

API 网关

最佳实践

发布日期 2023-04-30

目 录	目录
-----	----

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

云容器引擎	工作负载 / nginx-demo	2 进入工作负载详情页		编辑YAML 日志
总览 应用管理	工作负载名称	nginx-demo	类型 无线	北市工作负载
工作负载 🔺	状态	<ul> <li>运行中</li> </ul>	所運集群 den	no
无状态负载 Deployment	实例个数(正常/全部)	1/1	命名空间 defa	ault
有状态负载 StatefulSet	创建时间	2020/07/05 15:30:37 GMT+08:00	访问地址 查看	动向方式
守护进程集 DaemonSet	升级方式	滚动升级	标签 标	签管理
普通任务 Job	描述	🖉		
定时任务 CronJob				
容器组 Pod		3		
资源管理 🔹	实例列表监	空 访问方式 更新升级 伸缩 调度策略	工作负载运维 事件	
模板市场 🔹	前往网络管理查看全部	服务		在API网关中建立VPC通道对应的
插件管理	添加Service		访问方式需为"节点访问"	访问端口,即为此处的"访问端口
弹性伸缩 NEW	集群内部域名访问地	业 访问地址	访问方式	访问端口 -> 容器端口 / 协议
权限管理	nginx-demo.default.	svc.cluster.local:80 192.168.0.236 (私有)	节点访问	30249 -> 80 / TCP

#### 图 1-3 查询工作负载中实例所属弹性服务器的名称

云容器引擎	工作负载 / nginx-demo							
总策								
应用管理	工作负载名称	nginx-demo		类型	无状态工作负载			
工作负载 🔺	状态	◎ 运行中		所屈集群	demo			
无状态负载 Deployment	实例个数(正常/全部)	1/1		命名空间	default			
有状态负载 StatefulSet	创建时间	2020/07/05 15:30:37 GMT+08:00		访问地址	查看访问方式			
守护进程集 DaemonSet	升级方式	滚动升级	演动升级					
普通任务 Job	描述	🖉						
定时任务 CronJob								
容器组 Pod								
资源管理 ▼	实例列表 监控	空 访问方式 更新升级 伸缩	调度策略 工作负载运维	事件				
模板市场 🔹	删除实例			单击1 ,查看	5点IP地址,跳转到节点详情页 冒节点名称			
插件管理	实例(Poo	i) 状态 (三 最新事件	CPU申请量 (core) 内存申请	锤 (GiB) 所	在节点 运行时长 实例IP			
弹性伸缩 NEW	✓ 🗌 nginx-de	mo-5657 🧿 运行中	0.25	0.50 19	2.168.0.148 19 分钟 172.16.0.134(IP			
175.005 Aug 195								

	云容器引擎		节点管理 / demo-35000-mpwse						
	<i>щ</i> и			实例所属弹性云服务器的名称					
	应用管理		节点名称	demo-35000-mpwse 🕥	状态	◎ 可用			
	工作负载	•	节点IP	192.168.0.148	节点ID	481f2545-be8d-11ea-99de-0255ac101d49			
资源管理 🔺		*	所在子网	subnet-heru01	可用区	可用区1			
Γ	集 <b>群管理</b> 节点管理	1	操作系统	CentOS 7.6	创建时间	2020/07/05 15:00:59 GMT+08:00			
ľ	节点池管理	1	最大实例数	64 个 ⑦	云服务器组				
	网络管理								
	存储管理		概览	监控 事件 标签					
	命名空间								

• 获取"负载均衡"方式的访问信息:

云容器引擎	工作负能 / test							SHREEYAML	88	Ei	299	С
20												
工作负载	工作负载名称	test			供型	无状态工作负载						
无状态负载 Deployment	秋壶	◎ 遠行中			所懂集群	test						
有状态负载	实例个数(正第/金郎) 1/1				命名空间	default						
中PP进程编	的建筑同	2022/05/10 17:34:39 GMT+08:00			访问地址	意看访问方式						
DaemonSet	升级方式	滚动升级			标签	标签管理						
管理任务 Job 定时任务 CronJob	50× 0											
容器组 Pod												
治療管理 *												
横板市场 👻	实例列表 监护	空 · 访问方式 · 更新升级 · 仲	缩   调度策略   工作负载3	画曲 事件								
插件管理	前往网络管理查看全部经	92										
弹性伸缩	満,t@Service										C	;
权限管理	集群内部植名访问地址		访问地址		访问方式		访问第口 -> 容器第口 / 协议				操作	
122年0 ·	test.default.svc.cluster/	ocal:443	192.168.1.170 (私海)		负数均衡		443 > 443 / TCP				899	E
系统管察 -												Ģ
· 現像公卒 ₽												4

#### 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<mark>开放API</mark>。

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

API网关	4	VPC通道 ⑦ 您	还可以创建30个VPC	通道,最多可创建30个V	PC通道。	2 创建快速通道
实例概览						法論入通道を称 0 C
开放API	*					Hiddamy Operation Last 17.
API分组		通道名称	状态	类型	端口 创建时间	操作
API管理						
流量控制						
访问控制					d d	
环境管理					无记录	
签名密钥						
VPC通道	1					

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

<	新建VPC通道	I			
1	VPC通道配置		3完成		
	您的API后端配置	此处的VPC通道,使得APIi	青求分发到通道中的云服	鎊醫。 如何创建VF	PC通道?
	<b>基本信息</b> * 通道名称	apig-cce			
	* 端口	30249	CCE工作负载的	访问端口	
	分发算法	加权轮询	加权最小连接	源地址哈希	URI哈希
		结合弹性服务器权重值	, 将请求轮流转发到每	一台服务器。	
	健康检查配置				
	API网关会定期向 <sup>1</sup>	/PC通道中的云服务器发送	请求以测试其服务状态	,这些测试称为健康	<sup>融查</sup> 。如何配置健
	协议 ⑦	ТСР	HTTP HTTPS	i	
	高级设置 🖌				

