

API 网关

最佳实践

文档版本 02
发布日期 2026-06-05



版权所有 © 华为云计算技术有限公司 2026。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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 最佳实践汇总	1
2 开放 API	3
2.1 使用 APIG 专享版开放 CCE 工作负载	3
2.1.1 使用 APIG 专享版开放 CCE 工作负载方案概述	3
2.1.2 使用 APIG 专享版开放 CCE 工作负载资源规划	4
2.1.3 使用 APIG 专享版开放 CCE 工作负载操作流程	5
2.1.4 使用 APIG 专享版开放 CCE 工作负载实施步骤	5
2.1.4.1 准备 CCE 工作负载信息	5
2.1.4.2 方式一：通过创建负载通道的方式开放 CCE 工作负载	6
2.1.4.3 方式二：通过导入 CCE 工作负载的方式开放 CCE 工作负载	9
2.1.4.4（可选）配置工作负载标签实现灰度发布	11
2.2 使用 APIG 专享版开放本地数据中心的服务能力	14
2.3 使用 APIG 专享版跨 VPC 开放后端服务	16
2.3.1 使用 APIG 专享版跨 VPC 开放后端服务方案概述	16
2.3.2 使用 APIG 专享版跨 VPC 开放后端服务资源规划	17
2.3.3 使用 APIG 专享版跨 VPC 开放后端服务操作流程	17
2.3.4 使用 APIG 专享版跨 VPC 开放后端服务实施步骤	18
2.4 使用 APIG 专享版实现 gRPC 服务的路由转发	24
2.4.1 使用 APIG 专享版实现 gRPC 服务的路由转发方案概述	24
2.4.2 使用 APIG 专享版实现 gRPC 服务的路由转发操作流程	25
2.4.3 使用 APIG 专享版实现 gRPC 服务的路由转发实施步骤	25
2.5 使用 APIG 专享版实现 WebSocket 服务的转发	28
2.6 使用 APIG 专享版实现 http 到 https 自动重定向	30
2.6.1 使用 APIG 专享版实现 http 到 https 自动重定向方案概述	30
2.6.2 使用 APIG 专享版实现 http 到 https 自动重定向操作流程	30
2.6.3 使用 APIG 专享版实现 http 到 https 自动重定向实施步骤	31
2.7 使用 APIG 专享版实现不同后端服务的调用	32
2.7.1 使用 APIG 专享版实现不同后端服务的调用方案概述	32
2.7.2 使用 APIG 专享版实现不同后端服务的调用操作流程	32
2.7.3 使用 APIG 专享版实现不同后端服务的调用实施步骤	33
2.8 使用 APIG 专享版对接后端 FunctionGraph	35
2.9 通过 VPCEP 实现跨 VPC 访问 APIG 专享版 NLB 实例开放的 API	39
2.10 通过 NAT 网关实现 APIG 专享版 NLB 实例的公网出口访问	43

3 API 认证	46
3.1 使用 FunctionGraph 服务实现 APIG 的自定义认证.....	46
3.2 使用 APIG 的 APP 认证和自定义认证实现 API 的双重认证.....	51
3.3 配置 APIG 专享版与客户端间的单向认证或双向认证.....	57
4 API 策略	62
4.1 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控.....	62
4.1.1 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控方案概述.....	62
4.1.2 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控操作流程.....	63
4.1.3 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控实施步骤.....	64
4.2 使用 APIG 专享版的 JWT 认证策略实现身份认证和密钥轮转.....	68
5 API 安全	74
5.1 使用 WAF 对 APIG 进行安全防护.....	74
5.2 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击.....	77
5.2.1 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击方案概述.....	77
5.2.2 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击资源规划.....	78
5.2.3 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击操作流程.....	78
5.2.4 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击实施步骤.....	79
5.3 APIG 安全最佳实践.....	81
6 版本迁移	83
6.1 APIG 共享版迁移到专享版.....	83

1 APIG 最佳实践汇总

本文汇总了基于API网关服务（APIG，APIGateway）常见应用场景的操作实践，为每个实践提供详细的方案描述和操作指导，帮助用户轻松构建基于APIG的业务。

表 1-1 APIG 最佳实践一览表

最佳实践	说明
使用APIG专享版开放CCE工作负载	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。
使用APIG专享版开放本地数据中心的服能力	使用专享版API网关为本地数据中心搭建一条与API网关（所绑定的华为云VPC）之间的专线。
使用APIG专享版跨VPC开放后端服务	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，通过跨VPC对接开放后端服务。
使用APIG专享版实现gRPC服务的路由转发	当用户使用gRPC服务时，可以通过API网关创建API，实现gRPC服务的路由转发。
使用APIG专享版实现WebSocket服务的转发	API网关支持WebSocket API，其创建过程和创建HTTP API一致。WebSocket是一种全双工通信协议，建立在单个TCP连接上，允许在客户端和服务器之间进行双向通信。
使用APIG专享版实现http到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，可以使用API网关的重定向功能将API升级为安全的https协议访问，同时兼容已有的http协议。
使用APIG专享版实现不同后端服务的调用	API网关支持定义多个策略后端，通过不同的策略条件，将API请求转发到不同的后端服务中，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”，通过调用前端自定义认证参数，为特殊调用方分配专用的后端服务。
使用APIG专享版对接后端FunctionGraph	创建一个FunctionGraph函数，并将其作为API的后端服务，实现高效集成。

最佳实践	说明
使用FunctionGraph服务实现APIG的自定义认证	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。
使用APIG的APP认证和自定义认证实现API的双重认证	在API网关提供的安全认证模式下，用户可根据业务需求，配置自定义认证实现API的双重认证方式。
配置APIG专享版与客户端间的单向认证或双向认证	API前端定义中的请求协议支持HTTPS时，API所属分组在绑定独立域名后，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，当SSL证书带有CA证书时，默认开启客户端认证即双向认证；反之，开启单向认证。
使用APIG专享版的流量控制2.0策略实现API的精细流控	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。
使用APIG专享版的JWT认证策略实现身份认证和密钥轮转	API网关的JWT认证策略支持从Header、Query、Cookie多种位置设置Token，通过校验Token实现身份认证。用户还可以通过设置JWKS_URI远程服务地址，通过定期更换该地址返回的公钥，实现无缝密钥轮转。
使用WAF对APIG进行安全防护	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。
使用DDoS防护服务为APIG抵御DDoS攻击	当用户在公网中调用APIG上公开的业务API时，会存在DDoS攻击风险，为防范DDoS攻击，华为云提供了DDoS防护服务。
APIG安全最佳实践	本章节介绍APIG使用过程中的安全最佳实践，提供可操作的规范性指导以提升整体安全能力。
APIG共享版迁移到专享版	APIG共享版即将退市，为了避免影响用户的业务，需要将共享版上已有资源迁移到专享版上继续使用。
通过VPCEP实现跨VPC访问APIG专享版NLB实例开放的API	客户端与APIG专享版NLB实例同区域不同VPC时，可通过创建VPC终端节点实现跨VPC访问。
通过NAT网关实现APIG专享版NLB实例的公网出口访问	APIG专享版NLB位于无EIP的私有子网，需配置公网NAT网关的SNAT规则，以实现安全访问互联网后端服务。

2 开放 API

2.1 使用 APIG 专享版开放 CCE 工作负载

2.1.1 使用 APIG 专享版开放 CCE 工作负载方案概述

应用场景

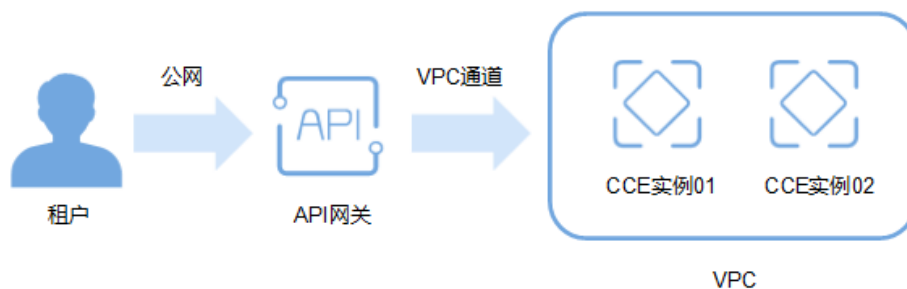
云容器引擎（Cloud Container Engine，即CCE）中的工作负载，以及微服务，可通过API网关将服务能力以API形式对外开放。

