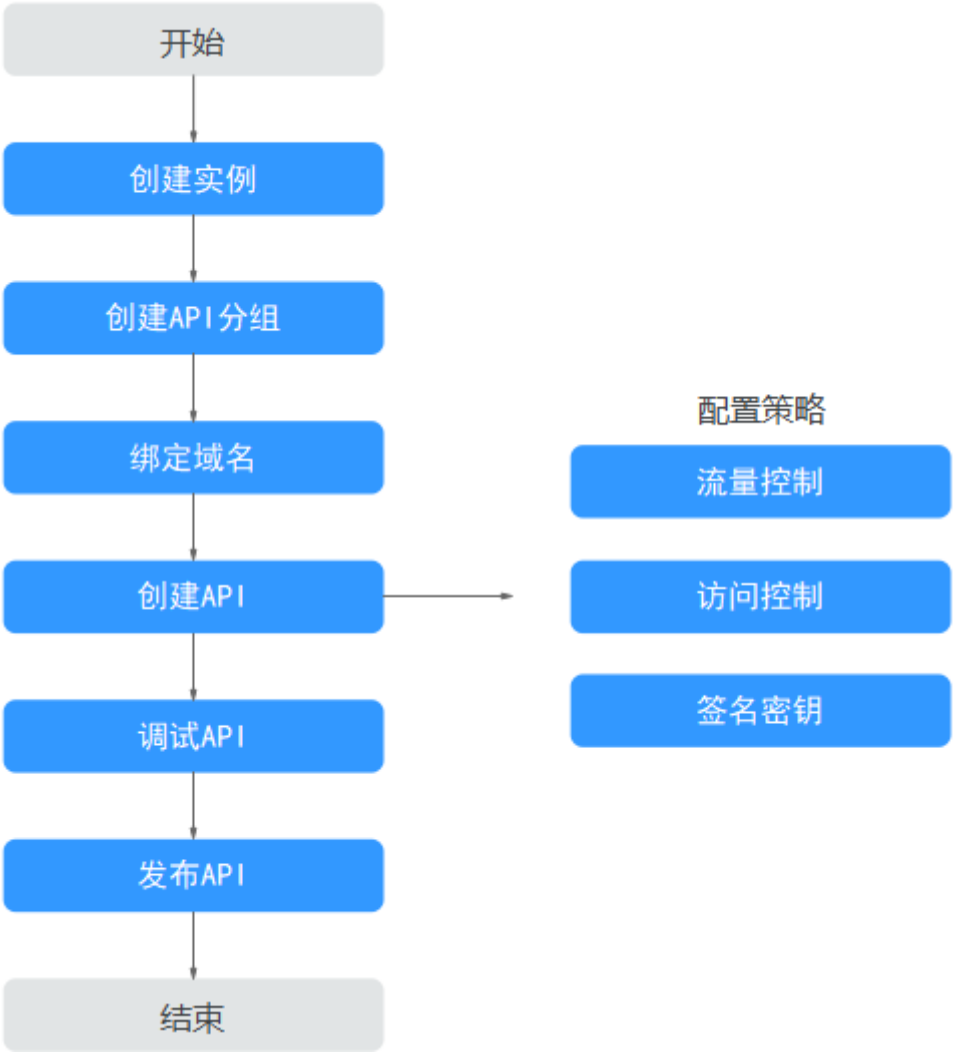
- **开放API**
  企业或开发者通过API网关开放自身的服务与数据。

  图 13-1 API 网关服务开放 API



开放API的业务使用流程如下图所示。

图 13-2 API 网关服务开放 API 基本流程



a. 创建实例

共享版无需购买实例，可直接进入**共享版**。

b. **创建API分组**

每个API都归属到某一个API分组下，在创建API前应提前创建API分组。

c. **绑定域名**

在开放API前，您需要为API分组绑定一个独立域名，供API调用者访问API使用。

在绑定独立域名前，您可以使用系统为API分配的默认子域名进行API调试，每天最多可以访问默认子域名1000次。

d. **创建API**

把已有后端服务封装为标准RESTFul API，并对外开放。

API创建成功后，您可根据业务需求对API设置访问策略：

- **流控控制**

  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。

- **访问控制**

  访问API的IP地址和账户，您可以通过设置IP地址或账户的黑白名单来拒绝/允许某个IP地址或账户访问API。

- **签名密钥**

  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。

e. **调试API**

   验证API服务的功能是否正常可用。

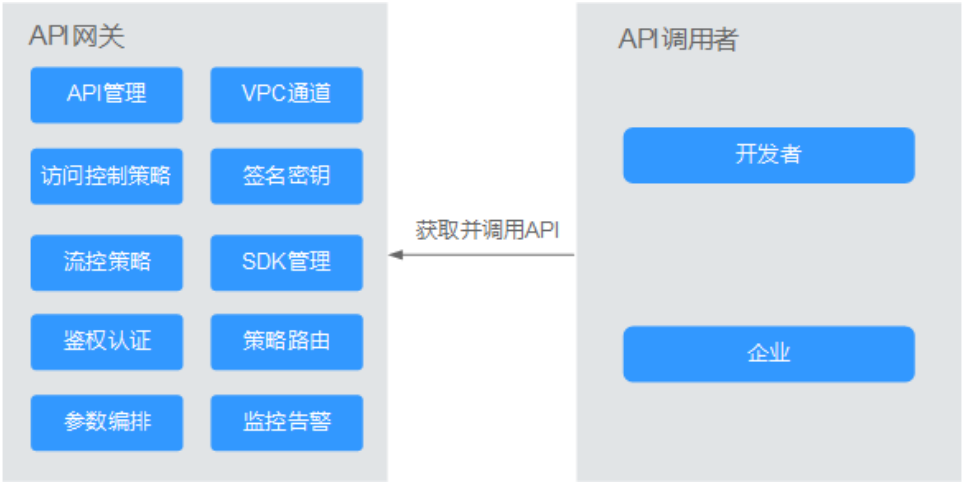
f. **发布API**

   把API发布到环境中，API只有在发布到环境后，才支持被调用。

- **调用API**

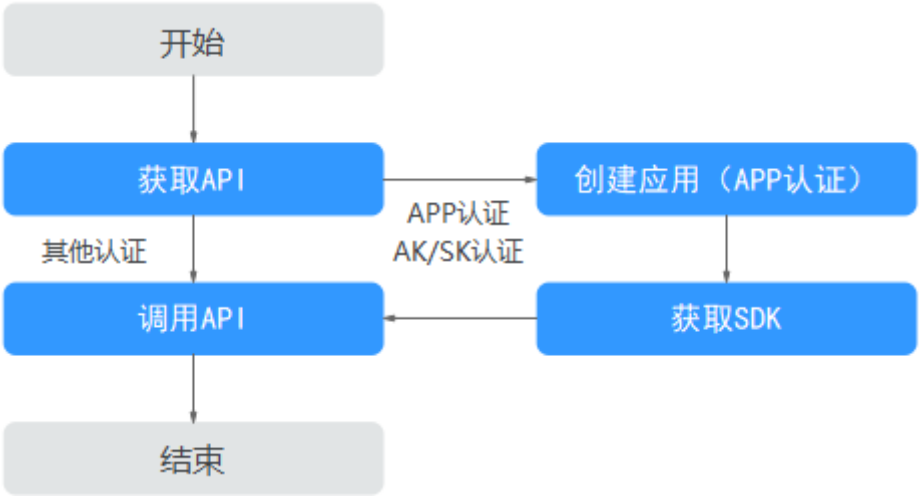
  企业或开发者如何获取并调用他人在API网关开放的API，减少开发时间与成本。

图 13-3 API 网关服务调用 API



调用API的业务使用流程如下图所示。

图 13-4 API 网关服务调用 API 基本流程



a. **获取API**

获取API的请求信息，包括访问域名、请求协议、请求方法、请求路径以及认证方式等信息。

b. **创建应用**

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，使用APP认证调用API。

c. **获取SDK**

可通过SDK对AK/SK生成签名，并调用API。

d. **调用API**

通过获取API及API访问地址，调用API。根据API使用认证方式的不同，调用API时需要进行不同的认证鉴权操作。

13.2 进入共享版控制台

存量用户进入共享版控制台操作如下。

步骤1 登录**API网关控制台**页面。

步骤2 在“总览”页面的右上角单击“进入共享版控制台”，进入共享版页面。

----结束

13.3 API 分组管理

13.3.1 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。

操作步骤

步骤1 **进入共享版控制台**。

步骤2 单击“开放API > API分组”，进入到API分组信息页面。

步骤3 单击“创建分组”，弹出“创建分组”对话框。填写如**表13-1**所示信息。

表 13-1 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。

信息项	描述
描述	对分组的介绍。

步骤4 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。
- 共享版中的API，分组子域名可公网访问。
- 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。