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。

く)新建VPC通道										
① VPC通道配置 —— 2 添加云服务器 —	③ 完成									
您还可以添加200个云服务器,您最多可以添加	四200个云服务器。		×							
	添加云服务器									
云服务器名称	→ → → → → → → → → → → → → → → → → → →									
	创建云服务器	请输入云服务器名称 Q C								
	■ 云服务器名称	云服务器ID	-4							
	demo-35000-0sgl9 CCE实例所属弹性	239d4433-fd32-430f-8a2b-fafd9f31f7f4	无记录							
2	✓ demo-35000-mpwse 云服务器名称	262d802e-4937-4219-ab0a-c4dbe6307481								
	Cli-demo	a26d406c-49df-4f71-b4b7-341c1498528a								
	3 添加	取消								

#### 步骤4 单击"完成",添加VPC通道。

⑦ 添加弹性云服务器				
弹性云服务器名称		弹性云服务器ID	权重 ⑦	操作
cce-node		19dba5f7-e1cc-4911-8208-7fbf1bfd5f6f	1	删除
上一步	取消 完成	•		
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

API网关	4	API分组 ⑦ 惣	5可以创建29个分组,最多可创建30个分组。		2	创建分组
实例概览				×	、分组名称	QC
Thttapi	Î	创建分组			操作	
API管理		* 分组名和			API管理 编辑 更多	•
流量控制			又持汉子,央义,数子,卜划线,且共服以央义和汉子开头,3-04子付			
访问控制		佃还	使用API网大开放CCE架例			
外境管理 						
VPC通道			14/255			
自定义认证			<b>确定</b> 取消			
调用API	-					

#### 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

API网关	*	API管理 ⑦ 您还可以创想	PI管理 ① 题还可以创建99个API, 最多可创建100个API.         2         新建API         导入API         导致性的         特別         特別								
实例概览		HOT 【日常任务】前	住 会员中心 领태	取日常任务, 嬴研	可更换好礼	L!					
开放API	*										
API分组		授权发布	下线	删除 ⑦	所有	组		▼ 所有运行环境 ▼	请输入API名称	Q 标签	× C
API管理	l										
次日共和		API 运行	类型	安全认证	所属	描述	标签	更新时间	操作		
远遥控制		API	公开	APP认证	APIG			2019/06/24 19:19:00 GMT+08:0	0 授权 2	定布   更多 ▼	
访问控制											
环境管理											
签名密钥											

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

く 新建API	
1 基本信息 —	
基本信息	
* API名称	cce_demo 支持汉字,英文、数字,下划线,且只能以英文和汉字开头。3-255字符
* 所属分组	cce_group         ▼         C         新識分組           当前选中分组下已创建0个API,还可以创建200个API
* 网关响应	default 🔹
类型	
安全认证	APPULic         华为IAMULit         自定义认证         无认证           无认证模式、安全级剧低、新有用户均可访问、不维导使用。
标签	- 清縮入标签名

3. 在"定义API请求"界面,输入如下图所示信息。

く 新建API	
1 基本信息	- 2 定义API请求
定义API请求	
域名	5e3e17a8edfd4d488dd3a159975eceff
请求协议	HTTP HTTPS HTTP&HTTPS
* 请求Path	支持WebSocket / 请求Path可以包含请求参数,用①标识,比如/getUserInfo/(userId),支持 * % + 等符殊字符。
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, 请前住了解评情
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<mark>已 创建的VPC通道</mark>;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
你可以送加等略后送本美昌少后	洋宁 /
您还能创建5个后端策略	mack, 9 Fixeedam/ujitacka/Fixeedamit, 709 machanausiyea.cmu ayyu zoneedasiya
默认后端	+ 添加策略后族
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通道访问您邮署在VPC内的服务选择已创建好的VPC通道
* VPC通道	apig-cce - C 管理VPC通道
自中Vbort创城	
ELECTION	在達成物結局到VPC 通道中的云照各器能。 合体您自己 V 速度的Host 半線。 默认 格使用造成中间始的Host 半線。
* 后端请求Path	
	请求Path可以包含请求参数,用{}标识,比如/getUserInto/{userId},支持 * % 、 等特殊学符。
* 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。

く 新建API	
① 基本信息	<ol> <li>定义API请求 (3) 定义后端服务 (4) 定义返回结果</li> </ol>
返回结果基础定义	
* 成功响应示例	welcome to nginx.
	17/20,480
失败响应示例	
	0/20,480

- 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

AP	1管理 ⑦ 您还可!	以创建98个API,	最多可创建10	D∱API。					新建API	导入API 导出API
	HOT 【日常任务	】 前往 会员中	心 领取日常任务	, 赢码豆换好礼!						
	授权 发布	i 下线	删除	0		所有组		▼ 所有运行环境 ▼	请输入API名称	Q 标签 ※ C
	API名称	运行环境	类型	安全认证	所属分组	描述	标签	更新时间	操作	
	cce_demo		公开	无认证	cce_group			2020/07/05 16:28:40 GMT+08:00	) 授权 2	苑 更多 ▼
	API_PaaS		公开	APP认证	APIGroup			2019/06/24 19:19:00 GMT+08:00	) 授权 2	in i

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

API管	理	⑦ 您还可以	创建98个API,	最多可创建100	I/YAPI.					新建API	导入АРІ	导出API
C	ОТ	【日常任务】	前往 会员中心	> 领取日常任务	, 赢码豆换好礼!							
	授权	发布	下线	删除	0		所有组		▼ 所有运行环境 ▼ 1	青输入API名称	Q 标签	× C
		API名称	运行环境	类型	安全认证	所属分组	描述	标签	更新时间	操作		
		cce_demo		公开	无认证	cce_group			2020/07/05 16:28:40 GMT+08:00	授权 2	这布 更多 ▼	
		API_PaaS		公开	APP认证	APIGroup			2019/06/24 19:19:00 GMT+08:00	授权 2	技布 │ 更多 ▾	