开放CCE工作负载支持以下两种方式，推荐使用**方式一**直接创建负载通道的方式开放CCE工作负载。

- 方式一
在API网关中直接创建负载通道，通过负载通道访问CCE工作负载中的实例地址，动态监测工作负载下实例IP地址变化。开放API时使用负载通道访问后端服务，通过API的形式将云容器应用的服务能力开放出来。
- 方式二
一键式导入CCE工作负载，自动生成API和负载通道，API与相应生成的负载通道绑定，动态监测工作负载下实例IP地址变化。通过API的形式开放云容器引擎中的工作负载以及微服务等能力。

方案架构

图 2-1 通过 API 网关访问 CCE 工作负载（由实例组成）



方案优势

- 无需设置弹性公网IP，节省网络带宽成本。
API网关可通过手动创建的负载通道或者导入CCE的工作负载生成的负载通道，访问CCE中工作负载的地址。
- API网关可通过手动创建的负载通道或者导入CCE的工作负载生成的负载通道，动态监测工作负载下所有实例的地址变化，并自动更新到负载通道中。
- 支持通过CCE工作负载标签配置进行灰度发布，完成灰度测试与版本切换。
- 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。

约束与限制

- 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集群所属同一个负载通道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。

2.1.2 使用 APIG 专享版开放 CCE 工作负载资源规划

表 2-1 资源规划

资源	数量
云容器引擎CCE	1
API专享版实例	1

2.1.3 使用 APIG 专享版开放 CCE 工作负载操作流程



1. 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，需要在云容器引擎控制台创建CCE集群（VPC网络模型）或Turbo集群。

2. 开放CCE工作负载

方式一：在API网关中直接创建负载通道并开放API，通过负载通道访问CCE工作负载中的实例地址。

方式二：在API网关中一键式导入CCE工作负载，自动生成API和负载通道，通过负载通道访问CCE工作负载中的实例地址。

3. （可选）配置工作负载标签实现灰度发布

通过CCE工作负载的标签配置，实现灰度发布。灰度发布是服务发布策略之一，旨在通过调整流量分配权重，逐步将流量从旧版本引导到新版本实例上。

2.1.4 使用 APIG 专享版开放 CCE 工作负载实施步骤

2.1.4.1 准备 CCE 工作负载信息

步骤1 创建集群。

1. 登录[云容器引擎控制台](#)，在“集群管理”页面购买CCE Standard集群或CCE Turbo集群。此处选择CCE Standard集群，容器网络模型为“VPC网络”，具体操作步骤请参见[购买CCE集群](#)。
2. 集群创建完成后，记录容器网段。
3. 在APIG专享版实例的“路由”中添加容器网段。
 - a. 进入API网关控制台，在左侧导航栏中“实例管理”。
 - b. 单击对应实例名称，进入实例信息页面。
 - c. 在“路由”区域添加容器网段。

步骤2 创建工作负载。

1. 在云容器引擎控制台的“集群管理”页面，单击已创建的集群名称，进入集群详情。
2. 在左侧导航栏中选择“工作负载”。
3. 单击“创建工作负载”。此处选择“无状态负载 Deployment”负载类型，具体操作步骤请参见《[云容器引擎用户指南](#)》。

您可以在“高级配置 > 标签与注释”中设置“Pod标签”，便于之后根据标签切换工作负载与服务版本。此处为“app=deployment-demo”，“version=v1”。如果您是通过导入YAML创建工作负载，也可以在yaml中添加“Pod标签”。Pod标签的具体使用请参见[设置标签与注释](#)。

在yaml中添加“Pod标签”：

```
spec:
  replicas: 2
  selector:
    matchLabels:
      app: deployment-demo
      version: v1
  template:
    metadata:
      creationTimestamp: null
    labels:
      app: deployment-demo
      version: v1
```

----结束

2.1.4.2 方式一：通过创建负载通道的方式开放 CCE 工作负载**步骤1** 创建负载通道。

1. 进入API网关控制台，在左侧导航栏上方选择实例。
2. 在左侧导航栏中选择“API管理 > API策略”。
3. 在“负载通道”页签中单击“创建负载通道”。
 - a. 基本信息配置。

表 2-2 基本信息配置

参数	配置说明
通道名称	填写负载通道名称，根据规划自定义。此处填写“VPC_demo”。
端口	填写已创建工作负载的容器端口，指工作负载中pod里业务直接对外开放的接口。此处填写“80”，80端口默认为http协议端口。
分发算法	此处选择“加权轮询”。通过分发算法确定请求被发送到哪台主机。结合弹性服务器权重值，将请求轮流转发到每一台服务器。
通道类型	此处选择“微服务”。

- b. 微服务配置。

表 2-3 微服务配置

参数	配置说明
微服务类型	默认选择“云容器引擎CCE”。
集群	选择 已创建的集群 。
命名空间	选择已创建集群中的命名空间，此处选择“default”。
工作负载类型	此处选择“无状态负载 Deployment”，与已创建的工作负载类型一致。
服务标识名	此处选择 已创建的工作负载 中的Pod标签“app”和“deployment-demo”，指定工作负载。
服务标识值	

c. 服务器分组配置。

表 2-4 服务器分组配置

参数	配置说明
服务器分组名称	此处填写“server_group_v1”。
权重分配	此处填写“1”。
后端服务端口	此处填写“80”，与已创建工作负载中的容器端口一致。
描述	此处填写“Pod标签version值为v1的服务器分组”。
标签	此处选择 已创建的工作负载 中的Pod标签“version=v1”。

d. 健康检查配置。

表 2-5 健康检查配置

参数	配置说明
协议	默认为“TCP协议”。
检查端口	填写为通道中后端服务器端口。
正常阈值	默认为“2”。判定VPC通道中主机正常的依据：连续检查x成功，x为您设置的正常阈值。
异常阈值	默认为“5”。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。
超时时间	默认为“5”。检查期间，无响应的的时间。
间隔时间	默认为“10”。连续两次检查的间隔时间。

- e. 单击“完成”。
在负载通道列表中，单击**负载通道名称**可查看创建的负载通道详情。

步骤2 开放API。

1. 创建API分组。
 - a. 在左侧导航栏中选择“API管理 > API分组”。
 - b. 单击“创建API分组 > 直接创建”。
 - c. 填写API分组信息后，单击“确定”。
2. 创建API并绑定已创建的负载通道。
 - a. 单击已创建的API分组名称，进入分组详情页面，在“API运行”页签中单击“创建API > 创建API”。
 - b. 配置前端信息后，单击“下一步”。

表 2-6 前端配置

参数	配置说明
API名称	填写API名称。
所属分组	API所属分组，此处选择 已创建的API分组 。
URL	<ul style="list-style-type: none">▪ 请求方法：接口调用方式，此处选择“ANY”。▪ 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。默认网关响应为“default”。
匹配模式	此处选择“前缀匹配”。
安全认证	选择API认证方式，此处选择“无认证”。（无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用）

- c. 配置后端信息后，单击“下一步”。

表 2-7 HTTP/HTTPS 类型定义后端服务

参数	配置说明
负载通道	选择“使用”负载通道访问后端服务。

参数	配置说明
URL	<ul style="list-style-type: none">请求方法：接口调用方式，此处选择“ANY”。请求协议：选择协议类型，此处选择“HTTP”。负载通道：填写已创建的负载通道。路径：后端服务的路径。

- d. 定义返回结果后，单击“完成”。
3. 调试API。
在“API运行”页签中，单击“调试”，进入调试页面。再次单击“调试”，响应结果中返回状态码“200”，表示调试成功，执行下一步。否则，请参考[错误码](#)章节处理。
4. 发布API。
在“API运行”页签中，单击“发布最新版本”，默认选择“RELEASE”环境，单击“确定”。发布按钮左上角的感叹号消失，表示发布成功，执行下一步。否则，根据错误信息提示修改。

步骤3 调用API。

1. 绑定独立域名。
在API分组详情页面单击“分组信息”页签。调试域名仅供开发测试使用，且每天最多访问1000次，因此用户需要绑定独立域名来访问分组内的API。
单击“绑定独立域名”，绑定已注册好的公网域名。绑定域名具体操作请参见[绑定域名](#)章节。
2. 复制API的URL到浏览器进行调用。
在“API运行”页面，复制API的URL。打开浏览器，在地址栏输入API的URL进行访问。显示创建API时填写的成功响应示例，表示调用成功。

图 2-2 复制 URL 示例



至此，实现了通过创建负载通道的方式开放CCE工作负载。

----结束

2.1.4.3 方式二：通过导入 CCE 工作负载的方式开放 CCE 工作负载

步骤1 导入CCE工作负载。

1. 进入API网关控制台，在左侧导航栏上方选择实例。
2. 在左侧导航栏中选择“API管理 > API分组”。
3. 单击“创建API分组 > 导入CCE工作负载”。
 - a. 填写导入CCE工作负载的信息。