13.3.2 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。

说明

- 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，最多可以添加5个独立域名，不限访问次数。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. 共享版：已将独立域名CNAME解析到分组的子域名上，具体方法请参见**增加CNAME类型记录集**。
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 **进入共享版控制台**。

步骤2 单击“开放API > API分组”，进入到API分组信息页面。

步骤3 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4 单击“绑定独立域名”，设置域名信息。

步骤5 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6 （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。

图 13-5 添加 SSL 证书

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。
- 如果需要更换/编辑此SSL证书，单击证书名称后的，修改证书信息。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。

13.3.3 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。

说明

如果API分组下存在API，API分组无法被删除。

前提条件

已创建分组。

操作步骤

步骤1 **进入共享版控制台**。

步骤2 单击“开放API > API分组”，进入到API分组信息页面。

步骤3 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4 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

13.3.4 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 **进入共享版控制台**。

步骤2 单击“开放API > API分组”，进入到API分组信息页面。

步骤3 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4 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13-3**。

----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13-2**，其中响应状态码可以按实际需要做自定义修改。

表 13-2 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	404	未匹配到API
请求参数错误	400	请求参数校验失败、不支持的HTTP方法
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 13-3 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调用生成请求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

运行时变量名称	描述
$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

13.4 API 管理

13.4.1 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。

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 **进入共享版控制台**。

步骤2 单击“开放API > API管理”，进入到API列表信息页面。

步骤3 单击“新建API”，进入“新建API”页面。填写如**表13-4**所示信息。

表 13-4 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。

信息项	描述
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。
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。 • 华为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**调用API**。 推荐使用APP认证方式。 **须知** • 认证方式为华为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4 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13-5所示信息。

图 13-6 定义 API 请求

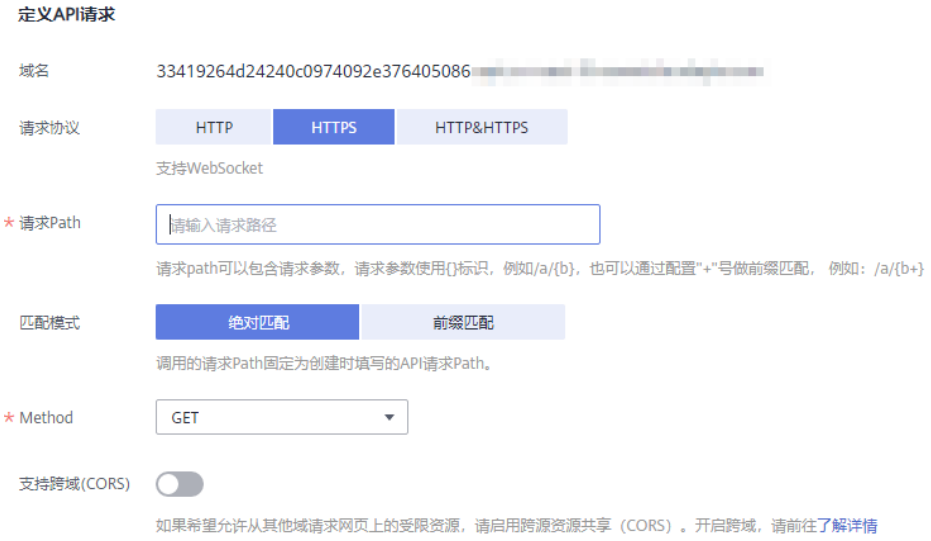


表 13-5 定义 API 请求

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 API网关支持WebSocket数据传输，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。
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}。如果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。

信息项	描述
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** ● 匹配url时，优先进行绝对匹配，再进行前缀匹配，前缀匹配短的优先级最低。 例如，请求路径为/a/b/c，使用绝对匹配；请求路径为/a和/a/b，使用前缀匹配。匹配url的顺序为/a/b/c > /a/b > /a。 ● 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。
支持跨域(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**。
请求体内容描述	**仅当“请求方法”选择“POST”、“PUT”、“PATCH”或“ANY”时可配置。** 填写API请求中请求体的描述信息，用于帮助API调用者理解如何正确封装API请求。

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13-6**所示信息。

表 13-6 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。
透传	请求参数是否透传到后端服务。
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。
枚举	请求参数的枚举值，请求参数的值只能从枚举值中选择，多个枚举值间用英文逗号隔开。
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13-7**、**表13-8**、**表13-9**。

表 13-7 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** • API网关支持WebSocket数据传输，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。 • 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。 • **如果使用VPC通道，选择已创建的VPC通道名称。** 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。 • **如果不使用VPC通道，需要设置后端服务地址。** 填写后端服务的访问地址，格式：“主机:端口”。主机为后端服务的访问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。 如果后端服务地址中需要携带环境变量，则使用“#变量名#”的形式将环境变量添加到后端服务地址中，如#ipaddress#。支持添加多个环境变量，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，可填写范围1ms~60000ms。 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 13-8 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。
版本或别名	支持选择函数的版本或别名，函数的版本或别名功能请参考《函数工作流 FunctionGraph用户指南》的“版本管理”和“别名管理”章节。
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13-7**中的后端超时。
后端认证	参考**表13-7**中的后端认证。

表 13-9 Mock 类型定义后端服务

服务参数	参数说明
Mock自定义返回码	选择API响应的HTTP状态码，如果当前实例不支持，请联系技术支持升级实例。
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13-7**中的后端认证。
请求头参数	自定义API响应的响应头信息。 单击“添加header参数”，并填写参数名、参数值和参数描述。

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“添加策略后端”。
2. 策略后端增加的参数，具体如表13-10所示，其他参数说明参见表13-7。

图 13-7 添加后端策略

表 13-10 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13-11所示。

表 13-11 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。

信息项	描述
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13-8所示。

图 13-8 后端服务参数配置

   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。

须知

常量参数会明文展示，为防止信息泄露，请谨慎配置。

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13-12所示信息。

图 13-9 添加常量参数

表 13-12 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。

信息项	描述
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13-13所示信息。

图 13-10 添加系统参数

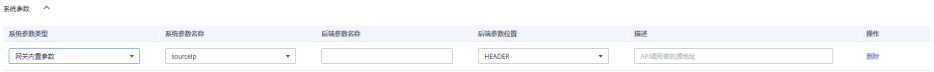


表 13-13 系统参数

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调用者的源地址。 ■ stage：API调用的部署环境。 ■ apiId：API的ID。 ■ appId：API调用者的APP ID。 ■ requestId：当次调用API所生成的请求ID。 ■ serverAddr：网关服务器的地址 。 ■ serverName：网关服务器的名称。 ■ handleTime：本次调用API的处理时间。 ■ providerAppId：API提供者的应用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。
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13-14所示信息。

表 13-14 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

创建 API 相关的 FAQ

API网关是否支持多后端节点方案?

为什么后端服务调用失败?

在API网关中创建完成API，调用时报“No backend available”错误，怎么解决?