2. 设置发布信息。

#### 图 1-12 发布 API

く   发布A	РІ
API名称 发布环境	cce_demo
说明	该操作将覆盖该API在选中环境的配置,请仔细确认。
 <u>ر</u> س م	请输入发布API的说明。

#### -----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

API网关	*	API管理 ⑦ 您还可以	人创建98个API,	最多可创建100	I/YAPI。					
实例概览		HOT 【日常任务】	】前往 会员中/	心 领取日常任务	, 嬴码豆换好礼!					
开放API	*									
API分组		授权发布	下线	删除	0		所有组	•	所有运行环境	• Ì
API管理										
101012		API名称	运行环境	类型	安全认证	所属分组	描述	标签	更新时间	
流量控制		cce_demo	RELEASE	公开	无认证	cce_group			2020/07/05 16:28:40 G	MT+08:00
访问控制				0.77						
环境管理		API_Paas		公开	APPiXiE	APIGroup			2019/06/24 19:19:00 G	MT+08:00

2. 在API详情界面,复制"API URL"。

#### 图 1-14 复制 API URL

API管理 / cce_demo 更换API									
总览	调用信息	授权信息	流控策略	ì	访问控制	签名密钥	发	布历史	
							*	/	
API URL	GET http://5e	3e17a8edfd4d488	dd3a159975ece	ff.			/ 🗖		

**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》。 ← → C ① 不安全 | 5e3e17a8edfd4d488dd3a159975eceff

#### 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 <u>nginx.org</u>. Commercial support is available at <u>nginx.com</u>.

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。

基本信息	
区域	▼ ▼ 不同区域的资源之间内网不互通。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	vpc1
IPv4网殿	192 · 168 · 0 · 0 / 16 ▼ 建议使用网除: 10.0.0/8-24 (选择) 172.16.0.0/12-24 (选择)
企业项目	default  C 新建企业项目 ③
高级配置 ▼	标签   描述
默认子网	
可用区	可用区1 • ⑦
名称	subnet-364f
子网IPv4网段	192     ・     168     ・     0     /     24     ▼     ⑦     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 ⑦
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

#### 图 2-1 创建 VPC 示例参考

#### 🛄 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工作流服务实现,用户在函数工作流中创建自 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

在函数工作流的控制台编写函数,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"。

在函数工作流页面创建一个函数,语言选Python 3.6。

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 3.6。

表 3-1 函数信息配置

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 dXNlcjE6cGFzc3dvcmQ=':
     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。

≡	API网关 6 自定义认证 ⑦ 您还可以创建10个自定义认证,最多可创建20个自定义认证。 创建自定义认证								
$\bigcirc$	CONTRACTOR						-		
6	Department.						×	人证名称 Q C	
ය	HERAPI	1	21 57	创建自定义认证				19.//:	
	API分组		RAME .	* 认证名称	authorizer			10x1F	
-	API管理		autr						
0	流量控制		Auth	* 庾型	別」時 /白湖市			编辑 删除	
Ô	访问控制		Auth	* 函数地址	urn:fss:cn-north-7:73d69ae0cfcf4 添加			编辑 删除	
$\Phi$	环境管理		Auth	身份来源 ⑦	参数位置 参数名	操作		编辑 删除	
e	签名密钥				<ul> <li>添加身份来源</li> </ul>				
<u>ن</u>	VPC通道		Autr	* 缓存时间(秒) 🕜	- 0 +				
	自定义认证		Auth	田白新田				编辑 删除	
	调用API		Auth		1999/74/~306			编辑 删除	
	440 I.S		Auth					编辑 删除	
					0/2,048				
			Autr		1 注意:用户数据会明文展示所输入信息。清防止信息;	Ψ		編編   翻除	
			Auth					编辑 删除	
					创建取消				

#### 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"}

≡	API分组 / APIGroup_0zfu		
	概范 API列表 变量管理	城名管理 网关响应	
6			
&	<ul> <li>新端网关调应</li> </ul>		响应详情
Ø	default	拒绝访问	自定义认证失败 自定义认证方证回认证失败
Ø		自定义认证配置错误	响应状态码
Φ		自定义认证失败	401
©		自定义认证身份来源错误	消息模板
<u></u>		认证失败	响应类型 application/json
		认证身份来源缺失	項应內容 1 {"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。

