



**API 网关**

**最佳实践**

发布日期 2023-04-30

---

# 目录

---

<b>1 使用 API 网关开放云容器引擎的工作负载.....</b>	<b>1</b>
<b>2 使用专享版 API 网关开放本地数据中心的服务能力.....</b>	<b>11</b>
<b>3 使用函数服务开发自定义认证.....</b>	<b>14</b>
<b>4 API 网关跨 VPC 开放后端服务.....</b>	<b>18</b>
4.1 方案概述.....	18
4.2 资源规划.....	19
4.3 操作流程.....	19
4.4 实施步骤.....	20
<b>5 对接 Web 应用防火墙 WAF.....</b>	<b>30</b>
<b>6 API 网关流量控制 2.0 策略.....</b>	<b>34</b>
6.1 方案概述.....	34
6.2 操作流程.....	35
6.3 实施步骤.....	36
<b>7 API 网关双重认证.....</b>	<b>39</b>
7.1 方案概述.....	39
7.2 操作流程.....	40
7.3 实施步骤.....	40
<b>8 修订记录.....</b>	<b>45</b>

# 1 使用 API 网关开放云容器引擎的工作负载

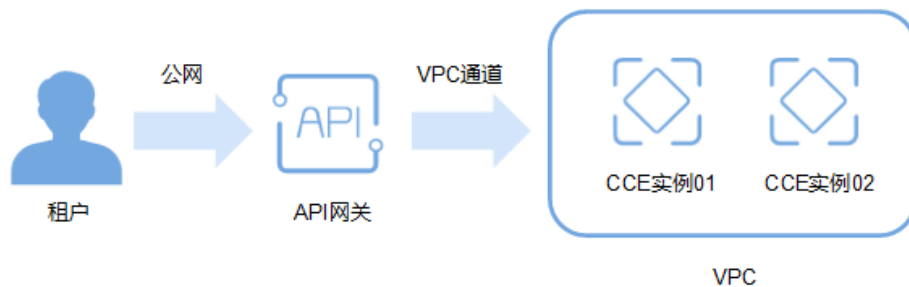
## 简介

云容器引擎（Cloud Container Engine，即CCE）中的工作负载，以及微服务，可通过API网关将服务能力以API形式对外开放。借助API网关开放容器应用，具有如下优势：

- 无需设置弹性公网IP，节省网络带宽成本  
API网关支持建立VPC通道，访问CCE中工作负载的地址。
- 提供多种认证方式，增加访问安全性
- 提供访问流量控制策略，增加后端服务的安全性  
与直接访问容器应用相比，API网关提供流量控制，确保后端服务稳定运行。
- 支持多实例负载均衡，合理利用资源，增加系统可靠性

本手册介绍如何通过API网关访问CCE中的工作负载。

图 1-1 通过 API 网关访问 CCE 工作负载（由实例组成）



## 准备 CCE 工作负载信息

在通过API网关将容器的工作负载对外开放前，需要在CCE服务控制台创建好集群和工作负载，并在工作负载中添加实例和容器，具体操作步骤请参见《云容器引擎用户指南》。

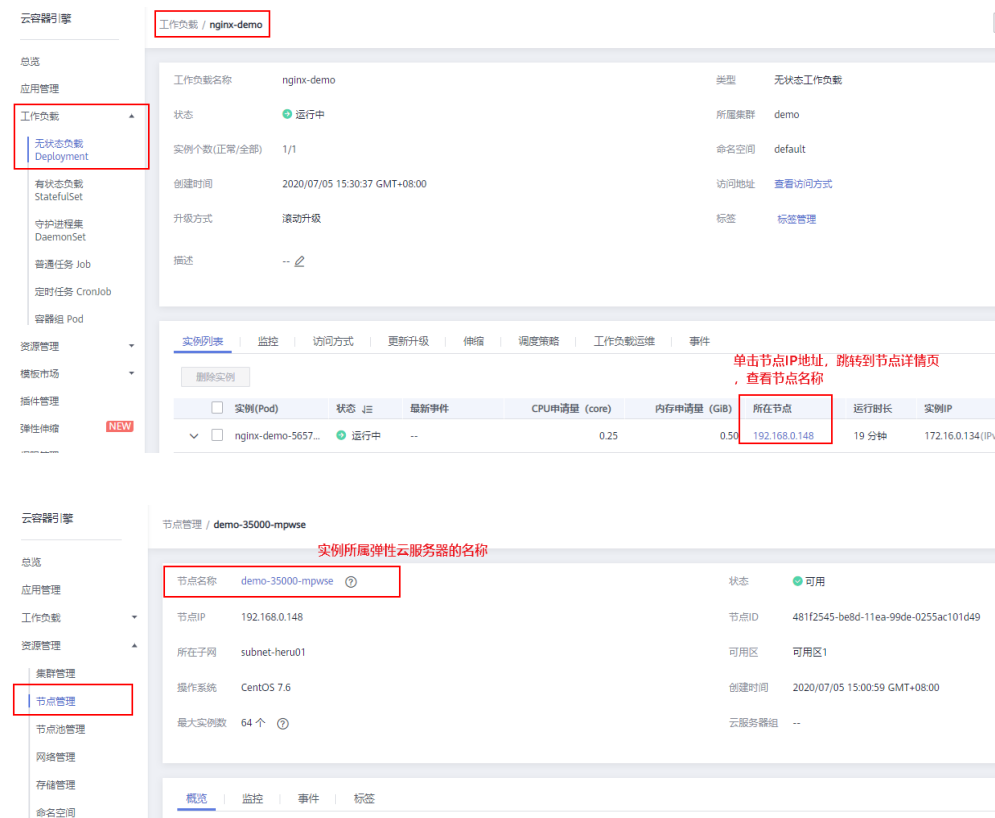
您需要在CCE控制台获取如下图所示信息，注意工作负载的访问方式，需配置为“节点访问”或“负载均衡”，具体操作步骤请参见“节点访问”或“负载均衡”章节。

- 获取“节点访问”方式的访问信息：

图 1-2 查询访问端口



图 1-3 查询工作负载中实例所属弹性服务器的名称



- 获取“负载均衡”方式的访问信息：



## 创建 VPC 通道

如果CCE工作负载的访问方式为“负载均衡”，请跳过该步骤，执行[开放API](#)。

**步骤1** 登录控制台，进入API网关服务。

**步骤2** 创建VPC通道。

1. 在“创建VPC通道”的“基本信息”界面，单击“创建快速通道”。

图 1-4 VPC 通道列表界面



2. 输入如下图所示信息，其他参数保持默认值。  
如果您想了解参数更详细的信息，请参见《API网关用户指南》。

图 1-5 设置 VPC 通道基本信息



**步骤3** 添加需要通过API网关访问的CCE工作负载的实例节点。

可添加多个实例，API网关支持负载均衡功能。



**步骤4** 单击“完成”，添加VPC通道。



----结束

## 开放 API

**步骤1** 创建分组，输入如图1-6所示信息。

图 1-6 创建分组



**步骤2 创建API。**

如果您想了解参数更详细的信息，请参见《API网关用户指南》。

1. 单击“新建API”，操作如下图所示。

图 1-7 API 列表



2. 在“新建API”的“基本信息”界面，输入如下图所示信息。

图 1-8 设置 API 的基本信息



3. 在“定义API请求”界面，输入如下图所示信息。

新建API

1 基本信息 2 定义API请求 3 定义后端服务 4 定义返回结果

定义API请求

域名 5e3e17a8edfd4d488dd3a159975e9eff...