后续操作

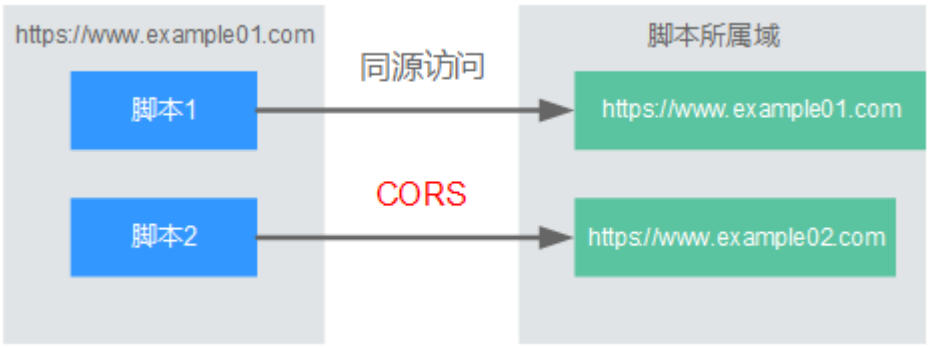
您创建完API后，通过**调试API**，验证服务是否正常。

13.4.2 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 13-11 跨域访问示意图



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。

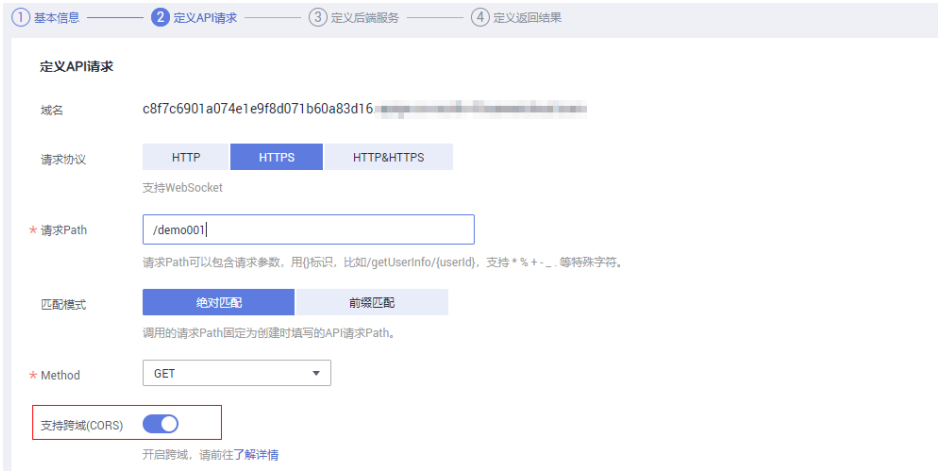
开启跨域访问

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**。

  图 13-12 支持跨域



- **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”。

图 13-13 预检请求-使用无认证

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

图 13-14 预检请求-设置 API 请求

c. 后端服务选择Mock。

图 13-15 预检请求-后端服务类型 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
Origin: 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
Origin: 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。