① 数化和目標         ② 数义和/講家         ④ 主义近朝地路         ④ 主义近朝地路         ④ 主义近朝地路           ● 取り込む加速地に加速した         ● 取りたりません         ● 取り込む加速地に加速した         ● 取りたりません           ● 取り込む加速地に加速した         ● 取りたりません         ● 取り込む加速地に加速した         ● 取りた           ● 取り込む加速地に加速した         ● 取りたりません         ● 取りた         ● 取りた           ● 取りた         ● 取りた	
安正規構成         NTTP/NTTPS         EncloseGaph         Mack             空間以認加度報告報申考提升化告端定义、申令儀報告論的合定之义多个集場条件、具有满是相应的情報条件的書次方会被转发到就算報告编。           空間以認加度報告報申考提升化告端定义、申令儀報告論的合定之义多个集場条件、具有满是相应的情報条件的書次方会被转发到就算報告编。           空間の認知意報告の告謝構成         中、認知意報告           文化活動         中、認知意報告           文化方面         中、認知意報告           夏秋日         中、           東方式         CET           夏秋日         予度用           伊田         中、           海方式         CET           「使用         予度用           伊田         ()         管理の           「使用         「使用         「           「使用         「	
つ い い い い い い い い い い い い い い い い い い	
おいばお御御に読みと見いて行きである。	
SZEBBUŻEYCERSHORE      SUCJECK      TALICE RALICERS      SUCJECK      SUCJEC	
Wix         HTTP           请求方式         GET           使用VPC通道         使用           使用VPC通道訪问您能看在VPC内的服务           **VPC適適         C 管理VPC通道           通常次的结婚期看在VPC内的服务           **VPC適適         C 管理VPC通道           通常次的结婚期看在VPC内的服务           **Craff         VPC doci           在请求您转发到VPC通道中的无服务器前,允许您自定义请求的Host头线,默认将使用请求中原始的Host头域,           **后請讓求和計「           / 方ackend           请求和时记私会请求条数,用(h运识,比如/getUserInfo/(userId),支持*% 等特殊字符,           **后請請請求如何           使用自定义认证获取授权信息未访问后請           你人PPL喝多可创道30个后猜服务争救,常量争数和系统参数,还可以创道349个,           后請疑务教 ② ~           凝集教 ③ ~           凝集教 ③ ~           系统教理         Ke教教在         Ki教教在	
Betware X           协议         HTTP           请求方式         GET           使用VPC通道         使用         不使用           使用VPC通道         使用         不使用           使用VPC通道         使用         不使用           使用VPC通道         C         管理VPC通道           直定Xhot线域         C         管理VPC通道           直定Xhot线域         C         管理VPC通道           正 在请求被转线到VPC通道中的云服务器前,允许您自定义请求的Hot线域、默认将使用请求中原始的Hot头域。         *           * 后請請求Path         /backend         ····································	
请求方式       GET         请求方式       GET         使用VPC通道       死便用         使用VPC通道       不便用         使用VPC通道       使用VPC通道         直定义host关域	
使用VPC通道     使用VPC通道访问您部署在VPC内的服务     使用VPC通道访问您部署在VPC内的服务     VPC通道     使用VPC通道访问您部署在VPC内的服务     VPC通道     管定义host关城     正在请求被转发到VPC通道中的云服务器前,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,     在请求被转发到VPC通道中的云服务器前,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可以包含请求参数,用(/场讯,比如/getUserInfo/(userId),支持*%,等特殊字符,     请求Path可以包含请求参数,用(/场讯,比如/getUserInfo/(userId),支持*%,等特殊字符,     请求和th可以包含请求参数,用(/场讯,比如/getUserInfo/(userId),支持*%,等特殊字符,     "后端器时(ms) 5000     质端处理 医维索勒和系统参数,还可以创建49个,     后端服务参数 ③ ~     系统参数 ④ ~     系统参数 ●      医结态数公数 ●      后续数公数 ●      后续数公数 ●      后续数公数 ●      后续数公数 ●      后续数公数 ●      后续数公数 ●      任	
ではついて、認識             のはのののののののののののののののののののののののの	
* VPC通道     VPC_doi     C 管理VPC通道     E定义host具域     E定义host具域     在请求被转发到VPC通道中的无服务器前,允许您自定义请求的Host具域,默认将使用请求中原始的Host具域,     在请求被转发到VPC通道中的无服务器前,允许您自定义请求的Host具域,默认将使用请求中原始的Host具域,     正确求求和可以包含请求参数,用()预识,比如/getUserInfo/(userId),支持*%够特殊字符,     语源时(ms) 5000     后端缺び     使用自定义认证获取授权信息未访问后端     何个API最多可创建50个后端服务参数,常量参数和系统参数,还可以创建49个,     后端服务参数 ② ~     聚合数 ② ~     系统参数 ② ~     系统参数 ◎ ~     系统参数 ●	
自定义host关域	
在请求被破发到VPC通道中的云服务器前,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, * 后读请求Path可以包含请求参数, 用()标识, 比如/getUserInfo/(userid), 支持 * % 等特殊字符, * 后读超时(ms) 5000 后读认证 ① 使用自定义认证获取提权信息未访问后读 每个API最多可创建50个后读服务参数, 常量参数和系统参数, 还可以创建49个, 后读服务参数 ② ~ 発量参数 ③ ~ 系统参数 ~	
<ul> <li>* 后端请求Path //backend 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。</li> <li>* 后端超时(ms) 5000</li> <li>后端认证 使用自定义认证获取授权信息来访问后端</li> <li>每个API最多可创建50个后端服务参数,常量参数和系统参数,还可以创建49个。</li> <li>后端段务参数 ② ~</li> <li>第最参数 ③ ~</li> <li>系统参数 ~</li> <li>系统参数 ~</li> <li>系统参数 本</li> <li>系统参数在 后端参数公案 后端参数公案 后端参数公案 描述 操作</li> </ul>	
<ul> <li>請求Path可以包含請求參数,用()标识,比如/getUserInfo/(userId),支持*%,等特殊字符。</li> <li>*后講題时(ms)</li> <li>/// 「</li> <li>// 使用自定义认证获取授权信息未访问后端</li> <li>// 使用自定义认证获取授权信息未访问后端</li> <li>// 每个API程参可创建50个后端服务参数、常量参数和系统参数,还可以创建49个。</li> <li>// 后端服务参数 ③ ~</li> <li>// 常量参数 ③ ~</li> <li>// 系统参数文章</li> <li>// 系统参数文章</li> <li>// 新修</li> <li>// 新修</li> <li>// 指修</li> </ul>	
<ul> <li>* 后端銀时(ms) 5000</li> <li>后端以近 ●</li> <li>使用自定义认证获取接权信息未访问后端</li> <li>每个API最多可创識50个后端服务参数、常量参数和系统参数,还可以创建49个、</li> <li>后端服务参数 ② ~</li> <li>第量参数 ③ ~</li> <li>第最参数 ③ ~</li> <li>系统参数 ~</li> <li>系统参数 本</li> <li>系统参数 本</li> <li>系统参数 本</li> </ul>	
后端认证 使用自定义认证获取授权信息未访问后端 每个API很多可创建50个后端服务参数、常量参数和系统参数,还可以创建49个。 后端服务参数 ① ~ 常量参数 ② ~ 系统参数 ▲ 系统参数 ▲ 系统参数 ▲ 系统参数 ▲	
使用自定义认证获取接权信息未访问后端 每个API最多可创建50个后端服务参数、常量参数和系统参数、还可以创建49个。 后续服务参数 ⑦ ~ 第最参数 ⑦ ~ 系统参数 ペ 系统参数 ペ 系统参数 ペ 系统参数 本 系统参数な数 后端参数な数 后端参数位置 描述 操作	
<ul> <li>毎个API最多可创連50个后端服务参数、常量参数和系统参数、还可以创建49个。</li> <li>后端服务参数 ⑦ ~</li> <li>常量参数 ⑦ ~</li> <li>系统参数 ^</li> <li>系统参数 本</li> <li>系统参数 「議参数欠款 」 后端参数欠款 」 后端参数位置 描述 操作</li> </ul>	
「請服務参数 ⑦ ∨ 常量参数 ⑦ ∨ 系统参数 ^ 系统参数 ▲ 系统参数 ▲	
常量参数 ⑦ ~ 系统参数 ^ 五体参数学型 五体参数文数 后端参数次数 后端参数位置 描述 操作	
系统参数 ^	
系统参观变型 条统参数名称 片端参数名称 片端参数位音 袖体 操作	
	1
前時八业参数 * user_name X-User-Name HEADER * 请知人加达 翻除	