表 2-8 工作负载信息配置

参数	配置说明
所属分组	工作负载所属分组，此处默认为“生成新的分组”。
集群	选择 已创建的集群 。
命名空间	选择已创建集群中的命名空间，此处选择“default”。
工作负载类型	此处选择“无状态负载 Deployment”，与已创建的工作负载类型保持一致。
服务标识名	此处选择 已创建的工作负载 中的Pod标签“app”和“deployment-demo”，指定工作负载。
服务标识值	
标签	自动选择工作负载的另外一个Pod标签“version=v1”。

- b. 配置生成的API信息。

表 2-9 配置生成的 API 信息

参数	配置说明
请求协议	API请求协议，默认选择“HTTPS”协议。
请求路径前缀	API的请求路径的前缀匹配字符串，可按需手动填写，默认为“/”。此处填写为“/”。
端口	此处填写“80”，与已创建工作负载中的容器端口一致。
安全认证	默认为“无认证”。（无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用）
支持跨域CORS	默认不开启。
后端超时（ms）	填写后端超时时间默认为“5000”。

4. 单击“完成”。CCE工作负载导入成功，并生成API分组、API和负载通道。

步骤2 查看生成的API及相应负载通道。

1. 查看生成的API。
 - a. 单击**已创建的API分组名称**，进入“API运行”页签，可查看API的名称、请求方法、发布状态等。

- b. 单击“后端配置”页签，查看API绑定的负载通道。
2. 查看生成的负载通道。
 - a. 在左侧导航栏中“API管理 > API策略”。
 - b. 在“负载通道”页签中，查看负载通道。
3. 确认生成的负载通道与API所绑定的负载通道一致后，执行下一步。否则，重复步骤1。

步骤3 开放API。

通过“导入CCE工作负载”开放CCE工作负载时，已经自动创建API分组与API。因此，只需要将API发布到对应的环境中即可。

1. 调试API。

在“API运行”页签中，单击“调试”，进入调试页面。再次单击“调试”，响应结果中返回状态码“200”，表示调试成功，执行下一步。否则，请参考[错误码](#)章节处理。
2. 发布API。

在“API运行”页签中，单击“发布最新版本”，默认选择“RELEASE”环境，单击“确定”。发布按钮左上角的感叹号消失表示发布成功，执行下一步。

步骤4 调用API。

1. 绑定独立域名。

在API分组详情页面单击“分组信息”页签。调试域名仅供开发测试时使用，且每天最多访问1000次，因此用户需要绑定独立域名来访问分组内的API。

单击“绑定独立域名”，绑定已注册好的公网域名。绑定域名具体操作请参见[绑定域名](#)章节。
2. 复制API的URL到浏览器进行调用。

在“API运行”页面，复制API的URL。打开浏览器，在地址栏输入API的URL进行访问。显示创建API时填写的成功响应示例，表示调用成功。

图 2-3 复制 URL 示例



至此，实现了通过一键式“导入CCE工作负载”的方式来开放CCE工作负载服务的能力。

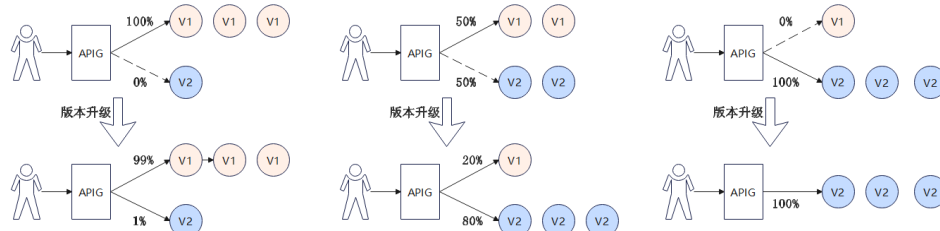
----结束

2.1.4.4（可选）配置工作负载标签实现灰度发布

灰度发布是服务发布策略之一，旨在通过调整流量分配权重，逐步将流量从旧版本引导到新版本实例上。服务发布升级过程中可以逐步验证版本是否符合预期，如果版本符合预期，则可以逐渐加大新版本实例流量占比，减小旧版本实例流量占比，直至将

新版本服务权重增加到100，旧版本服务权重减少至0，完成从旧版本到新版本服务的引流。

图 2-4 灰度发布示意图



云容器引擎CCE工作负载根据Pod标签的标签选择器配置实现灰度发布，实现原理请参见[使用Service实现简单的灰度发布和蓝绿发布](#)，帮助用户实现新功能的快速上线与验证，进而完成流量引导与服务器切换。

下文完成特性从V1版本到V2版本的切换，保证服务升级的过程中流量平稳切换，通过灰度发布逐步将流量从V1版本迁移到V2版本。

步骤1 新建工作负载并设置“Pod标签”，且app值与已创建工作负载的app值一致。具体步骤请参考[已创建的工作负载](#)。

您可以在“高级配置 > 标签与注释”中设置“Pod标签”，此处为“app=deployment-demo”，“version=v2”。如果您是通过导入YAML创建工作负载，也可以在yaml中添加“Pod标签”。

步骤2 调整Pod标签为“version= v1”的服务器分组的权重。

1. 在API网关控制台的左侧导航栏上方选择实例。
2. 在左侧导航栏中选择“API管理 > API策略”。
3. 在“负载通道”页签中，单击[已创建的负载通道名称](#)。
4. 在“后端服务器地址”区域，单击“编辑”。
5. 将“权重分配”改为“100”，并单击“确定”。

权重分配即为流量转发的权重。此时，全部流量都将转发到服务器分组“server_group_v1”中的实例ip上。

步骤3 创建Pod标签为“version= v2”的服务器分组并设置权重分配。

1. 在“后端服务器地址”区域，单击“创建服务器分组”。

表 2-10 服务器分组配置

参数	配置说明
服务器分组名称	此处填写为“server_group_v2”。
权重分配	此处填写为“1”。
后端服务端口	此处填写为“80”。
标签	此处选择Pod标签“version=v2”

2. 单击“确定”。

步骤4 刷新后端服务器地址。

通过刷新页面来刷新后端服务器的地址，负载通道将自动监测工作负载下的实例IP地址并动态添加到后端服务地址中。如下图所示，根据标签“app=deployment-demo”，“version=v2”能够自动匹配到已创建工作负载的实例ip，即后端服务器地址。

图 2-5 自动匹配工作负载的实例 ip



此时流量权重分配到“server_group_v1”分组的比例为100/101（服务器分组权重/服务器分组权重之和），分配到“server_group_v2”分组的比例为1/101（服务器分组权重/服务器分组权重之和），将有小部分请求被引流到“server_group_v2”分组的最新版本上。

图 2-6 单击页面右上角编辑查看



步骤5 验证新特性通过灰度发布到V2版本是否运行稳定。

您可以自行验证新版本功能是否符合预期，如果符合预期请执行步骤6。否则，新特性发布失败。

步骤6 逐步调整不同版本服务器分组的权重配置。

逐步减小“server_group_v1”分组的权重，增大“server_group_v2”分组的权重。重复步骤5~步骤6，直到“server_group_v1”分组的权重为“0”，“server_group_v2”分组的权重为“100”。



如图，表示请求转发时，分配到服务器分组“server_group_v1”的比例为0，服务器分组“server_group_v2”的比例为100%，即请求将全部转发到服务器分组“server_group_v2”上，完成从“version=v1”的工作负载“deployment-demo”到“version=v2”的工作负载“deployment-demo2”之间的切换，进而实现了新特性从V1版本到V2版本的灰度发布。（注意：请求转发的流量权重分配比例可自行设置与调整）

步骤7 删除Pod标签为“version= v1”的服务器后端分组server_group_v1。

现已将全部流量引导到“version= v2”的服务器后端分组的后端服务地址上，因此，可将V1版本所在服务器后端分组删除。

1. 进入API网关控制台的负载通道详情页面，在“后端服务器地址”区域逐个将V1版本后端服务器地址列表中的IP地址移除。
2. 然后单击“后端服务器地址”区域右侧的“移除”，删除“version= v1”的服务器后端分组。