请求协议 HTTP HTTPS HTTP&HTTPS

支持WebSocket

\* 请求Path /

请求Path可以包含请求参数,用{}标识,比如/getUserInfo/{userId},支持\*%+.\_-等特殊字符。

匹配模式 绝对匹配 前缀匹配

路径前缀匹配,如配置的是/a,则访问/a/开头的URL都匹配到该API

\* Method GET

支持跨域(CORS)

开启跨域,请前往了解详情

入参定义

4. 在“定义后端服务”界面，输入如下图所示信息。

如果CCE工作负载的访问方式为“节点访问”，则选择“使用”VPC通道，选择**已创建的VPC通道**；如果为“负载均衡”，则选择“不使用”VPC通道，输入负载均衡的**访问地址和端口**。此处以“节点访问”方式为例。

定义后端服务

后端服务类型 HTTP/HTTPS FunctionGraph Mock

您可以添加策略后端来差异化后端定义。每个策略后端允许定义多个策略条件，只有满足相应的策略条件的请求才会被转发到该策略后端。  
您还能创建5个后端策略

默认后端 + 添加策略后端

基础定义

协议 HTTP

请求方式 GET

使用VPC通道 使用 不使用

使用VPC通道访问您部署在VPC内的服务

\* VPC通道 apig-cce 管理VPC通道

自定义host头域

在请求被转发到VPC通道中的云服务商前，允许您自定义请求的Host头域。默认将使用请求中原有的Host头域。

\* 后端请求Path /

请求Path可以包含请求参数,用{}标识,比如/getUserInfo/{userId},支持\*%+.\_-等特殊字符。

\* 后端超时(ms) 5000

5. 在“返回结果基础定义”界面，输入“成功响应示例”，在本示例中，输入内容仅供参考，无实际作用。





6. 单击“完成”，完成API的创建。

### 步骤3 调试API。

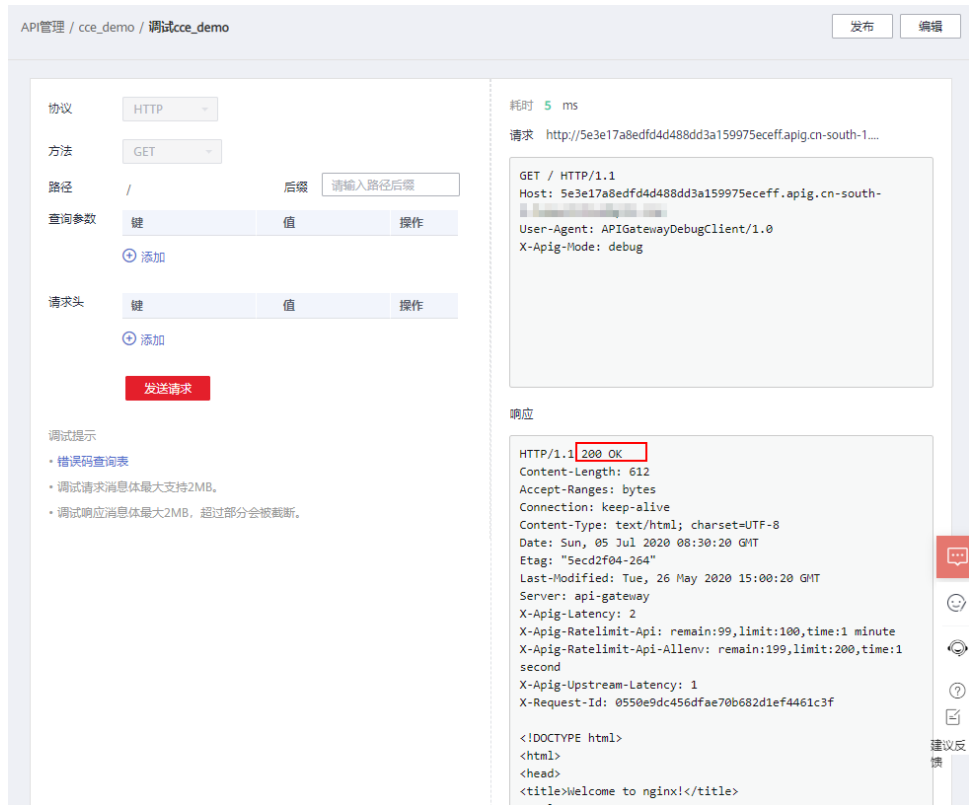
1. 单击“调试”，操作如下图所示。

图 1-9 API 列表界面



2. 调试API，操作如下图所示。

图 1-10 调试 API，返回 200，表示调用成功



步骤4 发布API。

1. 单击“发布”。

图 1-11 列表界面



2. 设置发布信息。

图 1-12 发布 API



----结束

## 调用 API

**步骤1** 在API详情界面，复制“API URL”。

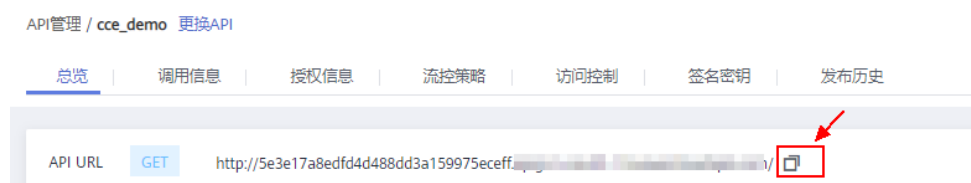
1. 进入API详情界面。

图 1-13 进入 API 详情界面



2. 在API详情界面，复制“API URL”。

图 1-14 复制 API URL



**步骤2** 打开浏览器，在地址栏粘贴“API URL”的地址。请求API成功时，显示如下界面。

如果想要设置一段时长内API的调用次数，请设置流控策略，具体参见《API网关用户指南》。

← → ↻ ① 不安全 | 5e3e17a8edfd4d488dd3a159975e9eff

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](https://nginx.org).  
Commercial support is available at [nginx.com](https://nginx.com).

*Thank you for using nginx.*

----结束

# 2 使用专享版 API 网关开放本地数据中心的服务能力

API网关的后端服务有3类部署形态：

- 后端服务部署在虚拟私有云（以下简称VPC）中，仅支持私有地址访问。  
可在API网关创建VPC通道，利用VPC通道，打通API网关与虚拟私有云的网络路由。
- 后端服务部署在公网环境中，即可以直接通过公网地址访问。
- 后端服务部署在本地数据中心，且不能通过公网地址直接访问。

如果您使用专享版API网关，可为本地数据中心搭建一条与API网关之间的专线。

本节针对后端服务部署在本地数据中心的场景，介绍使用API网关开放API的注意事项。

## 连通云专线与 API 网关

**步骤1** 创建VPC。

具体请参考《虚拟私有云用户指南》中的“创建虚拟私有云和子网”章节。

专享版API网关需要绑定1个VPC，将本地数据中心与VPC之间建立云专线后，API网关即可访问本地数据中心的服务。

图 2-1 创建 VPC 示例参考

**基本信息**

区域  不同区域的资源之间网不互通。请选择靠近您客户的区域，可以降低网络时延，提高访问速度。

名称

IPv4网段  建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

**⚠ 该VPC网段 (192.168.0.0/16) 与当前区域下其他VPC网段重叠，如需使用VPC互通服务，建议您修改VPC网段。查看区域下已有vpc网段**

企业项目  [新建企业项目](#) [?](#)

---

高级配置 [标签](#) | [描述](#)

---

**默认子网**

可用区  [?](#)

名称

子网IPv4网段  [?](#) 可用IP数: 251 子网创建完成后，子网网段无法修改

子网IPv6网段  开启IPv6 [?](#)

关联路由表  [?](#)

---

高级配置 [网关](#) | [DNS服务器地址](#) | [DHCP租约时间](#) | [标签](#) | [描述](#)

### 📖 说明

- 需要为API网关规划1个子网段。
- 一条云专线只能打通本地数据中心到1个VPC的网络，您在云上的资源，建议都绑定到同一VPC中，避免不同VPC都需要使用云专线访问本地数据中心带来的成本增加。
- 如果已有VPC，可不用新建。

### 步骤2 购买专享版API网关。

具体请参考《API网关用户指南》的“购买实例”章节。

### 步骤3 请参考《云专线用户指南》，开通云专线。

#### 1. 接入物理连接。

请向您的专属客户经理提交物理连接的开通申请，如果没有专属客户经理请联系技术支持。

#### 2. 创建虚拟网关。

虚拟网关用于关联专享版API网关绑定的VPC。

### 📖 说明

在选择VPC网段时，需要添加专享版API网关所使用的网段，表示允许专线可访问的VPC子网。可在专享版API网关控制台查询网段详情。

#### 3. 创建虚拟接口。

虚拟接口将物理连接与虚拟网关（配置了VPC和网段）关联绑定，打通物理与专享版API网关所在VPC的网络。

注意远端网关与远端子网要分别配置您本地数据中心的开放API接口访问的网关和子网。例如您本地数据中心的API调用地址为`http://192.168.0.25:80/{URI}`，则远端网关和远端子网要配置192.168.0.25所在的子网段与网关。

#### 步骤4 验证网络连通。

再创建一台按需的ECS，选择与专享版API网关相同的VPC、子网与安全组。只要本地数据中心能连通ECS，则与专享版API网关也能连通。

----结束

## 使用专享版 API 网关开放 API

本地数据中心与专享版API网关的网络连通后，您可以正常使用API网关的所有操作。具体请参考《API网关用户指南》的“快速入门 > 开放API”章节。

注意，API的后端服务地址填写您本地数据中心的API调用地址。

# 3 使用函数服务开发自定义认证

## 简介

在API的安全认证方面，API网关提供IAM认证、APP认证等方式，帮助用户快速开放API，同时API网关也支持用户使用自己的认证方式（以下简称自定义认证），以便更好地兼容已有业务能力。