说明

跨域共享资源插件不需要创建一个“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
Origin: 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"}
```

13.4.3 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 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”。

图 13-16 调试界面

左侧为API请求参数配置区域，参数说明如表13-15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 13-15 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。
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。

说明

不同类型的请求，调试界面展现的信息项有差异。

步骤4 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5 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**。

13.4.4 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，才支持被授权。
- 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 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“更多 > 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4 选择API授权环境，查询并勾选应用后，单击“授权”。

步骤5 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。

13.4.5 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 通过以下任意一种方法，进入“发布API”页面。

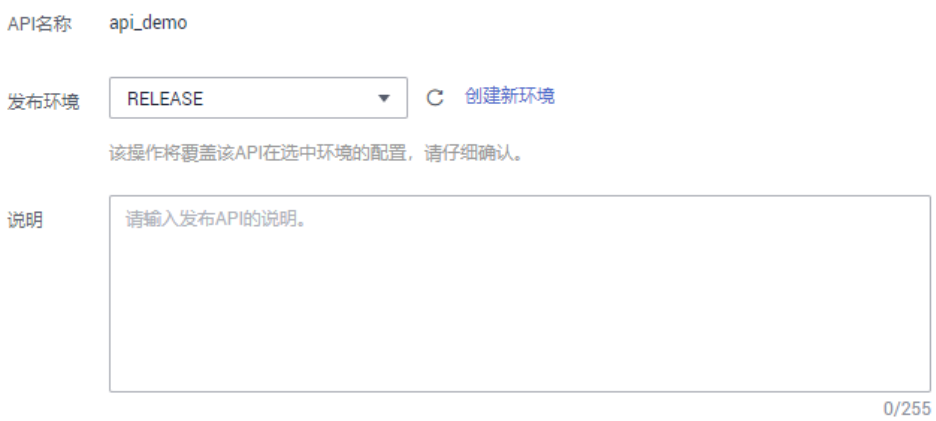
- 在待发布的API所在行，单击“发布”。
- 单击“*API名称*”，进入API详情页面。在右上角单击“发布”。

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4 选择API需要发布到的环境，并填写发布说明。

图 13-17 发布 API



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5 单击“发布”，完成API发布。

----结束

查看发布历史

步骤1 单击“开放API > API管理”，进入到API管理信息页面。

步骤2 单击待查看发布历史的API名称，进入API详情页面。

步骤3 单击“发布历史”，进入“发布历史”页签。

查看API的发布历史信息。

图 13-18 发布历史

步骤4 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5 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

发布 API 相关的 FAQ

对API的修改是否需要重新发布?

API发布到RELEASE环境可以正常访问，发布到非RELEASE环境无法访问?

API发布到不同环境后，会调用不同的后端服务吗?

13.4.6 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 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4 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。

13.4.7 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 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4 按照提示，在输入框中输入“DELETE”，单击“确定”，完成API删除。

----结束

13.4.8 导入 API

操作场景

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。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。

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

- 导入API前，您需要在导入的API定义文件中补全Swagger扩展定义。如果“扩展定义”中未包含需要的定义，请提前在API网关中创建。
- 导入API前，请确保API分组和API的配额满足需求。

操作步骤

步骤1 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 单击“导入API”，进入“导入API”界面。

步骤4 选择如表13-16所示参数。

图 13-19 导入 API

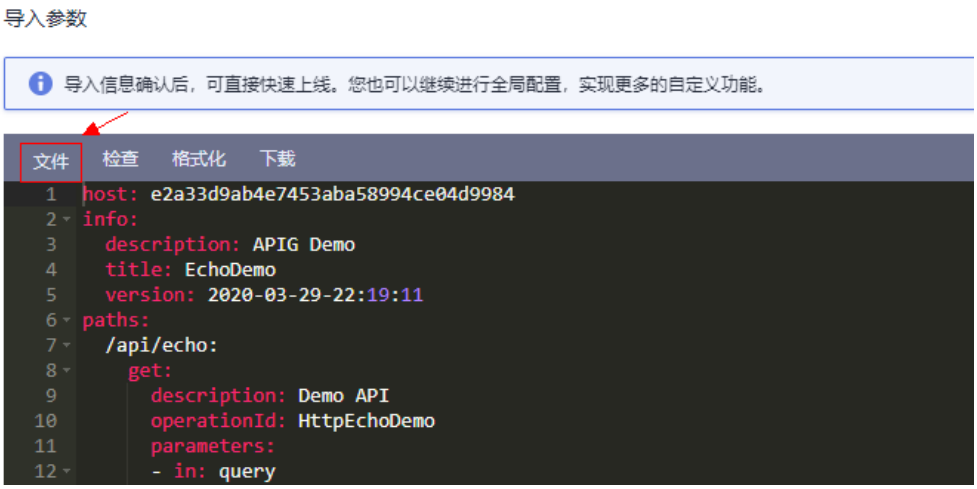
表 13-16 导入 API

参数名称	说明
导入方式	导入方式包含以下2种： • 生成新的分组：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。 • 选择已有分组：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“选择已有分组”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名称相同时，导入的API会覆盖已有的API。 仅在选择“选择已有分组”时，需要选择是否覆盖。
扩展覆盖	勾选后，当导入API扩展定义项名称（ACL，流控等）与已有的策略（ACL，流控等）名称相同时，会覆盖已有的策略（ACL，流控等）。

步骤5 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。

图 13-20 导入参数



步骤6 （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。

图 13-21 修改全局配置

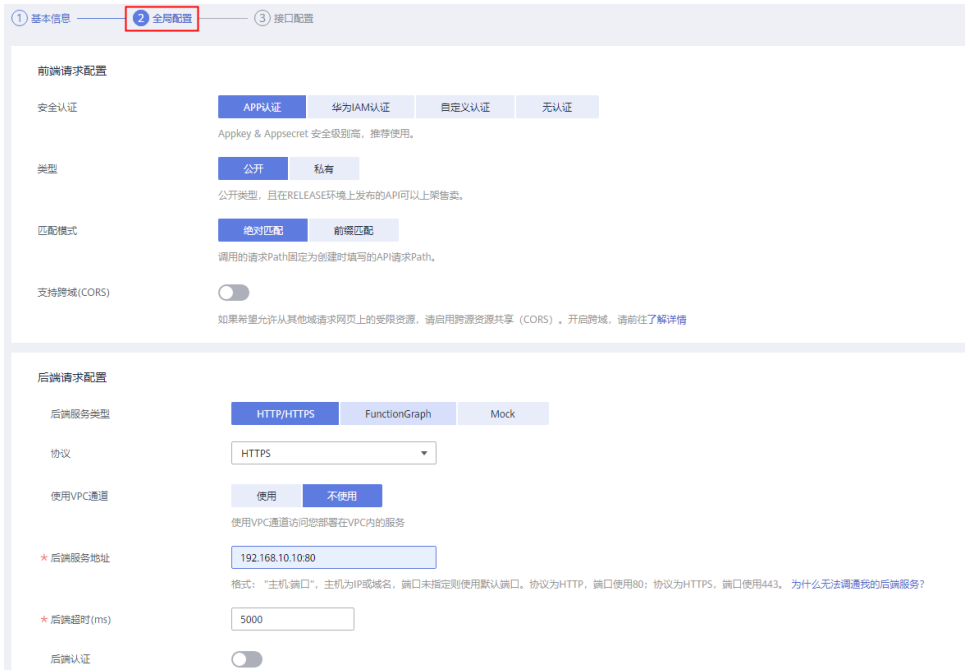


图 13-22 修改接口配置

步骤7 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。

13.4.9 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 进入共享版控制台。

步骤2 单击“导出API”，进入“导出API”界面。

步骤3 设置如表13-17所示参数。

图 13-23 导出 API

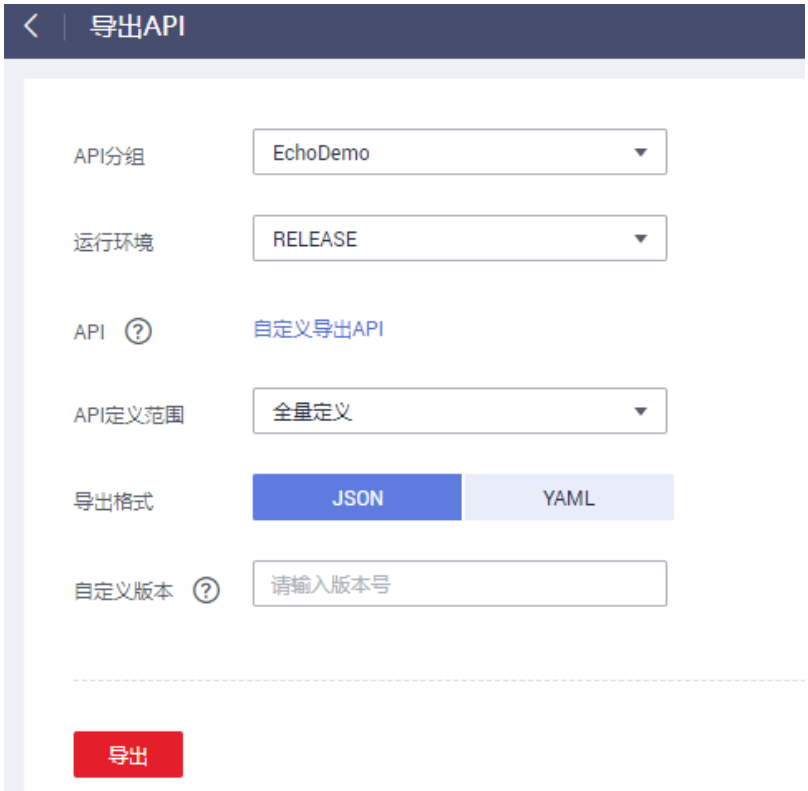


表 13-17 导出 API

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。

参数名称	说明
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。
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4 单击“导出”，右侧显示导出结果。

----结束

13.5 流量控制

13.5.1 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

- 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。
- 如果API未绑定流控策略，共享版API网关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 **进入共享版控制台**。

步骤2 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤3 单击“创建流控策略”，弹出“创建流控策略”对话框。输入如表13-18所示信息。

表 13-18 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。

信息项	描述
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APP认证或IAM认证**。 ● 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。 ● 如果主账号下有多个子用户访问API，按主账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**。 ● 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4 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。