保留Pod标签为“version= v2”的服务器后端分组“server_group_v2”分组。

----结束

2.2 使用 APIG 专享版开放本地数据中心的服务能力

应用场景

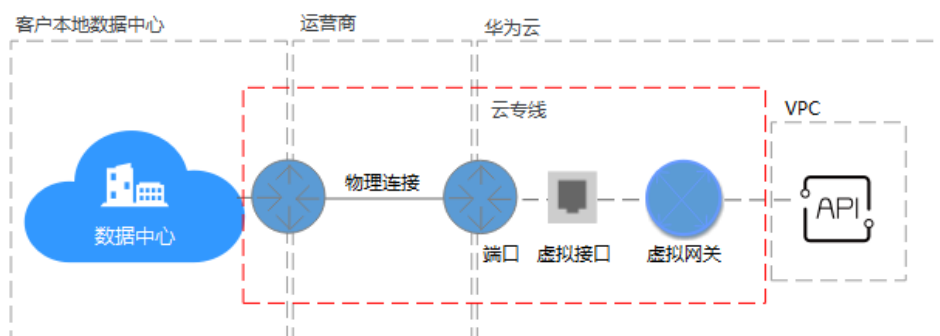
API网关的后端服务有3类部署形态：

- 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（所绑定的华为云VPC）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的实践步骤。

方案架构

图 2-7 使用云专线连通客户本地数据中心与华为云专享版 API 网关



连通云专线与 API 网关

步骤1 创建VPC。如果已有VPC，可跳过此步骤。

具体操作请参考《[虚拟私有云 VPC](#)》。

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。

- 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。

图 2-8 创建 VPC 示例参考

基本信息

区域

名称 vpc1

IPv4网段 192.168.0.0 / 16

企业项目 default

高级配置(可选)

子网设置 1

子网名称 subnet-3a1e

可用区 可用区1 (center) 可用区2 (center) 可用区3 (center) 可用区4 (center)

子网IPv4网段 192.168.0.0 / 24 可用IP数: 251

子网IPv6网段(可选) 开启IPv6

关联路由表 默认

步骤2 创建专享版API网关。

具体请参考[购买专享版API网关](#)章节。

步骤3 购买云专线。

购买一条连接本地数据中心到华为云API网关（所绑定的虚拟私有云）的云专线，请按以下操作顺序执行：

1. 购买物理连接接入

即购买一条连接本地数据中心与华为云的运营商线路。建议您选择“一站式接入”，华为云负责施工工程。

如果已有数据中心到华为云的物理连接，可直接使用。

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。

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。

4. 配置本地路由

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。

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。

步骤5 连通云专线与API网关后，然后[使用专享版API网关开放API](#)。

----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](#)》。

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。

2.3 使用 APIG 专享版跨 VPC 开放后端服务

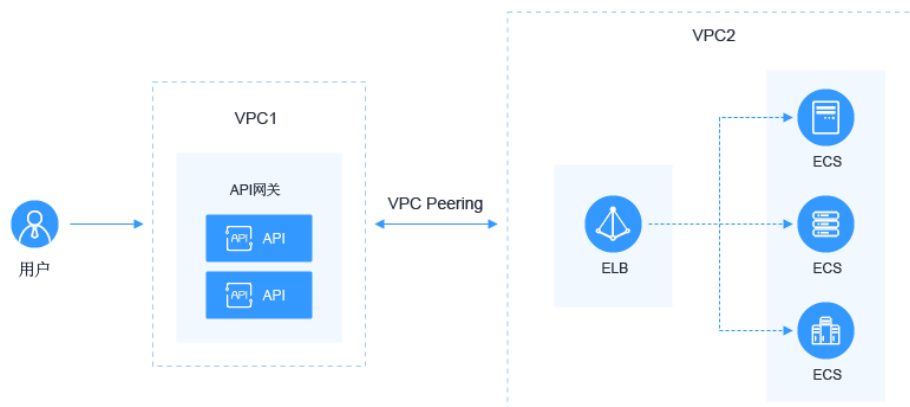
2.3.1 使用 APIG 专享版跨 VPC 开放后端服务方案概述

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 2-9 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

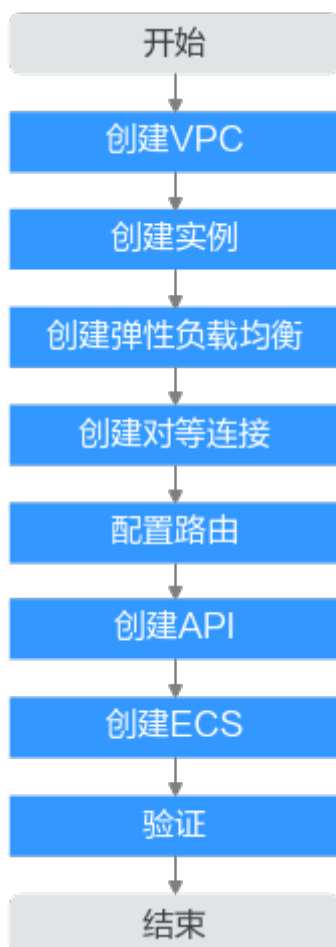
VPC1、VPC2、APIG实例系统VPC网段不能重叠。关于APIG实例VPC网段规划，请参考表2-13。

2.3.2 使用 APIG 专享版跨 VPC 开放后端服务资源规划

表 2-11 资源规划

资源	数量（个）
VPC	2
API专享版实例	1
ELB	1
ECS	1

2.3.3 使用 APIG 专享版跨 VPC 开放后端服务操作流程



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为购买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。

2.3.4 使用 APIG 专享版跨 VPC 开放后端服务实施步骤

创建 VPC

步骤1 登录[虚拟私有云控制台](#)。

步骤2 在“虚拟私有云”页面，单击“创建虚拟私有云”，请参考[表2-12](#)和[表2-13](#)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: [下拉菜单]

名称: VPC1

IPv4网段: 192.168.0.0 / 16

企业项目: default

子网设置 1

子网名称: subnet-df38

可用区: 可用区1 (center) | 可用区2 (center) | 可用区3 (center) | 可用区4 (center)

子网IPv4网段: 192.168.0.0 / 24 可用IP数: 251

子网IPv6网段(可选): 开启IPv6

关联路由表: 默认

子网创建完成后，子网网段无法修改。因此创建之前，请您查看子网规划建议，合理规划子网网段。

表 2-12 配置信息

参数	配置说明
区域	选择所在的区域，此处选择“华北-北京四”。
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”。
可用区	选择子网所属可用区，此处选择“可用区1”。
名称	创建虚拟私有云的同时创建一个默认子网。

表 2-13 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3 单击“立即创建”。

步骤4 重复**步骤2~步骤3**，创建“VPC2（后端应用所在VPC）”。

---结束

创建实例

步骤1 进入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”。

表 2-14 实例信息

参数	配置说明
计费模式	选择实例的计费模式，此处选择“按需计费”。
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。
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”。

参数	配置说明
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，勾选用户协议和隐私政策的阅读并同意声明。开始创建实例，界面显示创建进度。

---结束

创建 ELB

步骤1 进入弹性负载均衡控制台。

步骤2 在“我的ELB”页面，单击“购买弹性负载均衡”。

步骤3 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[负载均衡器](#)章节。

表 2-15 弹性负载均衡参数

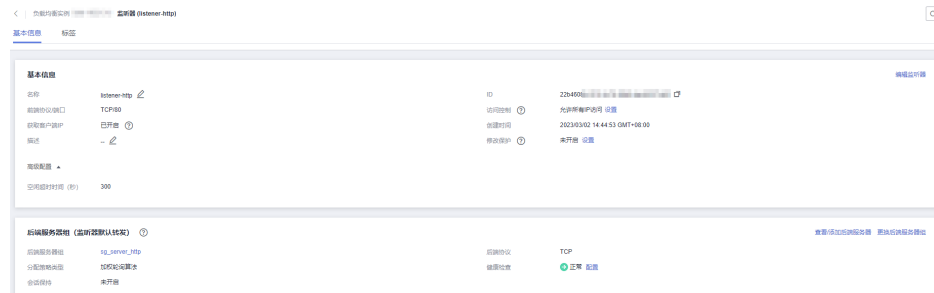
参数	配置说明
实例类型	选择实例的规格类型。
计费模式	此处默认选择“按需计费”。
区域	选择实例所在的区域，且与VPC2同一区域。
可用区	选择实例所在的可用区，此处选择“可用区1”。
名称	填写弹性负载均衡的名称，根据规划自定义。
企业项目	选择实例所属的企业项目，此处默认选择“default”。
规格	此处规格类型默认选择“固定规格”，规格默认选择“应用型”和“网络型”。
网络类型	此处默认选择“IPv4私网”。
所属VPC	所属虚拟私有云，选择已创建的虚拟私有云“VPC2”。
前端子网	选择子网。

步骤4 单击“立即购买”。

步骤5 确认信息无误后，单击“提交”。

步骤6 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 2-10 进入监听器详情，查看监听器基本信息和后端服务器组信息