API网关支持的自定义认证需要借助函数 workflow 服务实现，用户在函数 workflow 中创建自定义认证函数，API网关调用该函数，实现自定义认证。下面以Basic认证为例，介绍如何使用函数服务实现自定义认证。

## 编写自定义认证函数

在函数 workflow 的控制台编写函数，自定义认证的代码编写指南参见“开发指南 > 创建用于前端自定义认证的函数”。

在函数 workflow 页面创建一个函数，语言选Python 3.6。

表 3-1 函数信息配置

参数	配置说明
函数类型	默认“事件函数”。
区域	与API网关相同区域。
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。
委托名称	用户委托函数 workflow 去访问其他的云服务。此处选择“未使用任何委托”。
企业项目	默认“default”。
运行时	选择Python 3.6。

在“代码”页签，将以下代码复制到index.py中。

```
# -*- coding:utf-8 -*-  
import json
```



```
def handler(event, context):
#以下表示认证信息匹配正确，则返回用户名，
    if event["headers"]["authorization"]=="Basic dXNlcjE6cGFzc3dvcnQ=:
        return {
            'statusCode': 200,
            'body': json.dumps({
                "status": "allow",
                "context": {
                    "user_name": "user1"
                }
            })
        }
    else:
        return {
            'statusCode': 200,
            'body': json.dumps({
                "status": "deny",
                "context": {
                    "code": "1001",
                    "message": "incorrect username or password"
                }
            })
        }
}
```

## 创建自定义认证

在API网关页面，创建自定义认证，类型选择前端，函数地址选择上一步创建的函数。



## 创建自定义认证的 API

创建API，具体步骤请参见《API网关用户指南》中的“创建API”章节。将“安全认证”修改为“自定义认证”，并选择上一步创建的自定义认证。编辑完成之后发布API。

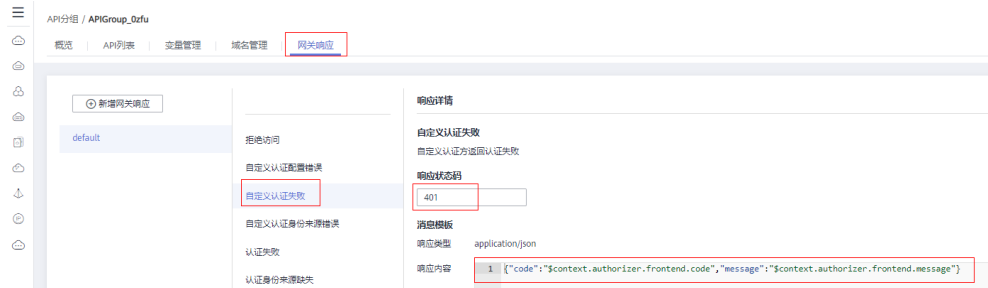
## 设置错误响应

调用API如果输入错误的认证信息，则返回结果如下：

```
{"error_msg": "Incorrect authentication information: frontend authorizer", "error_code": "APIG.0305", "request_id": "36e42b3019077c2b720b6fc847733ce9"}
```

为了让API响应结果为函数中返回的context中的字段，需要修改网关响应模板。在API所在的分组中，“分组信息”页签下的“网关响应”区域，编辑自定义认证失败的响应详情，将响应状态码改为401，将消息模板改为：

```
{"code":"$context.authorizer.frontend.code","message":"$context.authorizer.frontend.message"}
```



修改之后，调用API传入错误的认证信息，返回状态码为401，返回结果如下：

```
{\"code\":\"1001\",\"message\":\"incorrect username or password\"}
```

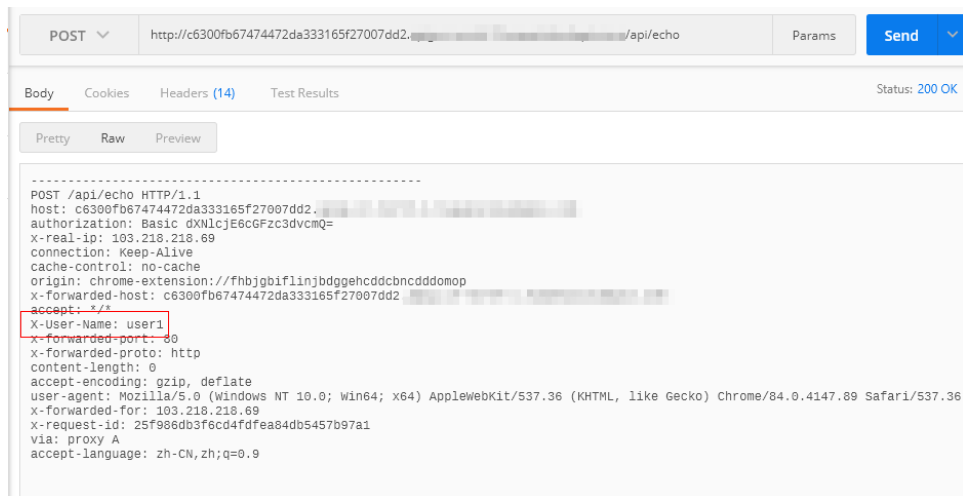
## 映射后端参数

如果认证通过，函数返回的context信息，可以传到后端，配置方式如下：

编辑API，在后端服务页面，添加系统参数，参数类型为前端认证参数，系统参数名称填自定义认证函数中context中的字段，后端参数名称和位置填需要传入到后端请求的参数名和位置。



编辑和发布完成之后，使用正确的认证信息调用API，可以看到后端打印了X-User-Name头，值为函数代码中写入到context中的user\_name字段的用户名。



# 4 API 网关跨 VPC 开放后端服务

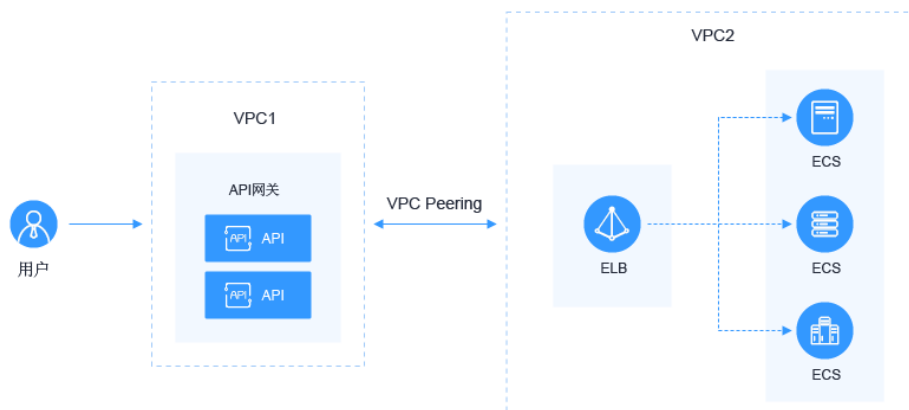
## 4.1 方案概述

### 应用场景

当用户后端服务器所在的VPC与创建实例所选择的VPC处于不同的场景时，该如何完成服务配置，以实现跨VPC对接？本文以Elastic Load Balance（弹性负载均衡ELB）为例，讲述如何在API网关上开放内网ELB中的服务。

### 方案架构

图 4-1 API 网关跨 VPC 开放后端服务



### 方案优势

帮助用户根据业务诉求进行灵活配置，无需修改原有业务网络架构，直接将请求转发到后端服务上。

### 约束与限制

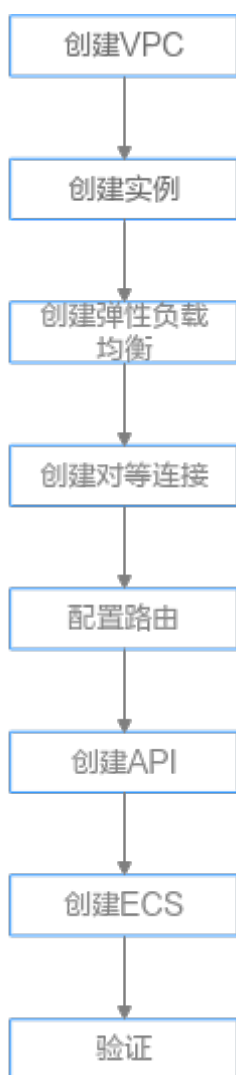
VPC1、VPC2、APIG实例系统VPC网段不能重叠。关于APIG实例VPC网段规划，请参考表4-3。