图 13-24 绑定 API

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，此应用的应用流量受特殊应用的阈值限制，而API流量和用户流量受流量策略限制。
- 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，此租户的用户流量受特殊租户的阈值限制，而API流量和应用流量受流量策略限制。

13.5.2 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 **进入共享版控制台**。

步骤2 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤3 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4 单击“确定”，完成流控策略的删除。

----结束

13.5.3 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 进入共享版控制台。

步骤2 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤3 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4 单击“特殊应用”，进入特殊应用页面。

步骤5 单击“添加特殊应用”，弹出“添加特殊应用”对话框。

步骤6 通过以下两种方式，添加特殊应用。

图 13-25 选择应用

- 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

特殊应用流控值和应用流量限制值共同作用时，以特殊应用流控值为准。

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

添加特殊租户

步骤1 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2 在“API凭证”页面查看账号ID和项目ID。

图 13-26 查看账号 ID 和项目 ID

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 单击待添加特殊租户的流控策略的名称，进入流控详情页面。

步骤5 单击“特殊租户”，进入特殊租户页面。

步骤6 单击“添加特殊租户”，弹出“添加特殊租户”对话框。

步骤7 输入如**表13-19**所示信息。

图 13-27 添加特殊租户信息

表 13-19 特殊租户信息

信息项	描述
租户ID	**步骤2**中获取的账号ID或项目ID。 • 绑定APP认证的API时，租户ID为项目ID。 • 绑定华为IAM认证的API时，租户ID为账号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8 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

13.5.4 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 进入共享版控制台。

步骤2 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤3 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4 单击“特殊应用”，进入“特殊应用”页面。

步骤5 在待删除的特殊应用所在行，单击“删除”，弹出对话框。

步骤6 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 选择“开放API > 流量控制”，进入到流量控制信息页面。

步骤2 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3 单击“特殊租户”，进入“特殊租户”页面。

步骤4 在待删除的特殊租户所在行，单击“删除”，弹出对话框。

步骤5 单击“确定”，完成对特殊租户的删除。

----结束

13.6 访问控制

13.6.1 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地址和账户，您可以通过设置IP地址或账户的黑白名单来拒绝/允许某个IP地址或账户访问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

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 进入共享版控制台。

步骤2 选择“开放API > 访问控制”，进入访问控制策略列表页面。

步骤3 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4 输入表13-20如所示信息。

表 13-20 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。 ● 账号名：允许/禁止访问API的账号名。
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/账号名。

信息项	描述
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。
账号名	输入需要允许或者禁止访问API的IAM账号，**仅适用于API的安全认证方式为IAM认证时**。 仅在“限制类型”为“账号名”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账号维度的访问控制，不能对单个IAM用户进行访问控制。

步骤5 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

13.6.2 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 进入共享版控制台。

步骤2 选择“开放API > 访问控制”，进入访问控制策略列表页面。

步骤3 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4 单击“确定”，完成访问控制策略的删除。

----结束

13.7 环境管理

13.7.1 创建环境和环境变量

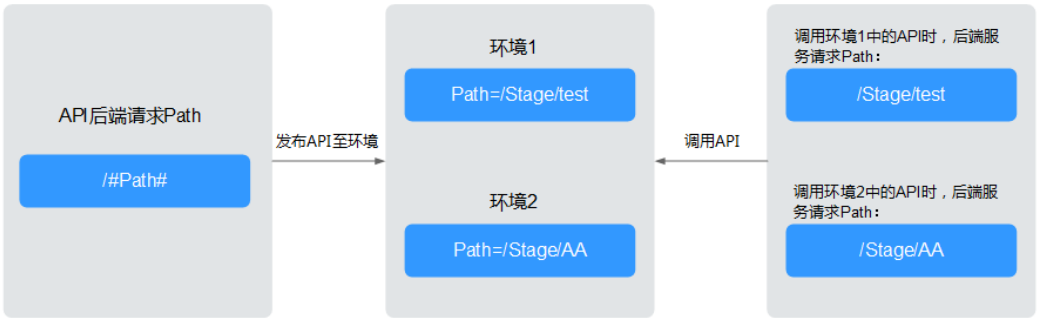
操作场景

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 13-28 环境变量



说明

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 进入共享版控制台。

步骤2 选择“开放API > 环境管理”，进入到环境管理信息页面。

步骤3 单击“创建环境”，弹出“创建环境”对话框。填写如表13-21所示信息。

图 13-29 创建环境

表 13-21 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4 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 选择“开放API > API分组”，进入到API分组信息页面。

步骤2 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3 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4 填写如表13-22所示信息。

图 13-30 新增变量

表 13-22 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5 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。

使用 API 方式创建环境

您还可以使用API的方式创建环境和变量，具体操作请查看以下链接。

创建环境

新建变量

环境变量相关的 FAQ

API发布到不同环境后，会调用不同的后端服务吗?

13.7.2 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 **进入共享版控制台**。

步骤2 选择“开放API > 环境管理”，进入到环境管理信息页面。

步骤3 在待删除的环境所在行，单击“删除”，弹出对话框。

说明

仅在环境未被API发布时，支持删除。

步骤4 单击“确定”，完成环境管理信息。

----结束

13.8 签名密钥

13.8.1 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。

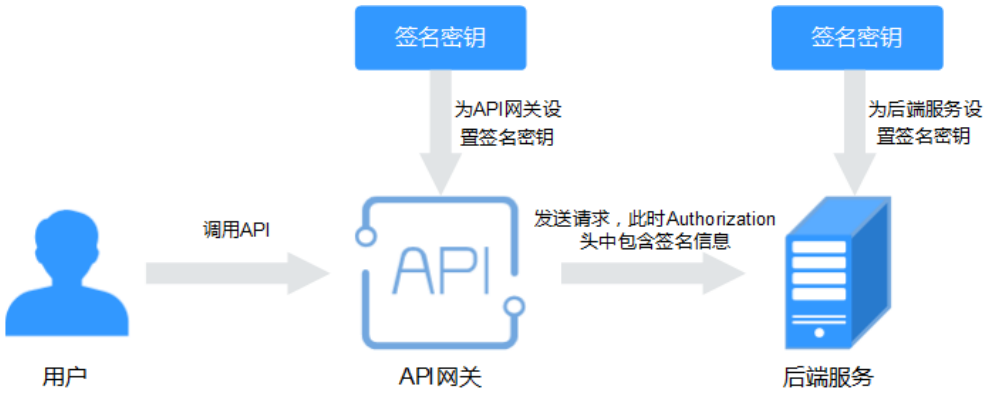
说明

同一个环境中一个API只能绑定一个签名密钥，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 13-31 签名密钥流程



创建签名密钥

步骤1 进入共享版控制台。

步骤2 单击“开放API > 签名密钥”，进入签名密钥管理信息页面。

步骤3 单击“创建密钥”，弹出“创建密钥”对话框。

步骤4 填写如表13-23所示信息。

表 13-23 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。