---结束

创建对等连接

步骤1 在网络控制台的左侧导航栏选择“虚拟私有云 > 对等连接”。

步骤2 单击“创建对等连接”，配置对等连接。

表 2-16 对等连接配置

参数	配置说明
区域	选择区域，且与VPC1同区域。
对等连接名称	填写对等连接的名称，根据规划自定义。
本端VPC	已创建的虚拟私有云“VPC1”。
账户	此处默认“当前账户”。
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3 单击“确定”。

步骤4 在弹框中单击“立即添加”，进入对等对接详情页面。

步骤5 在“关联路由”页签中单击“添加路由”。

1. 在弹窗中填写路由信息。

表 2-17 本端和对端的路由信息

参数	说明
本端路由	
虚拟私有云	已创建的虚拟私有云“VPC1”。
路由表	VPC1的路由表。
目的地址	为ELB详情页面，“基本信息”页签中的“服务地址”。
对端路由	
虚拟私有云	已创建的虚拟私有云“VPC2”。
路由表	VPC2的路由表。
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。

2. 单击“确定”。

----结束

配置路由

步骤1 返回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 在API网关控制台的左侧导航栏选择“API管理 > API列表”，单击“创建API > 创建API”。

步骤2 配置前端信息后，单击“下一步”。

表 2-18 前端配置

参数	配置说明
API名称	填写API名称。
所属分组	默认“DEFAULT”。

参数	配置说明
URL	<ul style="list-style-type: none">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”。
安全认证	选择API认证方式，此处选择“无认证”。（无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用）

步骤3 配置后端信息后，单击“下一步”。

表 2-19 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	<ul style="list-style-type: none">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4 定义返回结果后，单击“完成”。

----结束

创建 ECS

步骤1 进入弹性云服务器控制台。

步骤2 单击“购买弹性云服务器”。

步骤3 基础配置后，单击“下一步：网络配置”。

表 2-20 基础配置

参数	配置说明
计费模式	选择“按需计费”。
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。

参数	配置说明
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。
虚拟私有云	选择 已创建的虚拟私有云 “VPC2”。
主网卡	选择 已创建的虚拟私有云 的子网。
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”。
云服务器名称	填写弹性云服务器名称。
登录凭证	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。
企业项目	此处选择“default”。

步骤4 同意协议声明后，单击“立即购买”。

----结束

调试 API

步骤1 在**弹性负载均衡**的监听器详情中，单击“查看/添加后端服务器”。

步骤2 在“后端服务器”页签中，添加**云服务器**。

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。否则，请参考**错误码**章节处理。

----结束

2.4 使用 APIG 专享版实现 gRPC 服务的路由转发

2.4.1 使用 APIG 专享版实现 gRPC 服务的路由转发方案概述

应用场景

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

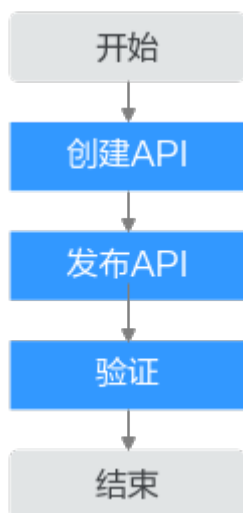
口定义语言（Interface Definition Language，缩写IDL），同时底层的消息交换格式也是使用protobuf。

当用户使用gRPC服务时，可以通过API网关创建API，实现gRPC服务的路由转发。

约束与限制

由于GRPCS协议的约束，gRPC类型的API不支持导入、导出、调试。

2.4.2 使用 APIG 专享版实现 gRPC 服务的路由转发操作流程



1. **创建API**
创建gRPC类型的API，前后端协议均为GRPCS。
2. **发布API**
将gRPC类型的API发布到环境上。
3. **验证**
使用gRPC客户端测试gRPC服务可用性，如果服务端正常返回响应，则表示gRPC服务可用。

2.4.3 使用 APIG 专享版实现 gRPC 服务的路由转发实施步骤

前提条件

- 客户端与服务端均为gRPC类型。
- 服务端已定义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接口服务的文件，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，充当客户端和服务端之间通信的合同。

创建 API

- 步骤1 登录[API网关控制台](#)。
- 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”。

步骤4 单击“创建API > 创建GRPC API”。更多详细指导，请参见[创建GRPC API](#)。

步骤5 根据下表参数说明，配置前端信息。配置完成后，单击“下一步”。

表 2-21 前端配置

参数	配置说明
API名称	填写API名称。
所属分组	API所属分组，此默认“DEFAULT”。
URL	<ul style="list-style-type: none">请求方法：接口调用方式，默认“POST”。请求协议：选择API请求协议，默认“GRPCS”。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“/helloworld.Greeter”。请求路径请参考proto文件，helloworld为包名，Greeter服务名。
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”。
匹配模式	此处选择“前缀匹配”。
安全认证	选择API认证方式，此处选择“无认证”。（无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用）

步骤6 根据下表参数说明，配置后端信息。配置完成后，单击“完成”。

表 2-22 后端配置

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	<ul style="list-style-type: none">请求方法：接口调用方式，默认“POST”。请求协议：选择协议类型，默认“GRPCS”。后端服务地址：填写后端服务地址及端口。路径：后端服务的路径。此处填写“/”。

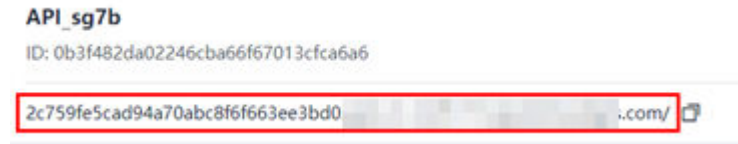
---结束

发布 API

步骤1 在“API运行”页面，选择已创建的API，单击“发布最新版本”。

说明

在“API运行”页面中，API的URL不显示调用方法以及协议，仅显示域名和路径部分。当发送gRPC请求时，填入域名部分即可。



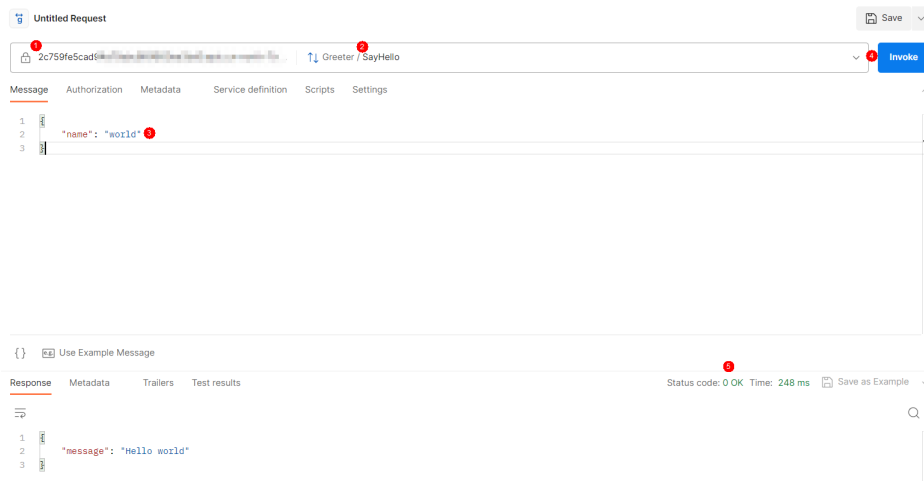
步骤2 选择API的发布环境，并填写发布说明。

步骤3 单击“确定”，API发布成功后，发布按钮左上角的红色感叹号消失。

----结束

验证

使用接口测试工具调用已创建的API，或者在客户端调用已创建的API。



步骤1 填写API所属分组的调试域名。

步骤2 导入服务端的proto文件。

此处的proto文件如下：

```
syntax = "proto3";
package helloworld;
// The greeting service definition.
service Greeter {
  // Sends a greeting
  rpc SayHello (HelloRequest) returns (HelloReply) {}
}
// The request message containing the user's name.
message HelloRequest {
  string name = 1;
}
// The response message containing the greetings
message HelloReply {
  string message = 1;
}
```

- helloworld: 包名
- Greeter: 服务名

- SayHello: 方法名
- HelloRequest: 请求体
- HelloReply: 响应体

步骤3 参考proto文件在“message”区域中填写API的Request。

```
{  
  "name": "world"  
}
```

步骤4 单击“Invoke”发送请求。

步骤5 在“Response”区域中返回API的Response，且状态码显示“0 OK”，表示调用成功。

----结束

2.5 使用 APIG 专享版实现 WebSocket 服务的转发

应用场景

API网关支持WebSocket API，其创建过程和创建HTTP API一致。WebSocket是一种全双工通信协议，建立在单个TCP连接上，允许在客户端和服务端之间进行双向通信。WebSocket的设计旨在解决HTTP协议在实时性和交互性方面的不足。它广泛应用于实时聊天、在线游戏、金融行业的实时数据更新等场景。