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。

post 🗸	http://c6300fb67474472da333165f27007dd2/api/echo	Params	Send	~
Body Cookies	Headers (14) Test Results		Status: 200	ок
Pretty Raw	Preview			
POST /api/echo host: c6300fb6; authorization: x-real-lpi 103 connection: Ket cache-control: origin: chrome- x-forwarded-ho: accept: x/* X-user-Name: us x-forwarded-pro content-length accept-encoding user-agent: Mo: x-forwarded-forwarded-forwarded-f	HTTP/1.1 474472da333165f27007dd2. Basic dXNL0[E6cGFzc3dvcmq= 218.28.69 p-Alive no-cache extension://fhbjgbiflinjbdggehcddcbncdddomop t: c6300fb6747472da33165f27007dd erf1 t: 68 t: c6300fb674472da33165f27007dd erf1 t: d0 t: c910, deflate 111a/5.0 (Windows NT 10.0; Win64; x64) ApplewebKit/537.36 (KHTML, like Gecko) Chrome/8 :103.218.218.69 :5f986db3f6cd4fdfea84db5457b97a1 :: zh-CN,zh;q=0.9	4.0.4147.89	Safari/537	.36

# 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





#### 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



**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。

- **创建实例** 在VPC1上创建API专享版实例。
- 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。
- 创建API 创建API,后端服务地址配置ELB的IP。
- 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)。
- **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<mark>表4-2和表4-3</mark>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	

基本信息			
区域	•		
	不同区域的云极势产品之间的网互不相遇;请截近选择能近您业务的区域,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。重看区域下已有vpc网段		
企业项目	default  v C 新建企业项目 ⑦		
高级配置 🔻	标签   描述		
默认子网			
<b>默认子网</b> <sup>名称</sup>	subnet-bf15		
<b>默认子网</b> 名称 子网IPv4网段 <b>⑦</b>	subnet-bf15		
<b>默认子网</b> 名称 子网IPv4网段 <b>⑦</b>	subnet-bf15       192 · 168 · 0 · 0 / 24 ▼       可用IP設: 251       子例创建师成后,子网网纪无法传改		
試入子阿 名称 子別Pv4网段 ⑦ 子別Pv6网段	subnet-bf15       192     ·       0     /       24     ▼       可用IP26: 251       子例阅建来成后, 子例网段无法传改       可用IPV6 ⑦		
試入子列 各称 子列(Pv4列段 ⑦ 子列(Pv6列段 关联指由表	subnet-bf15         192 · 168 · 0 · 0 / 24 ▼         可用P26: 251         子网创建和成后、子网网站无法传放         开曲Pv6 ②         新礼 ③		
款认子何           各称           子网IPv4网段           子网IPv6网段           子网IPv6网段           关联强由表           高級配置	subnet-bf15         192 · 168 · 0 · 0 / 24 ▼         可用IP数: 251         子列创建电成后,子列网段无法传放         开启IPv6 ⑦         默认 ⑦         网关   DNS报务器地址   DHCP程的时间   标签   描述		
款认子列 名称 子列IPv4网段 ⑦ 子列IPv6网段 关取指由表 高级配置 ▼	subnetbf15         192 · 168 · 0 · 0 / 24 ▼         可用P20: 251         子列創建現成后,子列列和无法傳改         开曲Pv6 ⑦         默从 ⑦         网关   DNS服务器地址   DHCP唱的时间   标签   描述		

#### **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"。

* 区域	▼ 不同的結果的意义用外科不正直,我的原则还能让你让你会必须的问题,可以提供和利用的目标。 提供你可以愿意。							
* 可用区	可用区1 可用区2	0						
* 实例名称	apig01 中英文字符开头,只能由中英文字符		下划线组成,长度为3~64的字符。					
* 实例规格	基础版		专业版		企业版		铂金质	
	每秒最大请求政 SLA	2,000 99.95%	每秒最大演求数 SLA	4,000 99.95%	每秒最大請求数 SLA	6,000 99.95%	每秒最大请求数 SLA	10,000 99.99%
* 可维护时间窗 * 企业项目	220000 020000 ・     ③       default ・     C       20回線協議会会会項目、第四項目220回線議業							
公网入口	□ 并是公用入口 ⑦							
公网出口	□ 并最公開出口 ⑦							
* 网络	VRC1         ▼         C         ②           X需給援除的点形成系示: 即可將往送時給鐵         ▼         C         ③							

#### **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"22:00:0002:00:00"。
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 <mark>已创建的虚拟私有云</mark> "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	接浮型						
<b>★</b> 区域	▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ▼ ■						
* 可用区	可用区1 💿 💌 负载均衡支持同时部署在多个可用区, 多活模式目	互为备份,可提供更高的可靠性。					
网络配置							
* 跨VPC后端	0						
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) (	Ð				
★ 所屬VPC	VPC2 v C 查看	<del>差</del> 拟私有云					
* 子网	subnet-02 (192.168.0.0/24) ・ C 査書 可用私有IP数量243个	子何					
★IPv4地址	目动分配IPv4地址 v						
* 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。					
	应用型(HTTP/HTTPS) 网络型(TCP/U	JDP) ⑦					
	规格	新建连接数 (CPS)	最大连接数	帶案 (Mbit/s)	LCU		
	④ 小型1	10,000	500,000	50	10		
	○小型Ⅱ	20,000	1,000,000	100	20		
	○中型Ⅰ	40,000	2,000,000	200	40		
		80,000	4,000,000	400	80		
	○大型Ⅰ	200,000	10,000,000	1,000	200		
	大型II         400,000         20,000,000         2,000         400						
	当前法理实例: 网络型(TCP/UDP)   小型 I ・ elbv3.basic.1az   10 LCU						
* 名称	elb-zjy						