类型	专享版支持选择签名密钥的认证类型，可选择“HMAC”和“Basic”。
Key	与“Secret”配合使用，表示签名密钥对。 • HMAC：填写hmac认证所使用密钥对的Key。 • Basic：填写basic认证所使用的用户名。
Secret	与“Key”配合使用，表示签名密钥对。 • HMAC：填写hmac认证所使用密钥对的Secret。 • Basic：填写basic认证所使用的密码。
确认Secret	填写与Secret一致的值。

步骤5 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**签名算法**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。

13.8.2 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 进入共享版控制台。

步骤2 单击“开放API > 签名密钥”，进入签名密钥管理信息页面。

步骤3 通过以下任意一种方法，弹出对话框。

- 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4 单击“确定”，完成密钥的删除。

----结束

13.9 VPC 通道

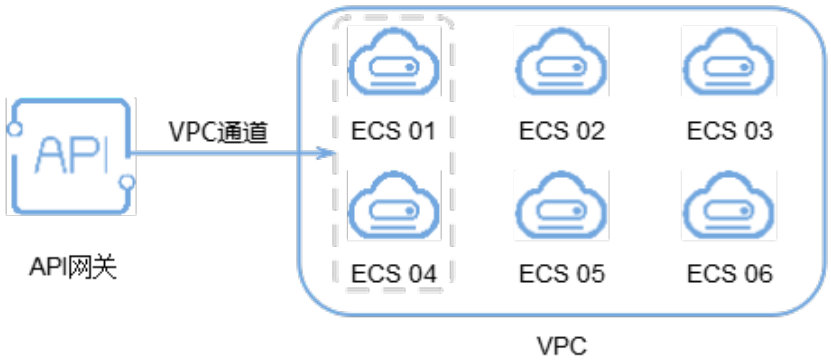
13.9.1 创建 VPC 通道

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。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 13-32 通过 API 网关访问 VPC 通道中的 ECS



说明

前提条件

- 已创建云服务器。
- 用户需要具备VPC Administrator角色权限。

创建快速通道

步骤1 进入共享版控制台。

步骤2 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤3 单击“创建快速通道”，进入“新建VPC通道”页面，填写如表13-24所示信息。

图 13-33 创建快速通道

表 13-24 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。
成员类型	选择负载通道中的服务器成员类型。成员类型在负载通道创建后将不能修改。 ● 实例：通过选择弹性云服务器的方式添加负载通道成员。 ● IP地址：通过填写IP地址的方式添加负载通道成员。
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 ● 加权最小连接 ● 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4 单击“下一步”，进入“添加云服务器”页面。

步骤5 单击“添加云服务器”，弹出“添加云服务器”对话框。

步骤6 勾选需要添加的云服务器，单击“添加”。

说明

使用共享版API网关时，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7 单击“完成”，完成快速通道的创建。

----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。

13.9.2 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 进入共享版控制台。

步骤2 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤3 通过以下任意一种方法，弹出对话框。

- 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4 单击“确定”，完成VPC通道的删除。

----结束

13.9.3 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 进入共享版控制台。

步骤2 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤3 单击“*VPC通道名称*”，进入VPC通道详情页面。

步骤4 单击“健康检查”，进入“健康检查”页签。

步骤5 单击“编辑”，弹出“编辑健康检查配置”对话框。

步骤6 编辑如表13-25所示信息。

表 13-25 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。

信息项	描述
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。
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7 单击“确定”，完成健康检查配置的修改。

----结束

13.9.4 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 进入共享版控制台。

步骤2 单击“开放API > VPC通道”，进入到VPC通道列表页面。

步骤3 单击“*VPC通道名称*”，进入VPC通道详情页面。

步骤4 单击“云服务器”，进入“云服务器”页签。

步骤5 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

13.10 自定义认证

13.10.1 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/华为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。

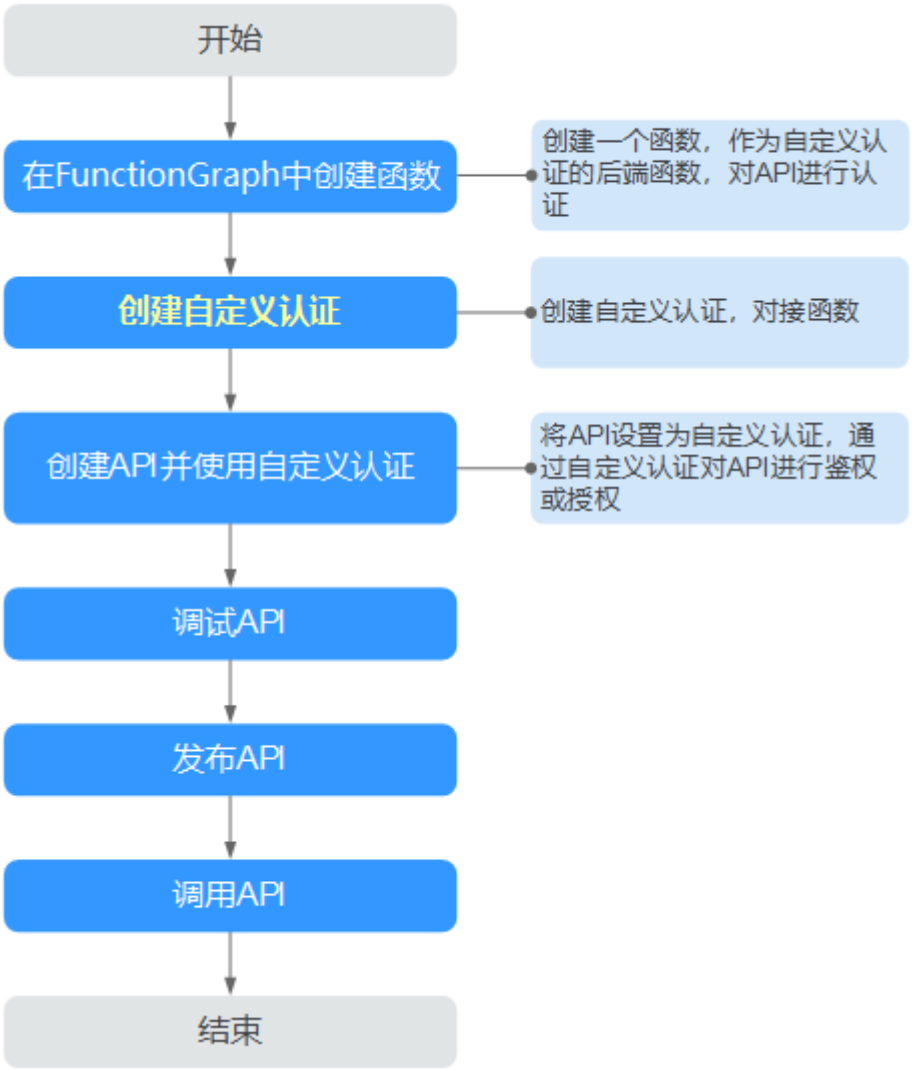
说明

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 13-34 通过自定义认证调用 API



前提条件

- 已在函数工作流服务中完成函数创建。
- 用户还需具备FunctionGraph Administrator角色权限。

操作步骤

步骤1 进入共享版控制台。

步骤2 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3 填写如表13-26所示信息。

表 13-26 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，支持添加Header参数和Query参数，其中Header的参数名不区分大小写。 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。
是否发送body	指是否将API请求的body体内容传递给认证函数。body体内容传给函数的方式，与header、query内容传递一致。
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4 单击“创建”，完成自定义认证的创建。

----结束

13.10.2 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 **进入共享版控制台**。

步骤2 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”，弹出对话框。

步骤3 单击“确定”。

----结束

13.11 监控

13.11.1 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 13-27 API 网关共享版支持的监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	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	单个API	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	单个API	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	单个API	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	单个API	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	单个API	1分钟
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	单个API	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	单个API	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	单个API	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	单个API	1分钟

维度

表 13-28 API 网关共享版监控指标测量维度

Key	Value
api_id	API

13.11.2 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 单击“*API名称*”，进入“总览”页面。

步骤4 单击“查看更多监控”，进入云监控界面，参考**创建告警规则**为API网关创建告警规则。