约束与限制

- WebSocket API不支持APIG控制台页面中的调试功能。
- WebSocket API受API超时时间的限制，如果当前WebSocket连接空闲时间超过了配置的超时时间，并且没有ping/pong保活，则连接会被自动断开。

前提条件

准备一个已做ping/pong保活的WebSocket服务后端。

操作步骤

- 步骤1** 登录[API网关控制台](#)。
- 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”。
- 步骤4** 单击“创建API > 创建API”，配置前端信息。

表 2-23 前端配置

参数	配置说明
API名称	填写API名称，例如“API01”。
所属分组	API所属分组，此处默认“DEFAULT”。

参数	配置说明
URL	<ul style="list-style-type: none">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，此处默认“HTTPS”，对应wss协议。如果选择“HTTP”，对应ws协议。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“/hello”。
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。此处默认“default”。
安全认证	选择API认证方式，此处选择“无认证”。（无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用）

步骤5 单击“下一步”，配置后端信息。

表 2-24 后端配置

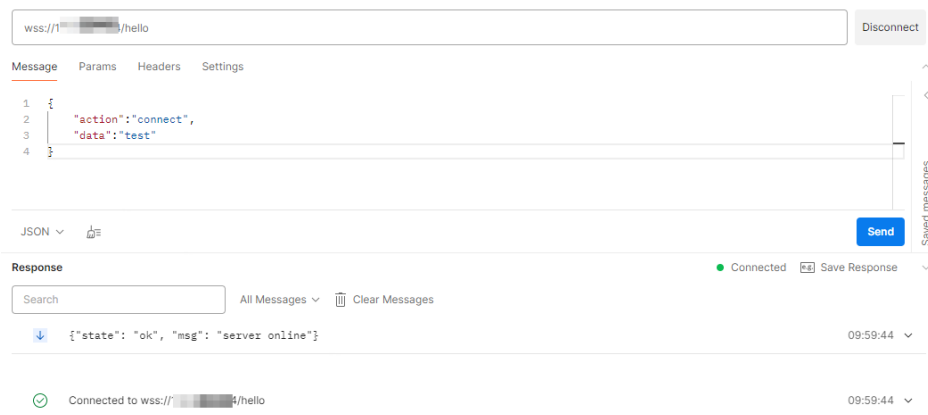
参数	配置说明
后端服务类型	此处选择“HTTP&HTTPS”。
负载通道	此处选择“不使用”负载通道访问后端服务。 WebSocket后端也可以通过负载通道配置，本实践中选择“不使用”负载通道为例进行说明。
URL	<ul style="list-style-type: none">请求方法：接口调用方式，此处选择“GET”。请求协议：选择协议类型，如果后端服务是ws协议类型，此处选择“HTTP”；如果后端服务是wss协议类型，此处选择“HTTPS”。后端服务地址：此处填写WebSocket后端服务地址及端口。路径：后端服务的路径。此处填写“/”。
后端超时(ms)	调整后端超时时间，使其长于ping/pong心跳时间。例如，ping/pong心跳时间为20s，那么超时时间可以设置区间为（20000ms，60000ms】。

步骤6 后端信息配置完成后，单击“完成”。

步骤7 API创建完成后，在“API运行”页签中，单击“发布最新版本”，发布API。

步骤8 使用接口测试工具调用API。

本实践通过IP调用DEFAULT分组下的API，输入“wss://IP地址/hello”发送请求即可。其中，IP地址为APIG控制台“实例信息”中的弹性IP地址。



----结束

2.6 使用 APIG 专享版实现 http 到 https 自动重定向

2.6.1 使用 APIG 专享版实现 http 到 https 自动重定向方案概述

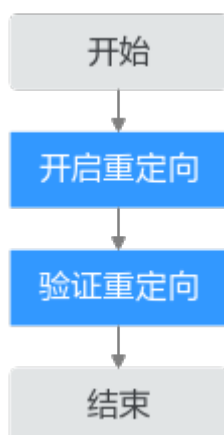
应用场景

API网关支持http重定向到https功能。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，可以使用API网关的重定向功能将API升级为安全的https协议访问，同时兼容已有的http协议。（2022年11月30日之后创建的实例支持http重定向到https）

约束与限制

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。

2.6.2 使用 APIG 专享版实现 http 到 https 自动重定向操作流程



1. 开启重定向

开启重定向功能的API的前端请求协议必须为“HTTPS”或“HTTP&HTTPS”。

2. 验证重定向

验证重定向功能是否生效。

2.6.3 使用 APIG 专享版实现 http 到 https 自动重定向实施步骤

前提条件

- 已创建API，API前端配置的请求协议必须选择“HTTPS”或“HTTP&HTTPS”。
- API已发布。
- API所属API分组已绑定独立域名和SSL证书。

API的相关操作及绑定域名和SSL证书，请参见《[API网关用户指南](#)》。

开启重定向

步骤1 登录[API网关控制台](#)。

步骤2 在左侧导航栏选择“API管理 > API分组”。

步骤3 单击分组名称，进入API所属分组的详情页面。

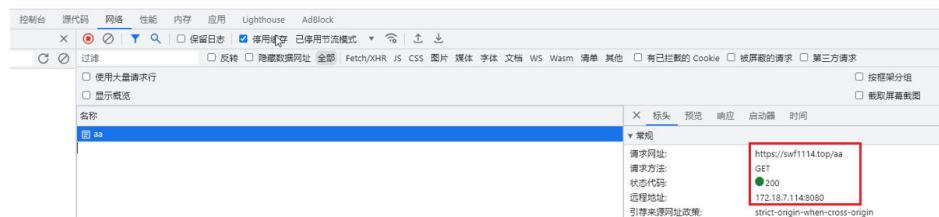
步骤4 在“分组信息”页签的“域名管理”区域，找到已绑定的独立域名，在“支持http to https自动重定向”列开启重定向功能。

----结束

验证重定向是否生效

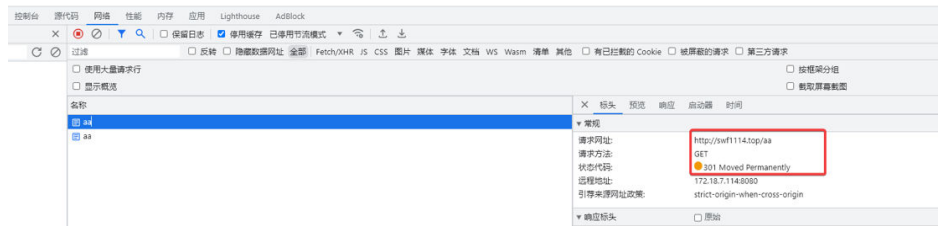
步骤1 通过浏览器采用https协议调用API。

1. 在浏览器的地址栏中输入“https://API请求路径”后回车。
2. 在键盘上按F12。
3. 在“网络”页签中状态码显示“200”表示调用成功。



步骤2 通过浏览器采用http协议调用API。

1. 在浏览器的地址栏中输入“http://API请求路径”后回车。
2. 在键盘上按F12。
3. 在“网络”页签中状态码显示“301”表示重定向成功。



----结束

2.7 使用 APIG 专享版实现不同后端服务的调用

2.7.1 使用 APIG 专享版实现不同后端服务的调用方案概述

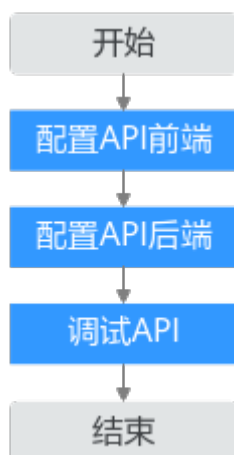
应用场景

API网关支持定义多个策略后端，通过不同的策略条件，将API请求转发到不同的后端服务中，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”，通过调用前端自定义认证参数，为特殊调用方分配专用的后端服务。本方案以“系统参数-前端认证参数”为例，讲述用户如何通过设置“系统参数-前端认证参数”策略条件将API请求转发到指定的后端服务中。

约束与限制

- 添加策略后端前，前端的安全认证方式应选“自定义认证”或使用双重认证（APP认证或IAM认证）。
- 添加策略后端前，必须定义一个默认后端，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。
- “系统参数-前端认证参数”策略条件的“条件值”只支持字符串、整数、布尔值三种类型的值。
- 一个API最多定义5个策略后端。