#### 表 4-5 弹性负载均衡参数

后端子网 | 描述 | 标签

高级配置 ▼

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 <mark>已创建的虚拟私有云</mark> "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 后望	服务器组 标签		
名称	listener-http 🖉	ID	d
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 ⑦
创建时间	2023/03/02 15:00:40 GMT+08:00	描述	- 🖉
高级配置 🔻			

#### 图 4-3 后端服务器组信息

基本信息	后;满服务:蓄组	标签		
名称	sg_serve	er_http	ID	0
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。
  - 1. 在"路由"区域单击"添加路由"。
  - 2. 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"。
  - 3. 单击"确定"。

#### **图 4-4** 本端路由

基本信息 本調路由 对鳞路由				
请前往路由家源加基于该对哪注册的路由。				
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-9be0-4db0-9058-1c2bfa5b627c)	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。
  - 1. 在"路由"区域单击"添加路由"。
  - 2. 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"出私网 IP"地址。
    - 下一跳类型:选择"对等连接"。
  - 3. 单击"确定"。

#### **图 4-5** 对端路由

基本信息 本洲路由 对通路由				
请前往路由表添加基于该对哪注题的路由。				
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-9be0-4db0-9058-1c2bfa5b627c)	rtb-vpc-002	
192.168.0.239/32	对等连接	peering-zjy(163a0a5f-9be0-4db0-9058-1c2bfa5b627c)	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。

基本信息	配置參数							
🗔 实例信	息 💿 遠行中				∂ 入口地址			
实例名称	apig-z]y 🖉	案例D	<i>a</i>		虚拟私有云访问地址	10.0.39.239		
规格	基础纸	描述	🖉		弹性IP地址	立即雇用		
可维护时间窗	22:00.0002:00:00 🖉	可用区	可用区1 ae-ad-1b		) Howe			
企业项目	default	enterin	2022/08/02 17:44:15 GMT+08:00		出公网吗	出私网IP	10.0.39.101,10.0.3	
					出公网带宽			
🕑 网络	置5							
虚拟私有云	VPC1							
子网	subnet-f9a9							
安全组	sg-zjy 🖉 通过公网访问APIG需要在安全组添加入方	RARONIAC	80、443、且提留"把内云服务器间开放所有满口"的规则					
①路由				更改				
• 10.101.0.0/1	16							

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"。

1 HARRY	- 2 RHRE - 3 RORE - 4 HUR	t.			
216	*           不同反始的无能发产品之间内间互不把握。请就让这样能达到上发出	EM. TROMANDA MAGRAMA.			
可用区	随机分配 可用区1 可用区2	0			
CPU研究 規格		▼ 内存 全部 超現い0型 GPU50建型 Alt	✓ 規握条件: (2#型 ⑦)	Q	
	彩彩光台	VCPLK LINEX(GIR) J=	CPU J=	新建 / 最大物家(⑦ 」=	=. (?) #\$\$\$\$\$\$\$
	s6.medium.2	1vCPUs   2 GIB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000
	56.medium.4 (己售信) 可购买区域	TVCPUs   4 GIB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000
	56.large.2 (已錄動) 可時形式地	2vCPUs   4 GIB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000
	55.large.4 (已思想) 可時形式編	2vCPUs   8 GIB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000
	s5.vlarge.2 (己告弟) 可购买区域	4vCPUs   8 GIB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	250,000
	二伯初始 通用型   séumedium.2   tvCPUs   2 GiB				
12.9	<u>☆用R\$</u> E有限者 共 <b>可</b> 限者				
	CentOS * CentOS 7.5 64bit(40GB)	• C			
系统盘	- 40 + GE	10P5上限1,440,10P5资发上限5,000 雇	<b>₩</b> ~		
	④ 増加一株数据量 您还可以注意23块V8D进量或59块5CS或量。				

#### 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 <mark>已创建的虚拟私有云</mark> "VPC2"和子网。
安全组	选择 <mark>专享版实例</mark> 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。

基本信息							
名称	server_group-zjy 🖉			ID	c4cc9d25-948f-497d-9efb-786b72e6b96d		
监听器	listener-zjy			后端协议	тср		
分配策略类型	配策略类型 加权轮询算法			健康检查	已开启 配置		
会活保持	会活界物 未开启			描述	🖉		
IP类型	双栈						
云服务器	跨VPC后端	辅助弹性网卡					
添加云服务	<b>器</b> 修改权量	移除 已添加1个云服务器			全部 ▼ 名称	Ŧ	QC
2 名称		状态	私网IP地址		健康检查结果 ⑦	权重	业务端口
ecs-zjy		● 运行中	10.101.0.187 主网卡		● 正常	1	80

- 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



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

-	①客户端发送请求到WAF	②WAF转发过滤后的请求到APIG	(API)	③APIG将请求路由到后端服务器	J
客户端	WAF		API网关		后端服务器

#### 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

<   API	Group_001 -			
分组信息	API运行			
APIGro	up_001 🖉			
创建时间	2022/11/17 14:39:25 GMT+08:00	更新时间	2022/11/17 14:39:25 GMT+08:00	
描述	2	分组ID	56a428d5c0a24351b387b6cddbfa45af	
调试城名	56a428d5c0a24351b;	]		

#### **图 5-3** 新建 API

< APIGroup_001 *		API列表	9±	899	С
相信息 API运行					
C MEAN C MESH					
	GERMIERMELTER-FE- Germier				