----结束

13.11.3 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 进入共享版控制台。

步骤2 单击“开放API > API管理”，进入到API管理信息页面。

步骤3 单击“*API名称*”，进入“总览”页面。

查看API的各项监控指标。

步骤4 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

13.12 应用管理

13.12.1 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**《API网关开发指南》**。

说明

- 使用无认证/华为IAM认证的API，无需创建应用。

创建应用

步骤1 进入共享版控制台。

步骤2 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 单击“创建应用”，弹出“创建应用”对话框。填写应用信息。

表 13-29 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4 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5 单击*应用名称*，进入应用详情页面，查看AppKey和AppSecret。

图 13-35 应用详情

----结束

绑定 API

步骤1 进入共享版控制台。

步骤2 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 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4 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

- 只有APP认证的API才可以被应用绑定。
- 一个应用可以绑定多个APP认证的API，一个APP认证的API也可以绑定多个应用。
- 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。

13.12.2 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 进入共享版控制台。

步骤2 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 通过以下任意一种方式，进入对话框。

- 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4 单击“确定”，完成应用的删除。

----结束

13.12.3 重置 AppSecret

操作场景

AppKey唯一且不可重置，AppSecret支持重置，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 进入共享版控制台。

步骤2 单击“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 单击待重置AppSecret的应用名称，进入应用详情页面。

步骤4 在右上角单击“重置AppSecret”，弹出“重置AppSecret”对话框。

步骤5 单击“确定”，完成AppSecret的重置。

----结束

13.12.4 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 进入共享版控制台。

步骤2 选择“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 单击待查看的应用名称，进入应用详情页面。

步骤4 单击“AppCode”页签，进入AppCode的管理界面。

步骤5 单击“添加AppCode”，生成AppCode。可自动生成，也可手动输入。

----结束

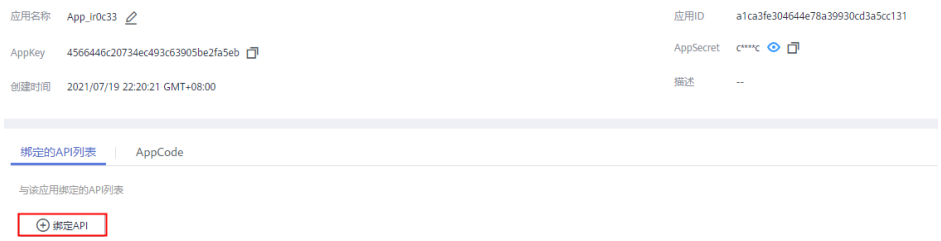
使用 AppCode 进行 API 请求的简易认证

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

13.12.5 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 进入共享版控制台。

步骤2 选择“调用API > 应用管理”，进入到应用管理信息页面。

步骤3 单击待查看的应用名称，进入应用详情页面。

步骤4 单击待查看的API名称，进入API详情页面，查看API详情。

----结束

13.13 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**调用API**。

本章节主要提供APP认证的SDK下载以及文档。IAM认证请参考“**使用IAM认证调用API**”章节。

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

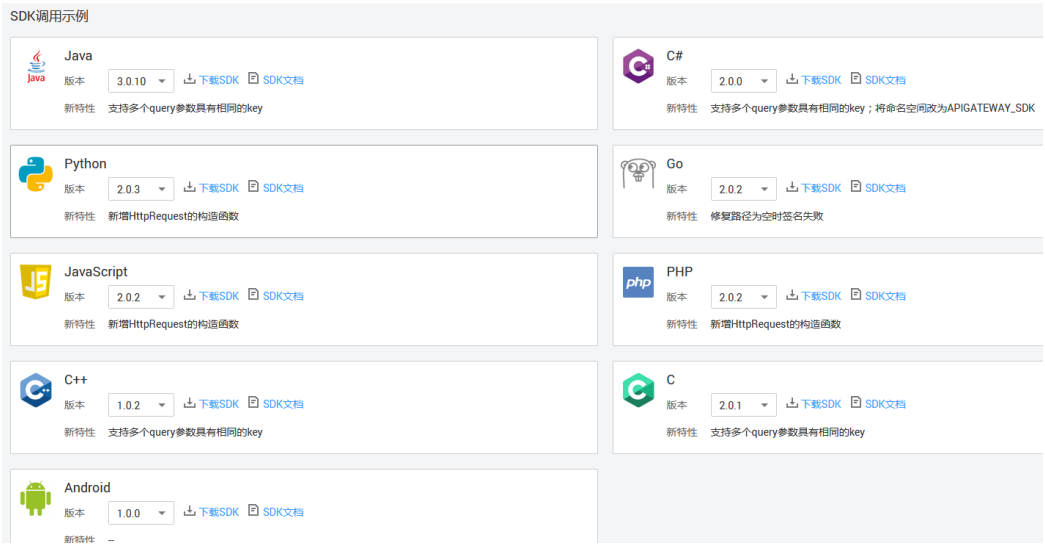
步骤1 进入共享版控制台，单击  。

步骤2 单击“帮助中心”，进入到帮助中心页面。

步骤3 单击“SDK使用指引”页签。

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

13.14 已购买 API

操作场景

API网关共享版支持查看已购买的API，明确已购买服务的详情。并通过调试API，验证服务是否正常。

已购买的API，需要通过APP认证方式调用。

前提条件

已从云商店购买了API。

操作步骤

步骤1 进入共享版控制台。

步骤2 单击“调用API > 已购买API”，进入到已购买API分组信息页面。

图 13-36 已购买 API 分组示例

步骤3 单击待查看的API分组名称，进入此分组详情页面。

查看此分组下已购买的API列表和此分组的详细信息。

图 13-37 已购买 API 的分组详情示例

步骤4 在待调试API所在行，单击“调试API”，跳转到“调试API”页面。

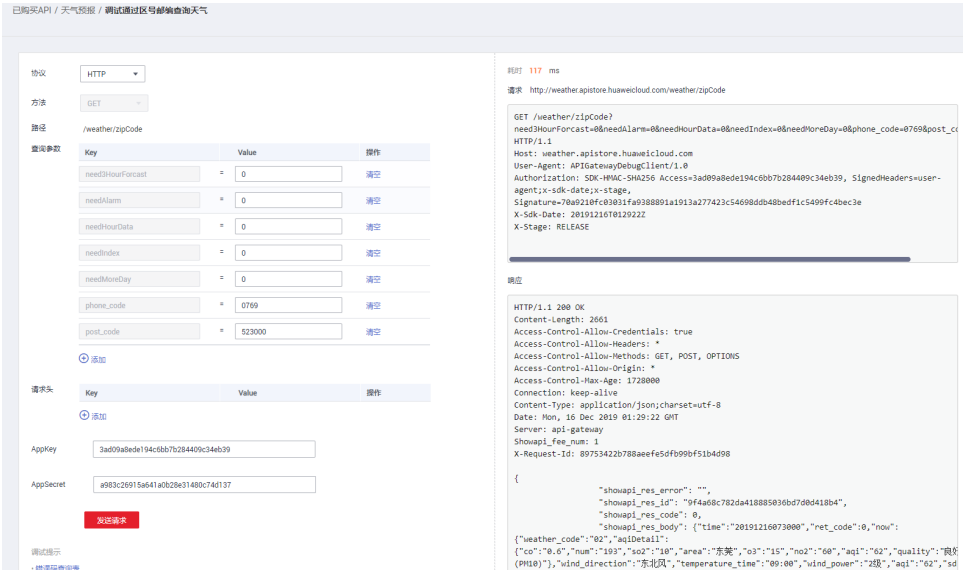
步骤5 左侧为API请求参数配置区域，参数说明如表13-30所示。右侧为API发送的请求信息和API请求调用后的返回结果回显。

表 13-30 调试 API

参数名称	说明
协议	仅在“请求协议”为“HTTP&HTTPS”时，支持修改。
方法	仅在“Method”为“ANY”时，支持修改。
路径	仅在“匹配模式”为“前缀模式”时，支持自定义路径。
路径参数	仅在“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。
Body	仅在“Method”为“PATCH”/“POST”/“PUT”时，支持修改。

步骤6 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。



步骤7 开发者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。

----结束

13.15 调用已发布的 API

13.15.1 调用 API

API提供者在API网关开放自己的API后，API调用者从API网关中调用API。

调用限制

如果您使用调试域名（创建API分组时系统分配的调试域名）访问API，该调试域名每天最多可以访问1000次。

获取 API 的调用信息

在调用API前，您需要向API提供者获取API的调用信息。

- 获取API的请求信息

  在API网关控制台选择“开放API > API管理”，单击API的名称进入“调用信息”页面，可获取API的“域名”、“请求方法”和“请求路径”，以及API的基本信息。

- 获取API的认证信息

  根据API使用的安全认证方式不同，还要获取相关的请求认证信息：

认证方式	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AppKey和AppSecret，以及认证签名所使用的SDK。
APP认证（简易认证）	向API提供者获取该API所授权应用的AppCode。

认证方式	认证信息
IAM认证（Token认证）	获取云服务平台的用户账号密码。
IAM认证（AK/SK认证）	获取云服务平台的用户账号的AK/SK，以及认证签名所使用的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。

- 获取应用的AppKey和AppSecret：

  在API网关共享版控制台选择“调用API > 应用管理”，在应用列表中单击API所授权应用的名称，进入应用详情页面，获取应用的AppKey和AppSecret。
- 获取认证签名所使用SDK：

  在API网关共享版控制台选择“帮助中心”，在“SDK使用指引”页签中下载对应语言所使用SDK。
- 获取AppCode：

  在API网关共享版控制台选择“调用API > 应用管理”，在应用列表中单击API所授权应用的名称，进入应用详情页面，在“AppCodes”页签中获取AppCode。

调用 API

说明

本章节仅提供请求地址和认证参数的配置指导，客户端的其他参数配置需要用户自行调整，如超时配置、SSL配置等。如果客户端参数配置错误会导致业务受损，建议参考业界标准进行配置。

1. 构造API请求，示例如下：