2.7.2 使用 APIG 专享版实现不同后端服务的调用操作流程



1. 配置API前端

在API的前端设置页面选择安全认证方式为“自定义认证”或使用双重认证（APP认证或IAM认证），并选择指定的自定义认证对象，如果没有，则需要创建自定义认证。

2. 配置API后端

在API的后端设置页面添加策略后端，策略条件的条件来源选择“系统参数-前端认证参数”，并完善参数名称、条件类型、条件值等，其中参数名称和条件值要与前端自定义认证函数返回值中context字段下的键值对一致。

3. 调试API

调试API，观察是否成功调用到已添加的策略后端。

2.7.3 使用 APIG 专享版实现不同后端服务的调用实施步骤

前提条件

1. 已创建自定义认证函数，如果未创建请[创建函数](#)章节创建，并且在函数的返回值中已设置context字段，字段中包含键值对。其中键值对的值只支持字符串、布尔、整型三种数值类型，键值对对应“系统参数-前端认证参数”策略条件的参数名称和条件值。

图 2-11 自定义认证函数



```
1 # -*- coding:utf-8 -*-
2 import json
3 def handler (event, context):
4     resp = {
5         "statusCode": 200,
6         "body": json.dumps({
7             "status": "allow",
8             "context": {
9                 "test": "123",
10                "authstatus1": False,
11                "authstatus2": True,
12                "num": 1001
13            }
14        }),
15        "headers": {
16            "Content-Type": "application/json"
17        }
18    }
19    print(resp)
20    return json.dumps(resp)
```

2. 已创建前端自定义认证。如果未创建，请参考[自定义认证](#)章节创建。

配置 API 前端

- 步骤1 登录[API网关控制台](#)。
- 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”。
- 步骤4 单击“创建API > 创建API”，配置前端信息。

表 2-25 前端配置

参数	配置说明
API名称	填写API名称。
所属分组	API所属分组，此处默认“DEFAULT”。
URL	<ul style="list-style-type: none">请求方法：接口调用方式，默认“GET”。请求协议：选择API请求协议，默认“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“/1234”。
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“自定义认证”。
自定义认证	选择 前提条件 中已创建的自定义认证。

----结束

配置 API 后端

步骤1 前端设置完成后，单击“下一步”，进入后端设置页面。

设置“默认后端”的后端服务类型为“Mock”类型，Mock返回结果填写“默认后端”。


步骤2 单击  根据下表添加策略后端。

表 2-26 配置策略后端

参数	配置说明
后端策略名称	填写后端策略名称。
后端服务类型	此处选择“Mock”。
Mock返回结果	此处填写“策略后端”。
策略条件	<ul style="list-style-type: none">条件来源：选择“系统参数-前端认证参数”。参数名称：填写前提条件已创建自定义认证函数返回体中context字段下的“authstatus1”。条件类型：选择“相等”。条件值：填写前提条件已创建自定义认证函数返回体中context字段下的“False”。

约束与限制

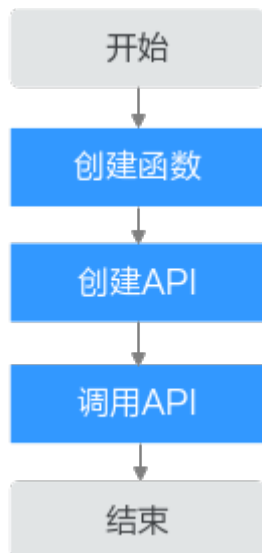
如果当前环境中未部署FunctionGraph服务，则后端服务类型FunctionGraph不可用。

资源规划

表 2-27 资源规划

资源	数量
FunctionGraph	1
APIG专享版实例	1

操作流程



1. 创建函数

在使用FunctionGraph类型定义后端服务之前，需要先在FunctionGraph服务中创建一个函数作为自己的后端服务。

2. 创建API

创建一个API，后端类型定义为FunctionGraph类型。

3. 调用API

验证APIG对接后端FunctionGraph是否成功。

使用 APIG 专享版对接函数后端实施步骤

创建函数

步骤1 登录[函数 workflow 控制台](#)页面。

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 2-28 配置函数

参数	配置说明
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。
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	如果您的企业有多个项目，建议选择相应的项目以实现资源的逻辑隔离。此处默认“default”。
委托	用户委托函数工作流去访问其他的云服务。此处默认“未使用任何委托”。
运行时	此处以“Python 3.9”语言为例。