## 4.2 资源规划

表 4-1 资源规划

资源	数量 (个)
VPC	2
API专享版实例	1
ELB	1
ECS	1

## 4.3 操作流程



1. **创建VPC**  
创建两个VPC，VPC1为API网关所在VPC，VPC2为后端应用所在VPC。
2. **创建实例**  
在VPC1上创建API专享版实例。
3. **创建弹性负载均衡**  
在VPC2上创建弹性负载均衡。
4. **创建对等连接**  
创建VPC Peering对等连接，打通VPC1和VPC2。
5. **配置路由**  
在API专享版实例上配置路由，配置IP为创建ELB所在VPC2网段。
6. **创建API**  
创建API，后端服务地址配置ELB的IP。
7. **创建ECS**  
选择VPC2为其VPC，并在其上部署后端应用服务，创建Elastic Cloud Server（应用服务器）。
8. **调试API**  
验证对接内网ELB是否成功。

## 4.4 实施步骤

### 创建 VPC

- 步骤1** 登录网络控制台。
- 步骤2** 在左侧导航栏选择“虚拟私有云 > 我的VPC”。
- 步骤3** 在“虚拟私有云”页面，单击“创建虚拟私有云”，请参考表4-2和表4-3配置信息。具体操作请参考《虚拟私有云服务用户指南》中的“创建虚拟私有云和子网”章节。

**基本信息**

区域: [选择区域] 不同区域的云产品之间内网互不相通; 请就近选择靠近您业务的区域, 可减少网络时延, 提高访问速度。

名称: VPC1

IPv4网段: 192.168.0.0 / 16 建议使用网段: 10.0.0.0/8-24 (选择) 172.16.0.0/12-24 (选择) 192.168.0.0/16-24 (选择)

**⚠️ 该VPC网段 (192.168.0.0/16) 与当前区域下其他VPC网段重叠, 如需使用VPC互通服务, 建议您修改VPC网段, 查看区域下已有vpc网段**

企业项目: default [新建企业项目](#)

---

高级配置: 标签 | 描述

---

**默认子网**

名称: subnet-bf15

子网IPv4网段: 192.168.0.0 / 24 可用IP数: 251  
子网创建完成后, 子网网段无法修改

子网IPv6网段:  开启IPv6

关联路由表: 默认

---

高级配置: 网关 | DNS服务器地址 | DHCP租约时间 | 标签 | 描述

[添加子网](#)

表 4-2 配置信息

参数	配置说明
区域	选择所在的区域。
名称	VPC1 (API网关所在VPC)。
企业项目	选择所属的企业项目, 此处选择“default”。
名称	创建虚拟私有云的同时创建一个默认子网。

表 4-3 VPC 网段规划

VPC1	APIG实例系统VPC	VPC2
10.X	172.31.0.0/16	不能与VPC1和APIG实例系统VPC重复。
172.X	192.168.0.0/16	
192.X	172.31.0.0/16	

**步骤4** 单击“立即创建”。

**步骤5** 重复**步骤3~步骤4**, 创建“VPC2 (后端应用所在VPC)”。

----结束

## 创建实例

- 步骤1** 登录API网关控制台。
- 步骤2** 在左侧导航栏选择“实例管理”。
- 步骤3** 单击“购买实例”。

The screenshot shows the 'Create Instance' page in the API Gateway console. The configuration is as follows:

- 区域 (Region):** 华北-北京
- 可用区 (Availability Zone):** 可用区1
- 实例名称 (Instance Name):** apig01
- 实例规格 (Instance Specification):** 专业版 (Professional Edition)
- 可维护时间窗 (Maintenance Window):** 22:00:00 -- 02:00:00
- 企业项目 (Enterprise Project):** default
- 公网入口 (Public Network In):**  开通公网入口
- 公网出口 (Public Network Out):**  开通公网出口
- 网络 (Network):** VPC1 (Virtual Private Cloud) and subnet-01 (Subnet)
- 安全组 (Security Group):** sg-01 (Security Group)
- 描述 (Description):** (Empty text box)

表 4-4 实例信息

参数	配置说明
区域	选择实例所在的区域，且与VPC1同区域。
可用区	选择实例所在的可用区，此处选择“可用区1”。
实例名称	填写实例的名称，根据规划自定义。建议您按照一定的命名规则填写实例名称，方便您快速识别和查找。
实例规格	选择实例的容量规格，实例创建后规格不可修改，此处选择“专业版”。
可维护时间窗	选择技术支持对实例进行维护的时间段，建议选择业务量较少的时间段，保持默认设置“22:00:00---02:00:00”。
企业项目	选择实例所属的企业项目，保持默认设置“default”。
网络	选择已创建的虚拟私有云“VPC1”和子网。
安全组	单击“管理安全组”，创建安全组，企业项目选择“default”后，即可创建。
描述	填写实例的描述信息。



**步骤4** 单击“立即购买”。

**步骤5** 规格确认无误后，单击“去支付”，实例开始创建，界面显示创建进度。

----结束

## 创建 ELB

**步骤1** 登录网络控制台。

**步骤2** 在左侧导航栏选择“弹性负载均衡 > 负载均衡器”。

**步骤3** 单击“创建弹性负载均衡”。

**步骤4** 配置负载均衡信息。具体操作请参考《弹性负载均衡用户指南》中的“负载均衡”章节。

**基础配置**

\* 实例类型: 独享型

\* 区域: 不同区域的云服务产品之间内网互不相通，请就近选择靠近业务的区域，可减少网络时延，提高访问速度。

\* 可用区: 负载均衡实例同时部署在多个可用区，多可用模式且互为备份，可提供更高的可用性。

**网络配置**

\* 跨VPC后端:

网络类型:  IPv4 公网(支持公网流量请求)  IPv4 私网(仅支持内网请求)  IPv6(支持IPv6公网、私网请求)

\* 所属VPC: VPC2 [查看虚拟私有云](#)

\* 子网: subnet-Q2 (192.168.0.0/24) [查看子网](#)  
可用私有IP数量: 243个

\* IPv4地址: 自动分配IPv4地址

\* 规格: 实例规格决定了负载均衡可创建的监听器类型，可根据业务特点选择规格类型，根据业务量选择规格大小。

规格	新建连接数 (CPS)	最大连接数	带宽 (Mbit/s)	LCU
<input checked="" type="radio"/> 小型 I	10,000	500,000	50	10
<input type="radio"/> 小型 II	20,000	1,000,000	100	20
<input type="radio"/> 中型 I	40,000	2,000,000	200	40
<input type="radio"/> 中型 II	80,000	4,000,000	400	80
<input type="radio"/> 大型 I	200,000	10,000,000	1,000	200
<input type="radio"/> 大型 II	400,000	20,000,000	2,000	400

当前选择实例: 网络型(TCP/UDP) | 小型 I | elbv3.basic.1az | 10 LCU

\* 名称: elb-zly

\* 企业项目: default [新建企业项目](#)

高级配置 | 高级子网 | 描述 | 标签

表 4-5 弹性负载均衡参数

参数	配置说明
实例类型	选择实例的规格类型。
区域	选择实例所在的区域，且与VPC2同一区域。
可用区	选择实例所在的可用区，此处选择“可用区1”。

参数	配置说明
网络类型	选择网络类型“私网”。
所属VPC	所属虚拟私有云，选择已创建的虚拟私有云“VPC2”。
子网	选择子网。
规格	选择“网络型”。
名称	填写弹性负载均衡的名称，根据规划自定义。建议您按照一定的命名规则填写实例名称，方便您快速识别和查找。
企业项目	选择实例所属的企业项目，此处选择“default”。

**步骤5** 单击“立即申请”。

**步骤6** 确认信息无误后，单击“提交”。

**步骤7** 添加监听器。

1. 单击已创建弹性负载均衡的名称，在“监听器”页签中单击“添加监听器”。
2. 配置监听器名称、前端协议及端口，单击“下一步”。
3. 配置后端服务器组名称、后端协议和分配策略类型，单击“下一步”。
4. 添加后端服务器，单击“下一步”。
5. 单击“提交”。下图所示为配置后的信息。

图 4-2 监听器基本信息

基本信息	后端服务器组	标签	
名称	listener-http	ID	
前端协议/端口	TCP/80	后端服务器组	sg_server_http
访问控制	允许所有IP访问 设置	获取客户端IP	已开启
创建时间	2023/03/02 15:00:40 GMT+08:00	描述	-

图 4-3 后端服务器组信息

基本信息	后端服务器组	标签	
名称	sg_server_http	ID	
后端协议	TCP	分配策略类型	加权轮询算法
健康检查	已开启   配置	会话保持	未开启
IP类型	双栈		

---结束

## 创建对等连接

**步骤1** 登录网络控制台。

**步骤2** 在左侧导航栏选择“虚拟私有云 > 对等连接”。

**步骤3** 单击“创建对等连接”，配置对等连接。

表 4-6 对等连接配置

参数	配置说明
名称	填写对等连接的名称，根据规划自定义。建议您按照一定的命名规则填写实例名称，方便您快速识别和查找。
本端VPC	已创建的虚拟私有云“VPC1”。
帐户	此处默认“当前帐户”。
对端项目	选择已有项目。
对端VPC	已创建的虚拟私有云“VPC2”。

**步骤4** 单击“确定”。

**步骤5** 在弹框中单击“查看路由”，进入对等对接详情页面。

**步骤6** 在“本端路由”页签中单击“路由表”，添加路由。

- 在“路由”区域单击“添加路由”。
- 在弹窗中填写路由信息。
  - 目的地址：为ELB详情页面，“基本信息”页签中的“服务地址”。
  - 下一跳类型：选择“对等连接”。
- 单击“确定”。

图 4-4 本端路由

目的地址	下一跳类型	下一跳地址	路由表	描述
10.101.0.191/32	对等连接	peering-zjy(163a0a5f-9be0-4db0-9058-1c2fa5b627c)	rtb-vpc-001	...