```
POST https://{Address}/{Path}?{Query}
{Header}

{
 {Body}
}
```

- **POST**：请求方法，需替换为**获取API的调用信息**中获取的请求方法。
- **{Address}**：请求地址，需替换为**获取API的调用信息**中获取的域名地址。

API调用场景	API请求参数配置
使用域名调用API	使用服务分配的调试域名或服务绑定的域名调用API，无需另外配置。
使用IP调用API	使用IP地址直接调用API，需要在请求消息中添加Header参数“host”。

- **{Path}**：请求路径，需替换为**获取API的调用信息**中获取的请求路径。
- **{Query}**：查询参数，可选，格式为“参数名=参数取值”，例如limit=10，多个查询参数之间使用“&”隔开。需根据**获取API的调用信息**中获取的请求参数进行设置。

- **{Header}**：请求头参数，格式为“参数名: 参数取值”，例如Content-Type: application/json。需根据**获取API的调用信息**中获取的请求参数进行设置。
- **{Body}**：请求消息体，JSON格式。需根据**获取API的调用信息**中获取的请求体内容描述进行设置。

2. 为API请求添加认证信息。

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**使用APP认证调用API**。
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的调用信息**中获取到的AppCode。具体请参考**快速入门**。
IAM认证（Token认证）	先获取云服务平台的认证Token，然后在API请求中添加Header参数“X-Auth-Token”，参数值为认证Token，具体请参考**Token认证**。
IAM认证（AK/SK认证）	使用获取的SDK对API请求进行签名，具体请参考**AK/SK认证**。
自定义认证	根据自定义认证的定义，在API请求参数中携带相关认证信息进行认证。
无认证	无需认证，可直接调用API。

13.15.2 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

响应消息头	描述	说明
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

13.15.3 错误码

当调用API时，可能遇到如**表13-31**所示的错误码。如果遇到“APIGW”开头的错误码，请参见**API网关错误码**进行处理。

说明

- 通过APIG接口管理API，发生错误时，产生的错误码请参考**错误码**。
- 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 13-31 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、路径和创建的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

错误码	错误信息	HTTP状态码	语义	解决方案
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
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.0203	Backend timeout.	504	后端超时	增大超时时间或缩小后端的处理时间
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，具体请参见**IAM信息认证错误**

错误码	错误信息	HTTP状态码	语义	解决方案
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	APP签名认证时，做如下检查： ● 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**使用APP认证调用API**检查签名代码的问题。 APPCODE简易认证时，做如下检查：检查请求是否携带了X-Apig-AppCode头域
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
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

错误码	错误信息	HTTP状态码	语义	解决方案
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.0501	The app quota has been used up.	405	APP已经超出配额	扩大APP配额
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	无法获取管理租户	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
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。

错误码	错误信息	HTTP状态码	语义	解决方案
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

13.16 云审计服务支持的关键操作

13.16.1 云审计服务支持的 APIG 操作列表

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、审计、问题定位等常见应用场景时，那么需要先**开通云审计服务**。

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

查看关键操作列表

通过云审计服务，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。

表 13-32 云审计服务支持的 API Gateway 操作列表

操作名称	资源类型	事件名称
创建API分组	ApiGroup	createApiGroup
删除API分组	ApiGroup	deleteApiGroup
更新API分组	ApiGroup	updateApiGroup
绑定域名	ApiGroup	createDomainBinding
修改安全传输协议	ApiGroup	modifySecureTransmission
解绑域名	ApiGroup	relieveDomainBinding
添加域名证书	ApiGroup	addDomainCertificate
删除域名证书	ApiGroup	deleteDomainCertificate
创建API	Api	createApi
删除API	Api	deleteApi
批量删除API	Api	batchDeleteApi
更新API	Api	updateApi
发布API	Api	publishApi
下线API	Api	offlineApi
批量发布/下线API	Api	batchPublishOrOfflineApi
切换API版本	Api	switchApiVersion
根据版本号下线API	Api	offlineApiByVersion
调试API	Api	debugApi
创建环境	Environment	createEnvironment
删除环境	Environment	deleteEnvironment
更新环境	Environment	updateEnvironment
创建环境变量	EnvVariable	createEnvVariable
更新环境变量	EnvVariable	updateEnvVariable
删除环境变量	EnvVariable	deleteEnvVariable
创建应用	App	createApp
删除应用	App	deleteApp
更新应用	App	updateApp
重置签名密钥	App	resetAppSecret
客户端绑定API	AppAuth	grantAuth

操作名称	资源类型	事件名称
客户端解绑API	AppAuth	relieveAuth
创建签名密钥	Signature	createSignature
删除签名密钥	Signature	deleteSignature
更新签名密钥	Signature	updateSignature
绑定签名密钥	SignatureBinding	createSignatureBinding
解绑签名密钥	SignatureBinding	relieveSignatureBinding
创建访问控制	Acl	createAcl
删除访问控制	Acl	deleteAcl
批量删除访问控制	Acl	batchDeleteAcl
更新访问控制	Acl	updateAcl
增加流控黑名单	Acl	addAclValue
删除流控黑名单	Acl	deleteAclValue
API绑定访问控制	AclBinding	createAclBinding
API解绑访问控制	AclBinding	relieveAclBinding
批量解绑访问控制	AclBinding	batchRelieveAclBinding
创建流控	Throttle	createThrottle
删除流控	Throttle	deleteThrottle
批量删除流控	Throttle	batchDeleteThrottle
更新流控	Throttle	updateThrottle
绑定流控	ThrottleBinding	createThrottleBinding
解绑流控	ThrottleBinding	relieveThrottleBinding
批量解绑流控	ThrottleBinding	batchRelieveThrottleBinding
创建特殊流控	ThrottleSpecial	createSpecialThrottle
删除特殊流控	ThrottleSpecial	deleteSpecialThrottle
更新特殊流控	ThrottleSpecial	updateSpecialThrottle
创建负载通道	Vpc	createVpc
删除负载通道	Vpc	deleteVpc
更新负载通道	Vpc	updateVpc
增加负载通道成员	Vpc	addVpcMember

操作名称	资源类型	事件名称
删除负载通道成员	Vpc	deleteVpcMember
导出单个API	Swagger	swaggerExportApi
批量导出API	Swagger	swaggerExportApiList
导出分组下所有API	Swagger	swaggerExportApiByGroup
导入API到新分组	Swagger	swaggerImportApiToNewGroup
导入API到已有分组	Swagger	swaggerImportApiToExistGroup
导出全部自定义后端	Swagger	SwaggerExportLdApi
导入自定义后端	Swagger	SwaggerImportLdApi
创建自定义认证	Authorizer	createAuthorizer
删除自定义认证	Authorizer	deleteAuthorizer
更新自定义认证	Authorizer	updateAuthorizer

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**删除追踪器**。

13.16.2 在 CTS 事件列表查看云审计事件

操作场景

用户进入云审计服务创建管理类追踪器后，系统开始记录云服务资源的操作。在创建数据类追踪器后，系统开始记录用户对OBS桶中数据的操作。云审计服务管理控制台会保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

- **在新版事件列表查看审计事件**
- **在旧版事件列表查看审计事件**

使用限制

- 单账号跟踪的事件可以通过云审计控制台查询。多账号的事件只能在账号自己的事件列表页面去查看，或者到组织追踪器配置的OBS桶中查看，也可以到组织追踪器配置的CTS/system日志流下面去查看。
- 用户通过云审计控制台只能查询最近7天的操作记录。如果需要查询超过7天的操作记录，您必须配置转储到对象存储服务(OBS)或云日志服务(LTS)，才可在OBS桶或LTS日志组里面查看历史事件信息。否则，您将无法追溯7天以前的操作记录。

- 云上操作后，1分钟内可以通过云审计控制台查询管理类事件操作记录，5分钟后才可通过云审计控制台查询数据类事件操作记录。
- 云审计控制台对用户的操作事件日志保留7天，过期自动删除，不支持人工删除。

在新版事件列表查看审计事件

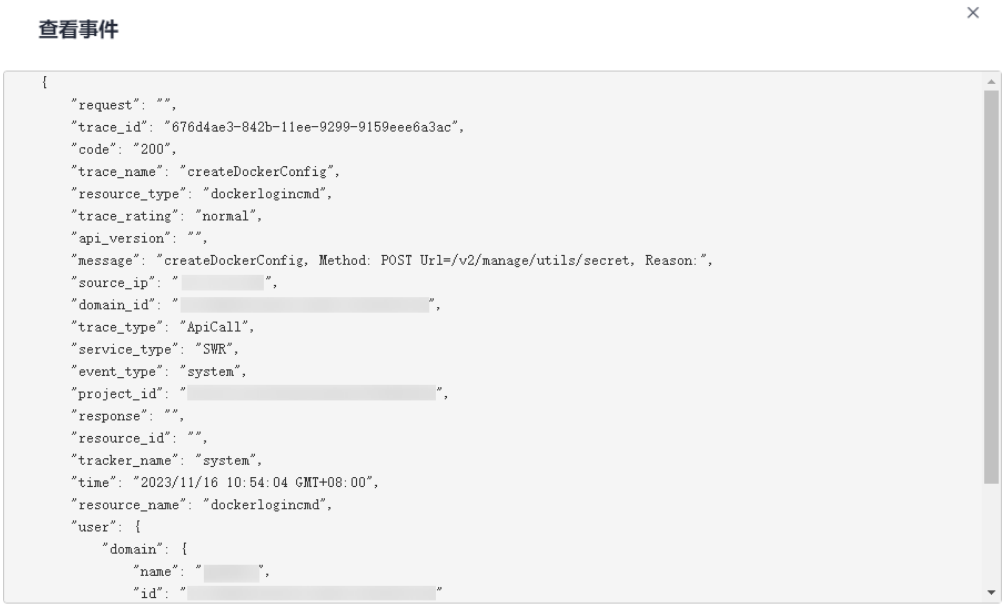
1. 登录管理控制台。
2. 单击左上角  ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 事件列表支持通过高级搜索来查询对应的操作事件，您可以在筛选器组合一个或多个筛选条件：
   - 事件名称：输入事件的名称。
   - 事件ID：输入事件ID。
   - 资源名称：输入资源的名称，当该事件所涉及的云资源无资源名称或对应的API接口操作不涉及资源名称参数时，该字段为空。
   - 资源ID：输入资源ID，当该资源类型无资源ID或资源创建失败时，该字段为空。
   - 云服务：在下拉框中选择对应的云服务名称。
   - 资源类型：在下拉框中选择对应的资源类型。
   - 操作用户：在下拉框中选择一个或多个具体的操作用户。
   - 事件级别：可选项为“normal”、“warning”、“incident”，只可选择其中一项。
     - normal：表示操作成功。
     - warning：表示操作失败。
     - incident：表示比操作失败更严重的情况，例如引起其他故障等。
   - 企业项目ID：输入企业项目ID。
   - 访问密钥ID：输入访问密钥ID（包含临时访问凭证和永久访问密钥）。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
5. 在事件列表页面，您还可以导出操作记录文件、刷新列表、设置列表展示信息等。
   - 在搜索框中输入任意关键字，按下Enter键，可以在事件列表搜索符合条件的数据。
   - 单击“导出”按钮，云审计服务会将查询结果以.xlsx格式的表格文件导出，该.xlsx文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击  按钮，可以获取到事件操作记录的最新信息。
   - 单击  按钮，可以自定义事件列表的展示信息。启用表格内容折行开关  ，可让表格内容自动折行，禁用此功能将会截断文本，默认停用此开关。
6. 关于事件结构的关键字段详解，请参见**事件结构**和**事件样例**。

7. （可选）在新版事件列表页面，单击右上方的“返回旧版”按钮，可切换至旧版事件列表页面。

在旧版事件列表查看审计事件

1. 登录管理控制台。
2. 单击左上角 ，选择“管理与监管 > 云审计服务 CTS”，进入云审计服务页面。
3. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
4. 用户每次登录云审计控制台时，控制台默认显示新版事件列表，单击页面右上方的“返回旧版”按钮，切换至旧版事件列表页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持四个维度的组合查询，详细信息如下：
   - 事件类型、事件来源、资源类型和筛选类型，在下拉框中选择查询条件。
     - 筛选类型按资源ID筛选时，还需手动输入某个具体的资源ID。
     - 筛选类型按事件名称筛选时，还需选择某个具体的事件名称。
     - 筛选类型按资源名称筛选时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询最近1小时、最近1天、最近1周的操作事件，也可以自定义最近7天内任意时间段的操作事件。
6. 选择完查询条件后，单击“查询”。
7. 在事件列表页面，您还可以导出操作记录文件和刷新列表。
   - 单击“导出”按钮，云审计服务会将查询结果以CSV格式的表格文件导出，该CSV文件包含了本次查询结果的所有事件，且最多导出5000条信息。
   - 单击 按钮，可以获取到事件操作记录的最新信息。
8. 在需要查看的事件左侧，单击 展开该记录的详细信息。

9. 在需要查看的记录右侧，单击“查看事件”，会弹出一个窗口显示该操作事件结构的详细信息。



10. 关于事件结构的关键字段详解，请参见《云审计服务用户指南》中的**事件结构**和**事件样例**。
11. （可选）在旧版事件列表页面，单击右上方的“体验新版”按钮，可切换至新版事件列表页面。