**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。

月站设置 / <b>添加防护用站</b>			
法保険型 ● 云横式 ○ 除草横式			3) 10:40
	* 防护城名	Baampie100.com ♥ ⊕55#3#□	
	* 98⊡	4443 V	
	*服务器配置	HYPHING         BANDAK         BANDAK         BANDAK           HITTIS	
	* 证书名称	tent · 甲AmEE	
	* 是否已使用代理	<b>2</b> 3	
	注意: 著已使用如	商助、CDN、云加速時代理,为了倒錄WAF的安全錄略能够针対真实源Pr生效,请各必选择"量",	

#### 步骤3 在APIG实例中,为API分组绑定已创建的防护域名。

< APIGroup_001 *					APIPER Bit I	the C
分组信息 API运行						
APIGroup_001 企 回題時間 2022/11/17 14/39/25 GN 届活 企 場合は総合 564420650824551b385 ▲ 第記地名のの形形出来	<del>御定独立城名</del> + 354 examples106.com	X 17 14 39 25 GMT+06 00 5c0a24351030706c00094541				
<b>域名管理 ⑦ ▲</b> ◎ #是独立城名	* 2558-0-1.555 ( 1.51.1 ) 1.51.2				请能入地名 C	2 C
独立地名	CNAMENER	S SLIEH	支持安全传输(最小TLS版本)	1011		
		(I) Firster				

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。

<b>实例</b> [[]]	配置参数 终端节点管理					
	參数	参数默认值	参数范围	參数运行值	更新时间	操作
	③ ratelimit_api_limits	200 次胞	1-1,000,000 35/89	200 20/82		85
	request_body_size	12 MB	1-9,536 MB	12 MB	44	#8
	③ backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	-	94 <b>8</b>
	③ app_token	orr	nion	orr		85
	③ app_basic	orr	On/Off	orr	44	#8
	③ atb <sup>-secuel</sup>	orr	On/Off	Off	-	94
	③ abb_tongs	orr	On/Off	orr	-	85
	backend_client_certificate			orr	44	98 9
	③ ssl_cipters	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-/	E	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-/	E -	94
^	Thu_mont_qi_lean	orr	OniOff	On	2022/11/17 14:57:29 GMT+08:00	85
	参数	參数默认值	参数范围	參数运行值	更能时间	提作
	③ xf_index	-t	int32有效值	1	2022/11/17 14:57:29 GMT+08.00	-
	vpc_name_modifiable	On	more	On	2022/11/02 19:57:59 GMT+08.00	948

-----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。

实例信息 配置·	P数 终端节点管理		
基本信息	warden d	() () () () () () () () () () () () () (	
实例D	48/35/96/274(	网络配置	
可用区援送	মঞ্জ হামাত্র। হামাত্র। ⊉	虚拟私有云 子网	vpo-kalka subne-kalka
企业项目 可确约时间曾	ostaut 22.00.00-02.00.00 🖉	安全组	sg-tafa 2 重过公司访问APAC國要在安全回源IDA力內規則的與口ao、443、且從圖 "因为云能計錄得开放所有與口" 的規則
计费信息		入口地址	100 1580 147 🗗
计模模式 创建时间	绘陶计编 2022/11/16 10:30:40 GMT-08:00	3种性IP地站(ELB)	

#### 步骤2 在DEFAULT分组中添加API。

< DEFAULT -	
分组信息 API运行	
<ul> <li>○ 創建API</li> <li>② 批量優作</li> </ul>	
请输入API名称搜索 Q	
6.5	( _ )
无记录	您月龄不设查tri@atri@atri@atri@atri@atri@atri@atri@a
	<u>© श्रीवित्रम</u>

**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。

1 域名配置 ——	<ul> <li>② WAF@潮IP加白</li> </ul>	(3) 修改DNS解t
网站名称		
* 防护域名	example100.com	
★ 端口	4443 🔹	
网站备注		
★ 服务器副量	ガ外抜攻 ⑦ 潤始抜攻 ⑦ 潤始始址 ⑦	
* 证书名称	test_cert v 导入新证书	
* 是否已使用代理	是否	
* 策略配置 (?)	注意:1、WAFQ交持Web流量,非Web流量接入WAF层无法转发(包括但不限于UDP、SMTP, FTP等非Web洗协议) 2、若已使用如高防、CDN、云加速等代理、为了保障WAF的安全策略能够针对真实源P生效,请务必选择"是" 系统自动生成策略	
	下一步 取消	

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

					APØ读 导出	1889 C
DEFAULT egilienit 2022/11/16 10:36 19 G sind: This is an automatical: sindista 44/78350050441teb sindista 64/7835005441teb	- 第2接立域名 - 第5	X ###955 202211116 18 36 19 GMT-08 00 0180 44478855566444 teabaeea56 1e59ea98				
<b>送名賞理 ③ ▲</b> ◎ #E独立城名 <sup>最多可做</sup> 。 独立城名	* 23582-715825 () T.911 () T.912 () () () () () () () () () () () () () (	555.亚书	支持安全传输(图小11.5版本)	操作	潮輸入域名	Q C

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。

突例仰	配置参数 终端节点管理					
	參数	参数默认值	参数范围	參數运行值	更新时间	操作
	③ ratelimit_api_limits	200 25/89	1-1,000.000 25/85	200 25/85	-	44
	request_body_size	12 MB	1-9,536 MB	12 MB		46
	③ backend_timeout	60,000 ms	1-600,000 ms	60,000 ms	-	94
	③ app_token	orr	On/Off	orr	-	44
	③ app_basic	orr	On/Off	orr	10	46
	③ atb <sup>-secuel</sup>	orr	On/Off	orr	-	94
	③ abb_tonge	orr	On/Off	orr	-	44
	backend_client_certificate			orr		44
	③ ssl_cipters	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-A	Ε	ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-A	E	94
^	() real_ip_trom_vtf	orr	On/Off	On	2022/11/17 14:57:29 GMT+08:00	44
	6h	使数据认值	条数正规	泰教运行值	电路线网	授作
	③ xf_index	4	int32有效攝	1	2022/11/17 14:57:29 GMT+08:00	
	vpc_neme_modifiable	On	Onioff	On	2022/11/02 19:57:59 GMT+00.00	88

----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。

- 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 
   ④ 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。

  - 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

转子层级

reqPath 💌 = 💌	r lfc ū	
OR 🗸		
reqPath 💌	= v /list	Ū
AND 🗸		
method 💌	= v get	Ū
÷		
$\oplus$		
	确定 取消	

 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工作流服务实现。

## 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。

 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 登录函数工作流控制台,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"。

2. 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。

环境变量 ⑦		
02	值	加密参数
lest	user@123	
loken		
- <del>R</del> #		

 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"。



a. 在下拉框中选择"配置测试事件"并配置。

🛄 说明

4.