**步骤7** 返回对等连接详情，在“对端路由”页签中单击“路由表”，添加路由。

- 在“路由”区域单击“添加路由”。
- 在弹窗中填写路由信息。
  - 目的地址：为API网关专享版实例概览页面，“基本信息”页签中的“出公网IP”地址。
  - 下一跳类型：选择“对等连接”。
- 单击“确定”。

图 4-5 对端路由

目的地址	下一跳类型	下一跳地址	路由表	描述
192.168.0.180/32	对等连接	peering-zjy(163a0a5f-9be0-4db0-9058-1c2fa5b627c)	rtb-vpc-002	...
192.168.0.239/32	对等连接	peering-zjy(163a0a5f-9be0-4db0-9058-1c2fa5b627c)	rtb-vpc-002	...

---结束

## 配置路由

- 步骤1 登录API网关控制台。
- 步骤2 在左侧导航栏选择“实例管理”。
- 步骤3 单击已创建**API网关专享版实例**的名称或“查看控制台”。
- 步骤4 在“路由”区域，单击“更改”配置路由，配置IP为创建ELB所在VPC2的网段。



- 步骤5 单击“保存”。

----结束

## 创建 API

- 步骤1 登录API网关控制台。
- 步骤2 在左侧导航栏上方选择已创建的实例。
- 步骤3 在左侧导航栏选择“API管理 > API列表”，单击“创建API”。
- 步骤4 配置前端信息后，单击“下一步”。

表 4-7 前端配置

参数	配置说明
API名称	填写API名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
所属分组	默认“DEFAULT”。
URL	请求方法：接口调用方式，此处选择“GET”。 请求协议：选择API请求协议，此处选择“HTTPS”。 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调试域名，此调试域名每天最多可以访问1000次。 路径：接口请求路径。
网关响应	API网关未能成功处理API请求，从而产生的错误响应。 默认的网关响应为“default”。

参数	配置说明
安全认证	选择API认证方式，此处选择“无认证”。

**步骤5** 配置后端信息后，单击“下一步”。

**表 4-8** HTTP/HTTPS 类型定义后端服务

参数	配置说明
负载通道	选择“不使用”负载通道访问后端服务。
URL	请求方法：接口调用方式，此处选择“GET”。 请求协议：选择协议类型，此处选择“HTTP”。 后端服务地址：填写创建ELB的服务地址。 路径：后端服务的路径。

**步骤6** 定义返回结果后，单击“完成”。

----结束

## 创建 ECS

**步骤1** 登录云服务器控制台。

**步骤2** 单击“创建弹性云服务器”。

**步骤3** 基础配置后，单击“下一步：网络配置”。

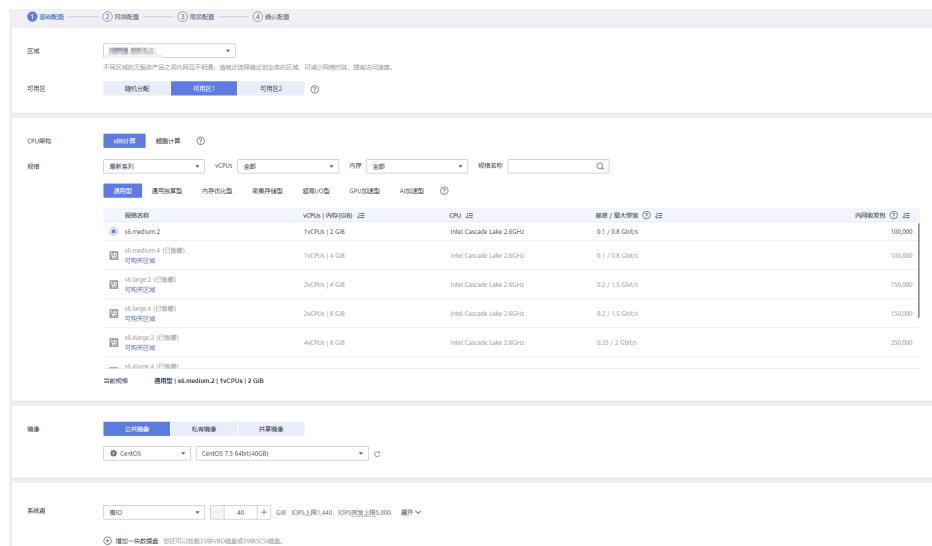


表 4-9 基础配置

参数	配置说明
区域	选择弹性云服务器所属区域，且与VPC2同一区域。
可用区	选择弹性云服务器所属可用区。
CPU架构	默认“x86计算”。
规格	根据业务规划，选择规格。
镜像	根据业务规划，选择镜像。

**步骤4** 网络配置后，单击“下一步：高级配置”。

表 4-10 网络配置

参数	配置说明
网络	选择已创建的虚拟私有云“VPC2”和子网。
安全组	选择专享版实例中已创建的安全组。
弹性公网IP	选择“暂不购买”。

**步骤5** 高级配置后，单击“下一步：确认配置”。

表 4-11 高级配置

参数	配置说明
云服务器名称	填写弹性云服务器名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
登录方式	登录云服务器凭证，此处默认“密码”。
用户名	默认“root”。
密码	填写登录云服务器的密码。
确认密码	保证密码正确性。