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				
事件模板 (16)		★ 事件名称 blank-event-czyxd3		
搜索	Q	1 { 2 "headers": {	Contraction of	
空白模版 apig-event-template cts-event-template dds-event-template gaussmongo-event-template		3         "token": "Basic dXNlcjE6cGFzc3dvcmQ="           4         },           5         "queryStringParameters" : {           6         "test": "user@123"           7                     8         }           9         }		
dis-event-template Image-lag kafka-event-template Iogin-security-template Its-event-template				
		创建		

b. 创建测试事件完成后,单击"测试"调试代码。

index.p	×		执行结果 ×	
1 2 3 4 5 6 6 7 8 9 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 23 24	<pre>1 ** codegust fa ** ipper; jon def hadder/event, context;) testParauter = context;getUscotas('test'); userRoke = context;getUscotas('test'); userRoke = context;getUscotas('test'); if event["weatring=aranticestas('test'); if event["weatri</pre>	20	<ul> <li>● (新活金)</li> <li>● (新活金)</li> <li>● (新活金)</li> <li>● (新潟(1))</li> <li>● (1)</li> <li>● (1)<!--</td--><td>), (*) (*) (*)()(*), (*Contracti': (*)(*Set**: **Set**)))* art invoke request 21617tid-des0-4436-dokfa0fta7ba2), variant islett minioria request 21617tid-des0-4436-dokfa0fta7ba2), 21607tid-des0-4436-dokfa0fta7ta2b 21607tid-des0-4436-dokfa0fta7ta2b 1364m 1354m 2160 21</td></li></ul>	), (*) (*) (*)()(*), (*Contracti': (*)(*Set**: **Set**)))* art invoke request 21617tid-des0-4436-dokfa0fta7ba2), variant islett minioria request 21617tid-des0-4436-dokfa0fta7ba2), 21607tid-des0-4436-dokfa0fta7ta2b 21607tid-des0-4436-dokfa0fta7ta2b 1364m 1354m 2160 21
24				

- 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。	
米型	此处选择"前端"。	
函数地址	单击"添加",选择 <mark>已创建函数</mark> 。	
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", 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
衣 /-3	削垢땁直

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 <mark>已创建自定义认证</mark> 。

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"。

- 3. 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。

API_70vi ID: aa61bd0e68bf485da3ba523a447ef1a4		⊙ #10₩8	₫ 没有	⊉ ⊺গ্ৰ	<i>L 编</i> 辑	▶ 语言	6	)現象 +		
GET https://1c9a6e58b1a9484cd aweicloudapis						潮波		×		
Parameters (1) Headers (1)										
参数名	学歌道									
token	Basic dXNIcjE6cGFzc3dvcmQ=									Ū
⊙ 約增屬冷容和										
✓ 満成提示										
请求		喇較性	塛				状态码	200	fel 4	,531 ms
1 Off / Appl/Log factor_athorhestucerMol23 MTM/h.1 Nutri LokeSoleSole Moli LokeSoleSole Moli LokeSoleSoleSole Moli LokeSoleSoleSole Moli LokeSoleSoleSole Moli LokeSoleSoleSole Moli LokeSoleSoleSoleSole Moli LokeSoleSoleSoleSoleSole Moli LokeSoleSoleSoleSole Moli LokeSoleSoleSoleSole Moli LokeSoleSoleSoleSoleSole Moli LokeSoleSoleSoleSoleSole Moli LokeSoleSoleSoleSoleSoleSoleSoleSole Moli LokeSoleSoleSoleSoleSoleSoleSoleSoleSoleSol			<pre>HTTP/11.200 OK Transfer-Encoding_bucked Transfer-Encoding_bucked DeterSat, 20 Ct 2022 07:53:12 Server: apl-sptismic Server: apl-sptemay X-kejg-tatency: 4527 mainten X-kejg-tatency: 4527 mainten X-kegest-Lis Coff4dc2f77d9facd hello backend info</pre>	607 ,limit:100,time main:9999,limit: 0001d623sfbe8b0	1 minute 10000,time:	L second				

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。

\$ cur	-k ->	( GET	"http	s://1		1	api/two_	factor_a	uthorizat	ion?tes	t=user%
40123'	'-H "t	token	: Basi	c dXN	lcjE6	cGFzc3d	vcmQ=" -	H "Host:	1c9a6e58	b1a9484	c8737ec
					huawe	iclouda	pis.com"	-H "X-S	dk-Date:	2022102	9T08021
2Z" -H	I "Auth	noriz	ation:	SDK-	HMAC-	SHA256	Access=c	bbbf0ee6	27c4024bf	c18	1
, Sigr	redHead	lers=	host;t	oken;	x-sdk	-date,	Signatur	e=376666	817679048	19ad3f8	d6b37a5
868058	39cb204	15 d 2				4"					
% To	otal	% R	eceive	d % X	ferd	Averag	e Speed	Time	Time	Time	Curren
t											
						Dload	Upload	Total	Spent	Left	Speed
100	18	0	18	0	0	76	0 -	-::	::	::-	- 76
hello	backer	nd in	fo								

----结束



#### 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> <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 <mark>网关跨VPC开放后端服务和对接Web应用防火墙</mark> WAF。
2021-09-30	第一次正式发布。