**步骤6** 确认配置信息后，选择企业项目，此处选择“default”。

**步骤7** 勾选协议声明后，单击“立即申请”。

----结束

## 调试 API

**步骤1** 在弹性负载均衡中的“后端服务器组”页签中，添加云服务器。



**步骤2** 进入弹性云服务器启动服务器。

**步骤3** 进入**专享版实例**中的“API管理 > API列表”页面，在**已创建API**所在行选择“更多 > 调试”。

**步骤4** 填写请求参数，单击“调试”。

状态码显示“200”表示调试成功。

----**结束**

# 5 对接 Web 应用防火墙 WAF

企业为了保护APIG及后端服务器免受恶意攻击，可在APIG和外部网络之间部署WAF。

图 5-1 后端服务器访问原理



## 方案一（推荐）：WAF 侧注册对外访问域名并配置证书，通过 APIG 实例的分组调试域名访问后端服务

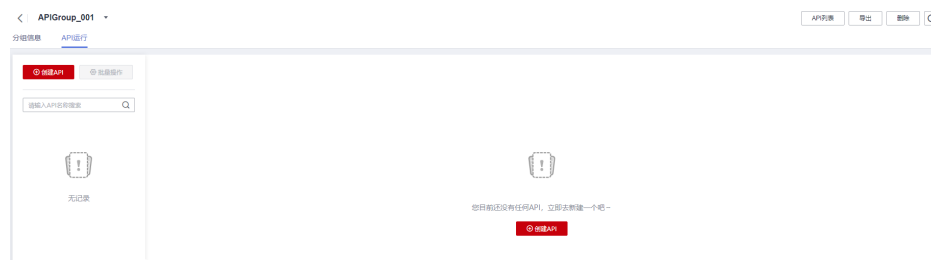
推荐原因：API分组通过域名方式对外提供服务，具备更强的可扩展性。

**步骤1** 在APIG实例中，新建API分组，并记录域名，将API添加在新建的分组中。

图 5-2 新建 API 分组并记录调试域名



图 5-3 新建 API

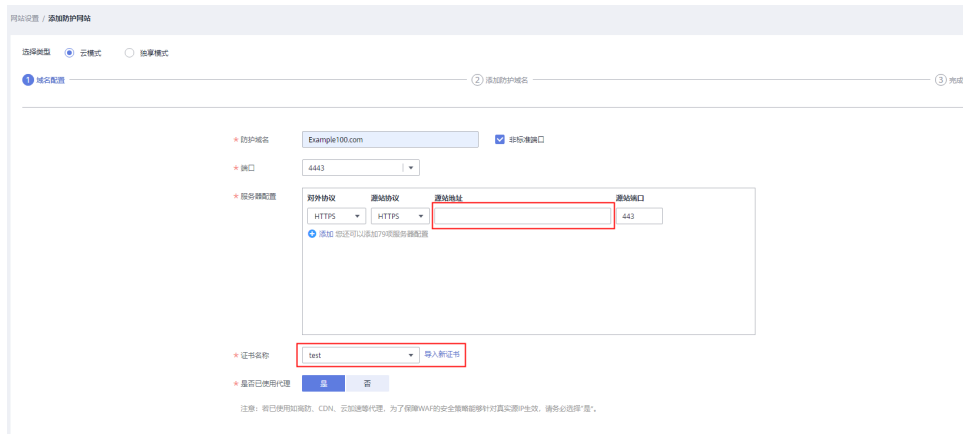


**步骤2** 在WAF侧添加防护域名时，配置“源站地址”填写为API分组的域名，并添加证书。详细操作步骤请参考《Web应用防火墙用户指南》中的“网站接入WAF（云模式）”。

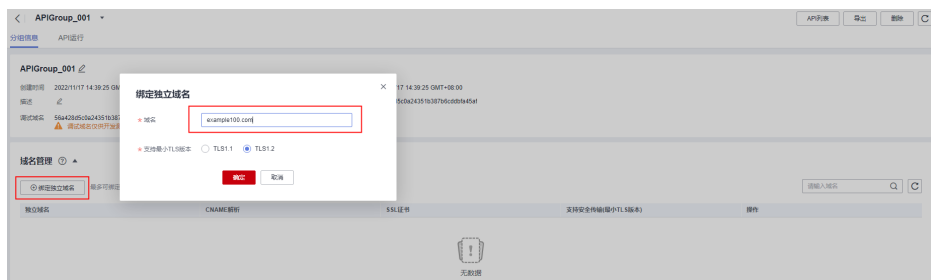


**说明**

客户从公网客户端访问WAF时，使用的是WAF对外访问域名，WAF转发给APIG时同样使用该对外访问域名，APIG收到访问该域名的请求无次数限制。



**步骤3** 在APIG实例中，为API分组绑定已创建的防护域名。



**步骤4** 在APIG实例中，将“real\_ip\_from\_xff”开关打开，并设置参数运行值为“1”。

**说明**

客户从公网客户端访问WAF时，WAF会在HTTP头部“X-Forwarded-For”中记录用户的真实IP，APIG需要据此解析出用户的真实IP。

参数	参数默认值	参数范围	参数运行值	更新时间	操作
request_body_size	12 MB	1-9,536 MB	12 MB	-	编辑
request_body_size	12 MB	1-9,536 MB	12 MB	-	编辑
backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	-	编辑
http_token	Off	On/Off	Off	-	编辑
http_basic	Off	On/Off	Off	-	编辑
http_redirect	Off	On/Off	Off	-	编辑
http_forward	Off	On/Off	Off	-	编辑
backend_client_certificate			Off	-	编辑
ssl_cipher	ECDHE-ECCGCM-AES256-GCM-SHA384:ECDHE-RSA-AE		ECDHE-ECCGCM-AES256-GCM-SHA384:ECCHE-RSA-AE	-	编辑
real_ip_from_xff	Off	On/Off	On	2022/11/17 14:57:29 GMT+08:00	编辑
xff_index	-1	HTTP头部位置	1	2022/11/17 14:57:29 GMT+08:00	编辑
vpc_name_modify	On	On/Off	On	2022/11/02 19:57:59 GMT+08:00	编辑

----结束

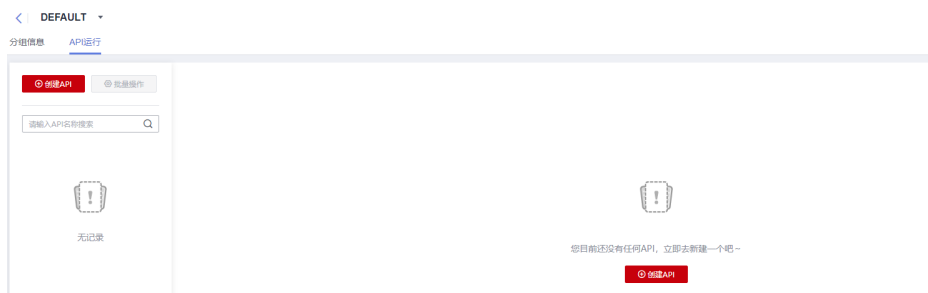
## 方案二（备选）：使用 DEFAULT 分组实现转发功能，WAF 侧通过 IP 访问后端服务

**步骤1** 在APIG实例中，查看入口地址。通过IP调用访问APIG实例，无访问次数限制。

- 虚拟私有云访问地址为VPC内网地址。
- 弹性IP地址为公网地址。



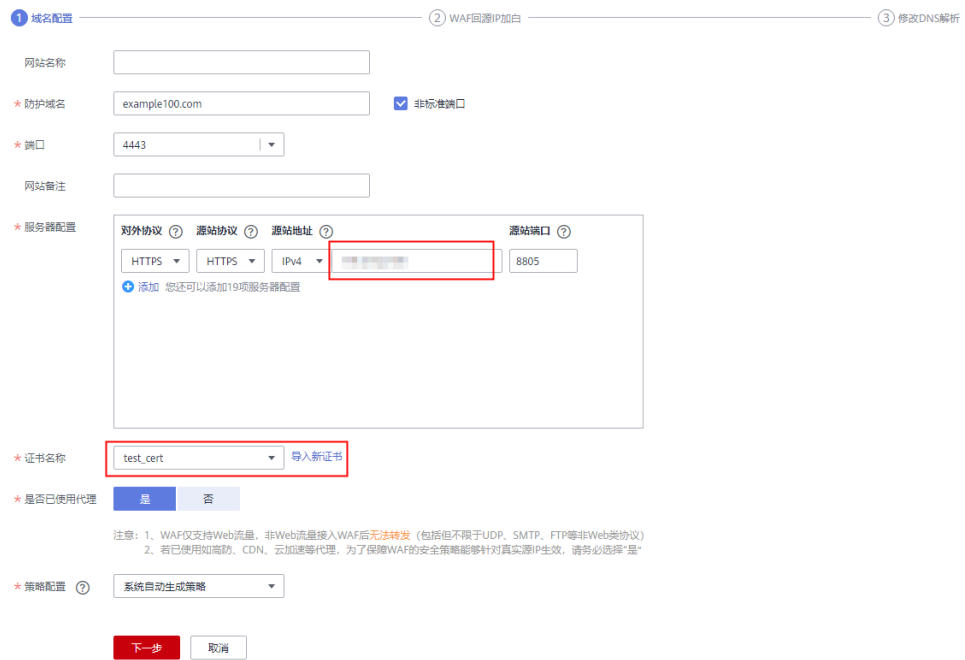
**步骤2** 在DEFAULT分组中添加API。



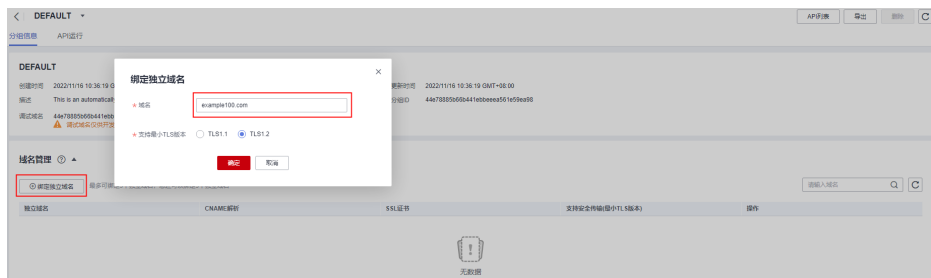
**步骤3** 在WAF侧添加防护域名时，配置“源站地址”为API网关实例的入口地址，并添加证书，以及复制WAF回源IP段。详细操作步骤请参考《WAF应用防火墙用户指南》中的“网站接入流程（云模式）”章节。

### 说明

- 如果WAF与APIG在同一VPC下，“源站地址”可以填写私网地址。
- 如果APIG绑定弹性IP，“源站地址”可以填写公网地址。



**步骤4** 在APIG实例中，为DEFAULT分组绑定已创建的防护域名。



**步骤5** 在APIG实例中，将“real\_ip\_from\_xff”开关打开，并设置参数运行值为“1”。

### 说明

客户从公网客户端访问WAF时，WAF会在HTTP头部“X-Forwarded-For”中记录用户的真实IP，APIG需要据此解析出用户的真实IP。

参数	参数取值	参数应用	参数运行值	更新时间	操作
request_timeout	200 次秒	1-1,000,000 次秒	200 次秒	-	编辑
request_body_size	12 MB	1-9,536 MB	12 MB	-	编辑
backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	-	编辑
app_debug	Off	On/Off	Off	-	编辑
app_basic	Off	On/Off	Off	-	编辑
app_secret	Off	On/Off	Off	-	编辑
app_debug	Off	On/Off	Off	-	编辑
backend_client_certificate	Off	On/Off	Off	-	编辑
ssl_ciphers	ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AE	ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AE	-	-	编辑
real_ip_from_xff	Off	On/Off	On	2023/11/17 14:57:29 GMT+08:00	编辑
xff_index	-1	http有效值	1	2023/11/17 14:57:29 GMT+08:00	编辑
vpc_name_modifiable	On	On/Off	On	2023/11/02 19:57:59 GMT+08:00	编辑

----结束

# 6 API 网关流量控制 2.0 策略

## 6.1 方案概述

### 应用场景

当在公网中调用APIG上公开的业务API时，如果不限制API调用的次数，随着用户的不断增加，会引起后端性能的下降，甚至会因为恶意用户发送的大量请求导致网站或程序崩溃。APIG提供了传统策略——流量控制，从API、用户、凭据、源IP等多个维度进行流控。

然而，随着用户多样性以及需求多样性的增加，传统流控策略无法满足更加精细的流量控制场景。比如针对某一请求参数的流控或者某一租户的流控，APIG在传统流量控制策略的基础上提供了插件策略——流量控制2.0，通过制定更加精细的方案来进行流控。

以下将以流量控制2.0为例，进行实践说明，讲述如何通过创建流量控制2.0策略来应对不同场景的网关限流。

### 方案优势

- 流量控制2.0策略可以限制单位时间内API的被调用次数，支持基础流控、参数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，与已有的流量控制策略说明功能一致，但配置方式不兼容。
  - 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：对某个租户或凭证进行特定的流控。
- 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。
- 支持按天以及按时分秒粒度的流量控制。

### 约束与限制

- API添加流量控制2.0策略相当于流量控制2.0策略同步绑定了API。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。（使用前提是绑定的API已发布。）

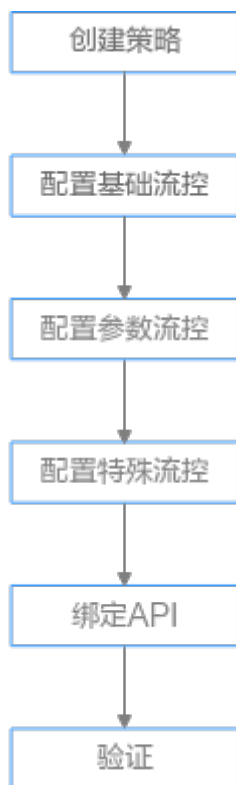
- 如果API未绑定流量控制2.0策略，流控限制值为实例“配置参数”中“ratelimit\_api\_limits”的参数运行值。
- 如果一个API绑定传统流量控制策略后，继续绑定流量控制2.0策略，传统流量控制策略会失效。
- 参数流控的规则最多可定义100个。
- 策略内容最大长度65535。
- 如果您的实例不支持流量控制2.0，请联系技术支持。

## 6.2 操作流程

假设您对一个API有如下的流控诉求：

1. 默认API流量限制为10次/60秒，用户流量限制为5次/60秒。
2. 对请求头Header字段为“Host=www.abc.com”的限制为10次/60秒。
3. 对请求方法为get且请求路径为“reqPath= /list”的限制为10次/60秒。
4. 对请求路径为“reqPath= /fc”的限制为10次/60秒。
5. 对特殊租户Special Renter的流量限制为5次/60秒。

您可以根据以下操作流程为API创建并绑定流量控制2.0策略。



1. **创建策略**  
填写流量控制2.0策略基本信息。
2. **配置基础流控**  
配置基础流量控制。
3. **配置参数流控**

- 开启参数流控配置开关，定义参数和规则配置参数流量控制。
4. **配置特殊流控**  
开启特殊流控配置开关，特殊凭据与特殊租户流量控制的使用场景。
  5. **绑定API**  
流量控制2.0策略绑定到API。
  6. **验证**  
通过相应的请求URL调用API，验证流量控制2.0策略是否生效。

## 6.3 实施步骤

### 步骤1 创建策略。

登录API网关控制台，创建流量控制2.0策略。具体操作步骤请参考《API网关用户指南》中的“流量控制2.0策略”章节。

在左侧导航栏中选择“API管理 > API策略”，单击“创建策略”，在弹窗中选择“流量控制2.0”。

根据流控诉求，配置策略基本信息。

表 6-1 策略基本信息

参数	配置说明
策略名称	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
流控类型	此处选择“高性能流控”模式。
策略生效范围	此处选择“单个API生效”，对单个API进行流量统计和控制。
时长	流量限制时长，根据诉求填写60秒。

### 步骤2 基础流控配置。



根据1，默认API在60秒内的流量限制为10次，用户流量限制为5次。

表 6-2 基础流控配置

参数	配置说明
API流量控制限制	10
用户流量控制限制	5

### 步骤3 参数流控配置。

1. 根据2，开启参数流控配置开关进行参数流量控制，定义参数Header并定义对应的规则。
  - a. 单击“添加参数”，在“参数位置”列选择“header”，在“参数”列填写“Host”。

- b. 在“定义规则”区域，单击“添加规则”，API流量限制设置为10次，时长为60秒；单击  编辑规则，设置“条件表达式配置”中匹配条件为“Host = www.abc.com”。
  - c. 单击“确定”，生成参数header为Host对应的匹配规则“Host = www.abc.com”，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。
2. 根据3、4，定义参数Path对应的多重规则。
    - a. 在“定义规则”区域，单击“添加规则”，API流量限制设置为10次，时长为60秒；单击  编辑规则，设置“条件表达式配置”中的匹配条件。
    - b. 依次添加三个条件表达式，请求路径为“reqPath= /fc”和“reqPath= /list”，请求方法为“method=get”。
    - c. 单击“转子层级”，进一步划分子层级约束条件。
    - d. 两个请求路径“reqPath”条件表达式为互斥关系，故将“AND”关系改为“OR”，表示请求路径为“reqPath= /fc”或者“reqPath= /list”。
    - e. 将“reqPath= /list”和“method= get”两个匹配条件进行约束，选中二者，单击“确定转子层级”，匹配条件默认为“AND”关系。

#### 条件表达式配置



The screenshot shows the 'Condition Expression Configuration' interface. At the top, there is a red button labeled '转子层级' (Rotor Level). Below it, a tree structure is visible. The root node is 'OR'. It has two children: a condition 'reqPath = /fc' and another 'AND' node. The 'AND' node has two children: 'reqPath = /list' and 'method = get'. Each condition has a trash icon to its right. At the bottom, there are two buttons: '确定' (Confirm) and '取消' (Cancel).

- f. 单击“确定”。表示在60s内，对于请求路径为“reqPath= /list”且请求方法为“method= get”的API或请求路径为“reqPath= /fc”的API，在API调用次数达到10次时，参数流控生效。

#### 步骤4 特殊流控配置。

根据5，开启特殊流控配置。对特殊租户Special Renter进行流量控制，限制该租户60秒内允许调用API的最大次数为5次。

表 6-3 特殊流控配置

参数	配置说明
租户ID	租户Special Renter的ID
阈值	5

**步骤5** 单击“确定”，流量控制2.0策略配置完成。

**步骤6** 绑定API。

1. 单击策略名称，进入策略详情。
2. 在“关联API”区域，选择RELEASE环境，单击“绑定API”。选择需要绑定的API，单击“确定”。

**步骤7** 验证。

通过相应的请求URL调用API，验证流量控制策略2.0是否生效。

----结束



# 7 API 网关双重认证

---

## 7.1 方案概述

### 应用场景

API网关提供了灵活的安全认证方式，用户可以配置自定义认证实现API的双重认证方式。本文以API前端认证使用APP认证和自定义认证（双重认证）结合场景为例，具体说明如何创建使用双重认证的API。

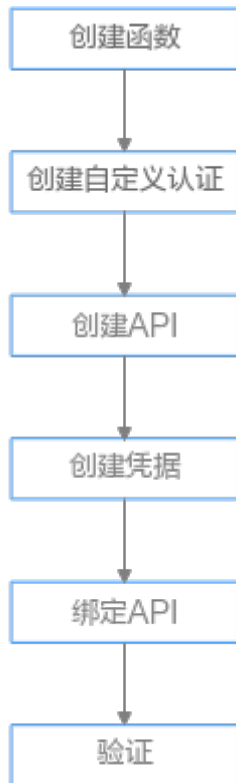
### 方案优势

API网关在提供安全的APP认证模式下，用户可根据业务需求，灵活实现自定义认证，保障API的安全问题。

### 约束与限制

API网关支持的自定义认证需要借助函数 workflow 服务实现。

## 7.2 操作流程



- 1. 创建函数**  
创建自定义的前端函数，使用函数服务开发自定义认证。
- 2. 创建自定义认证**  
创建自定义认证，类型选择“前端”，函数地址选择上一步创建的函数。
- 3. 创建API**  
安全配置中的安全认证选择APP认证，并勾选“支持双重认证”，选择上一步创建的自定义认证。
- 4. 创建凭据**  
使用APP认证的API，需要在API网关中创建一个凭据，生成凭据ID和密钥对（Key、Secret）。
- 5. 绑定API**  
将创建的凭据绑定API后，才可以使用APP认证调用API。
- 6. 验证**  
调用API，验证双重认证是否设置成功。

## 7.3 实施步骤

**步骤1** 登录函数 workflow 控制台，在“总览”页面，单击“创建函数”。详情请参考[使用函数服务开发自定义认证](#)。

1. 根据下表，填写函数信息后，单击“创建函数”。

表 7-1 函数信息配置

参数	配置说明
函数类型	默认“事件函数”。
区域	与API网关相同区域。
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。
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”。
企业项目	默认“default”。
运行时	选择“Python 3.9”。

- 在“设置”页签的左侧导航栏中选择“环境变量”，单击“添加环境变量”。参数token用于Header身份验证，test参数用于Query参数查询。对于敏感数据如token值，应开启加密参数选项。

名称	值	加密参数
test	user@123	<input type="checkbox"/>
token	*****	<input checked="" type="checkbox"/>

保存

- 在“代码”页签，编辑自定义认证代码，将以下代码复制到index.py中。完成后，单击“部署”。代码编写请参考《API网关开发指南》中的“创建用于前端自定义认证的函数”。

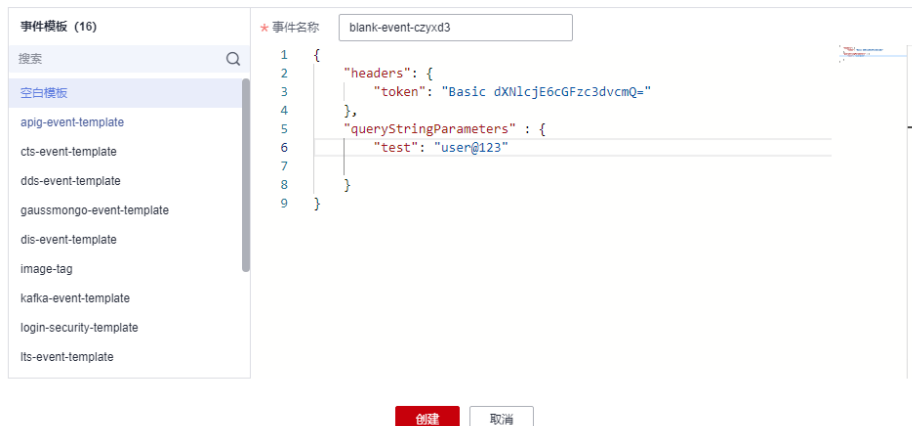
```
# -*- coding:utf-8 -*-
import json
def handler(event, context):
    testParameter = context.getUserData('test');
    userToken = context.getUserData('token');
    if event["headers"].get("token") == userToken and event["queryStringParameters"].get("test") == testParameter:
        resp = {
            'statusCode': 200,
            'body': json.dumps({
                "status": "allow",
                "context": {
                    "user": "auth success"
                }
            })
        }
    else:
        resp = {
            'statusCode': 401,
            'body': json.dumps({
                "status": "deny",
            })
        }
    return json.dumps(resp)
```

- 配置测试事件并调试代码，然后部署。
  - 在下拉框中选择“配置测试事件”并配置。

#### 说明

测试事件的参数值与环境变量中的参数值保持一致。

## 配置测试事件

 创建新的测试事件  编辑已有测试事件


b. 创建测试事件完成后，单击“测试”调试代码。



c. 单击“部署”。

**步骤2** 登录API网关控制台，在左侧导航栏选择“API管理 > API策略”。

在“自定义认证”页签中，创建自定义认证。

**表 7-2** 自定义认证配置

参数	配置说明
认证名称	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。
类型	此处选择“前端”。
函数地址	单击“添加”，选择已创建函数。
版本或别名	默认“通过版本选择”。
缓存时间(秒)	30
身份来源	第一个身份来源参数位置选择“Header”，参数名填写“token”；第二个身份来源参数位置选择“Query”，参数名填写“test”。

**步骤3** 在左侧导航栏选择“API管理 > API列表”，单击“创建API”。

1. 根据下表参数，配置前端信息。

表 7-3 前端配置

参数	配置说明
API名称	填写API名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
所属分组	默认“DEFAULT”。
URL	请求方法：接口调用方式，此处选择“GET”。 请求协议：选择API请求协议，此处选择“HTTPS”。 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调试域名，此调试域名每天最多可以访问1000次。 路径：接口请求路径。此处填写“/api/two_factor_authorization”。
网关响应	API网关未能成功处理API请求，从而产生的错误响应。 默认的网关响应为“default”。
安全认证	选择API认证方式，此处选择“APP认证”。
支持双重认证	勾选后，开启双重认证。选择 <a href="#">已创建自定义认证</a> 。

- 单击“下一步”，后端服务类型选择“Mock”。  
选择Mock自定义返回码和填写Mock返回结果，单击“完成”。
- 发布API。

**步骤4** 在左侧导航栏选择“API管理 > 凭据管理”，创建凭据。

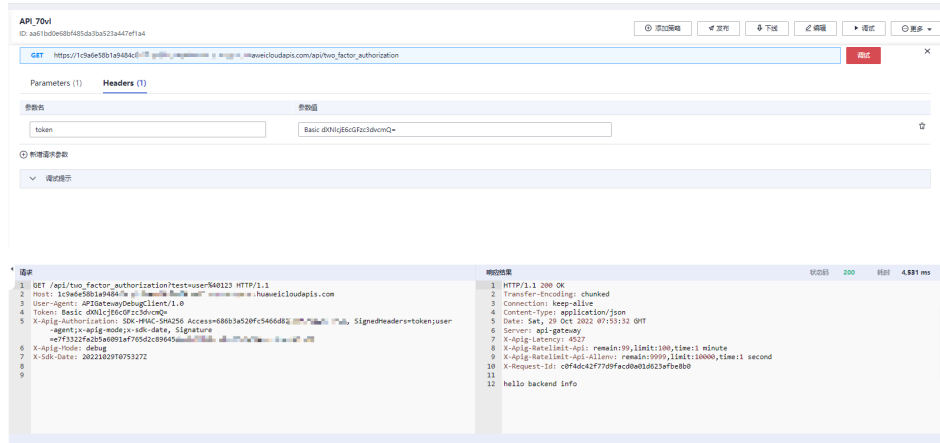
单击“创建凭据”，填写凭据名称后，然后单击“确定”。

**步骤5** 绑定API。

单击凭据名称，进入凭据详情。在“关联API”区域，单击“绑定API”，选择API并“确定”。

**步骤6** 验证。

- 您可以通过API网关的调试页面调用API，验证双重认证是否成功。  
分别在Parameters和Headers中添加定义的test和token参数，参数值确保与自定义认证函数中的参数值一致。如果请求参数与自定义认证函数不一致或参数错误，服务器返回401认证不通过。



- 您可以使用curl命令调用API，需要先下载JavaScript SDK。传入Key、Secret、以及自定义的Header、Query等参数生成curl命令，然后将curl命令复制到命令行调用API，具体操作步骤请参考《API网关开发指南》中“curl”章节。

```
$ curl -k -X GET "https://1c9a6e58b1a9484c8737ec.../api/two_factor_authorization?test-user=40123" -H "token: Basic dXN1cjE6cGFzc3dvcmQ=" -H "Host: 1c9a6e58b1a9484c8737ec... .huaweicloudapis.com" -H "X-Auth-Token: SDK-HMAC-SHA256 Access=6889b526fc346682... SignedHeaders=host;token;x-sdk-date, Signature=37666681767904819ad3f8d6b37a58680589cb2045d...4"
% Total % Received % Xferd Average Speed Time Time Time Current
t Dload Upload Total Spent Left Speed
100 18 0 18 0 0 76 0 --:--:-- --:--:-- --:--:-- 76
hello backend info
```

----结束

# 8 修订记录

表 8-1 文档修订记录

发布日期	修订记录
2023-04-30	本次变更： <ul style="list-style-type: none"><li>• 适配新版UI内容。</li><li>• 新增API网关流量控制2.0策略和API网关双重认证。</li></ul>
2023-04-12	本次变更如下： 新增API网关跨VPC开放后端服务和对接Web应用防火墙WAF。
2021-09-30	第一次正式发布。