步骤4 单击“创建函数”。创建完成后，检查函数列表中是否出现新创建的函数。

步骤5 进入函数详情，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):
    return {
        "statusCode": 200,
        "body": json.dumps("Hello from FunctionGraph"),
        "headers": {
            "Content-Type": "application/json"
        }
    }
```

步骤6 单击“测试”，配置测试事件。

步骤7 在测试事件的“事件模板”中选择“API网关服务（APIG专享版）”，根据实际情况修改后保存测试模板。

步骤8 单击“测试”。执行结果为“执行成功”时，表示测试成功。

----结束

创建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，确保与创建的函数位于同一区域。

步骤3 在左侧导航栏选择“API管理 > API列表”。

步骤4 单击“创建API > 创建API”，根据下表参数说明，配置前端信息。

表 2-29 前端配置

参数	配置说明
API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。

参数	配置说明
所属分组	API所属分组，此处默认“DEFAULT”。
URL	请求方法：接口调用方式，默认“GET”。 请求协议：选择API请求协议，默认“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“/fg”。
网关响应	网关响应配置用于定义API请求失败时的默认响应，建议根据业务需求进行调整。 此处默认为“default”。
安全认证	选择API认证方式，此处选择“无认证”。无认证模式，安全级别低，所有用户均可访问，不推荐在实际业务中使用。在实际业务中，建议使用更安全的认证方式，如APP认证或IAM认证等，以提高API的安全性。

步骤5 前端设置完成后，单击“下一步”，进入后端设置页面。

步骤6 在后端配置页面，选择API的“后端服务类型”为“FunctionGraph”。

步骤7 根据下表配置说明，配置后端信息。

表 2-30 FunctionGraph 类型后端服务配置

参数	配置说明
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”，添加已创建的函数。
版本或别名	选择函数的版本或别名，此处选择“通过版本选择 > latest”。
网络架构	选择函数网络架构，此处选择“V2”。
调用类型	选择函数的调用类型，可选择同步调用“Synchronous”和异步调用“Asynchronous”，此处选择“Synchronous”。
后端超时(ms)	后端服务请求的超时时间，可填写范围1ms~60000ms，此处默认5000ms。

步骤8 单击“完成”，完成创建API。创建完成后，检查API列表中是否出现新创建的API。

步骤9 在“API运行”页面，单击“调试”，调试已创建的API。再次单击“调试”。

响应结果中显示“200 OK”，表示API调用成功，否则，请参考[错误码](#)章节处理。

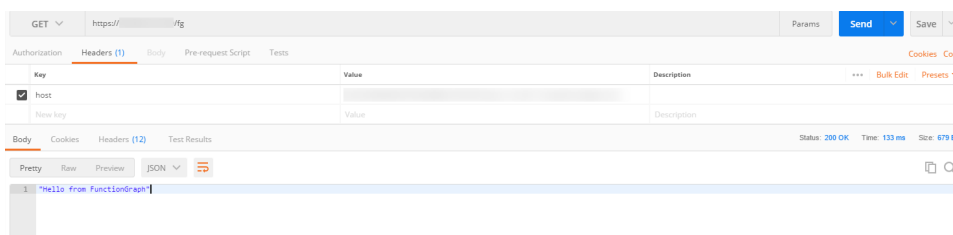
步骤10 在“API运行”页面，单击“发布最新版本”发布API。

发布环境默认选择“RELEASE”环境，单击“确定”。发布按钮左上角的感叹号消失，表示发布成功。

----结束

调用API

使用接口测试工具调用API，显示返回函数文本“Hello from FunctionGraph”，表示调用成功。



2.9 通过 VPCEP 实现跨 VPC 访问 APIG 专享版 NLB 实例开放的 API

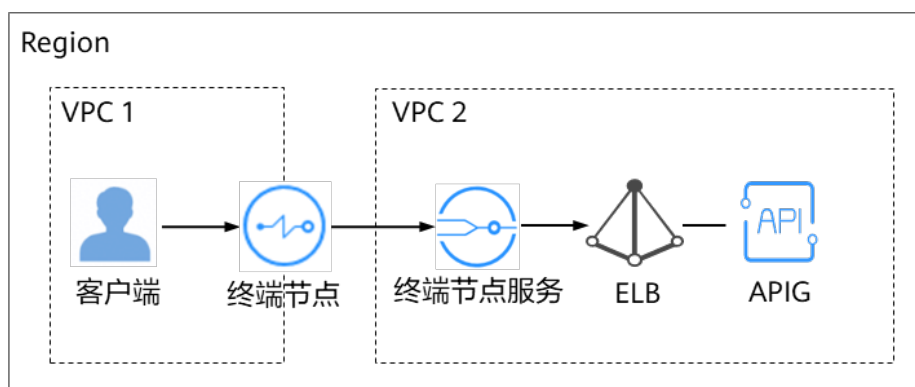
应用场景

客户端和APIG专享版NLB实例在同一区域的不同VPC中，由于VPC之间逻辑隔离，客户端和NLB实例不能直接通信。您可以通过以下任意一个方式实现跨VPC访问：

- 创建VPC对等连接，将两个VPC的网络打通，实现跨VPC访问。具体步骤请参考[对等连接](#)。
- 利用VPC终端节点在不同VPC间建立跨VPC的连接通道，实现客户端通过内网访问NLB实例开放的API。

本实践主要介绍通过VPC终端节点实现跨VPC访问的方法。

方案架构



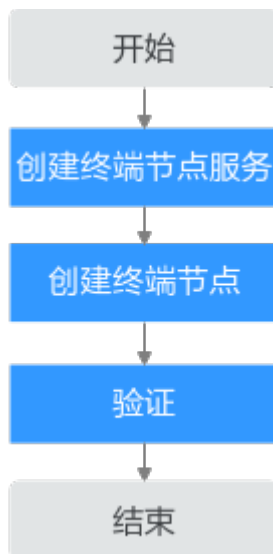
客户端在VPC1通过终端节点访问VPC2中的终端节点服务，该服务将请求转发给ELB，再通过ELB转发到APIG，从而实现跨VPC的安全高效访问。

前提条件

- 已创建APIG专享版NLB系列规格实例。如果未创建，请[创建APIG实例](#)。NLB系列规格实例受限使用，如需使用，请[提交工单](#)申请扩展。
- 已创建API。如果未创建，请[创建API](#)。

操作流程

本实践主要介绍同区域“同账号”的多个VPC中的云资源（即后端资源）如何实现跨VPC通信。同区域不同账号的多个VPC中的云资源（即后端资源）如何实现跨VPC通信，请参考[配置跨VPC通信的终端节点（不同账号）](#)。



1. 创建终端节点服务

为实现跨VPC通信，需将目标VPC内的云资源（即后端资源）配置为终端节点服务，使同一区域内其他VPC的终端节点可通过私网IP访问该服务。

2. 创建终端节点

完成终端节点服务创建后，需在访问方VPC内创建终端节点，作为租户跨VPC访问的流量入口，专门用于对接目标终端节点服务。

3. 验证

通过跨VPC调用API的方式，验证终端节点与终端节点服务的连通性及服务可用性，确认跨VPC通信是否生效。

创建终端节点服务

APIG专享版NLB实例以“弹性负载均衡”作为流量入口，因此本场景下的后端资源特指该弹性负载均衡。

步骤1 进入[终端节点服务](#)页面。

步骤2 在“终端节点服务”页面，单击“创建终端节点服务”。

进入“创建终端节点服务”页面，请根据下表参数说明配置参数，其余参数保持默认配置即可。

表 2-31 终端节点服务参数说明

参数	配置说明
区域	选择终端节点服务所在区域，与APIG实例所属区域保持一致。
名称	填写终端节点服务的名称。根据规划自定义，此处填写“VPCEP_demo”。
网络类型	选择终端节点服务的网络类型，此处默认选择“IPv4”。
虚拟私有云	选择终端节点服务所属虚拟私有云。建议与后端资源保持一致。
后端资源类型	此处默认选择“弹性负载均衡”，实际提供服务的后端资源。
选择负载均衡	选择绑定NLB实例对应的弹性负载均衡名称。
端口映射	终端节点服务与终端节点建立连接关系，进行通信。此处协议默认为“TCP”，服务端口填写“80”，终端端口填写“80”。

步骤3 单击“立即创建”。

----结束

创建终端节点

步骤1 进入[终端节点](#)页面。

步骤2 在“终端节点”页面，单击“购买终端节点”。

进入“购买终端节点”页面，请根据下表参数说明配置参数，其余参数保持默认配置即可。

表 2-32 终端节点参数说明

参数	配置说明
区域	选择终端节点所在区域，与APIG实例所属区域保持一致。
服务类别	此处默认选择“按名称查找服务”，连接的终端节点服务为用户私有服务。
服务名称	输入已创建的终端节点服务名称，单击“验证”。 <ul style="list-style-type: none">若显示“已找到服务”，继续后续操作。若显示“未找到服务”，请检查“区域”是否和终端节点服务所在区域一致或输入的“服务名称”是否正确。

参数	配置说明
创建内网域名	通过域名的方式访问终端节点，此处选择“创建内网域名”。 <ul style="list-style-type: none">终端节点创建完成后，即可通过内网域名直接访问终端节点。关联终端节点服务类型为“接口”时，需要在页面设置此选项。
终端节点类型	根据选择关联的终端节点服务的类型展示。此处选择关联接口型终端节点服务，默认展示“接口终端节点”。
实例类型	默认选择“专业型”。专业型终端节点是新上线终端节点实例类型。
网络类型	此处默认选择“IPv4”。
虚拟私有云	此处选择NLB实例的虚拟私有云。
子网	此处选择NLB实例的子网。
IPv4地址	终端节点的IPv4地址。此处默认选择“自动分配IPv4地址”。

步骤3 单击“立即购买”，进行规格确认。

规格确认无误，单击“提交”，任务提交成功。

步骤4 如果终端节点状态为“已接受”，表示终端节点已成功连接至终端节点服务；如果终端节点状态为“待接受”，表示要连接的终端节点服务开启了“连接审批”功能，需要先进行审批，操作如下：

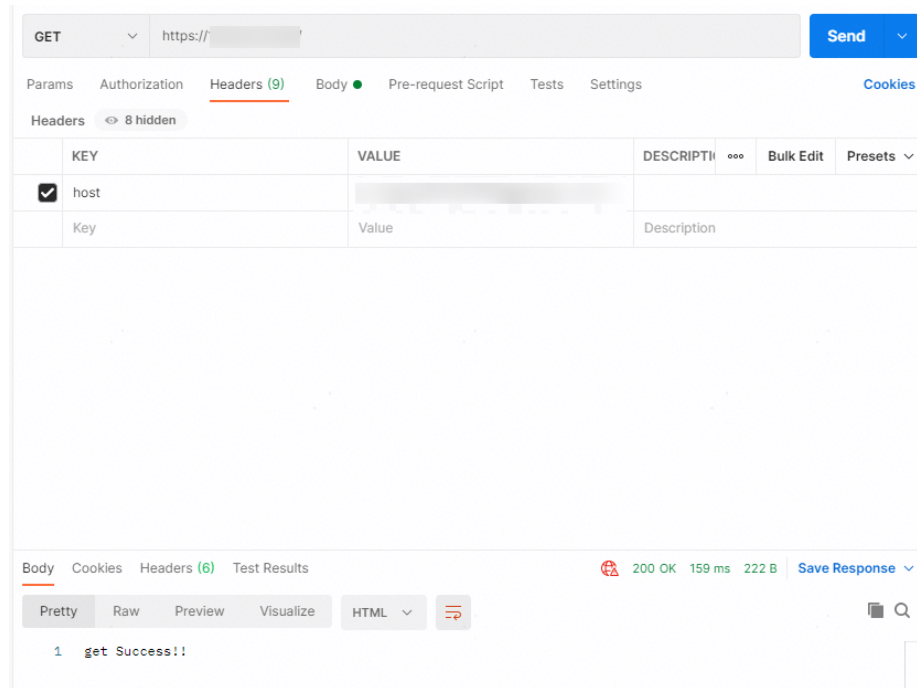
1. 单击对应的终端节点服务名称，进入终端节点服务详情页面。
2. 在终端节点服务详情页面，单击“连接管理”。
3. 在连接管理页面的“操作”栏下，单击“接受”。
4. 返回终端节点列表查看终端节点状态变为“已接受”，表示终端节点已成功连接至终端节点服务。

完成上述终端节点服务与终端节点配置后，即完成通过VPC终端节点（VPCEP）实现云内跨VPC与实例之间的连通性。

----结束

验证

使用接口测试工具调用API，IP填写创建终端节点时设置的“IPv4地址”。状态码显示“200”表示调用成功。

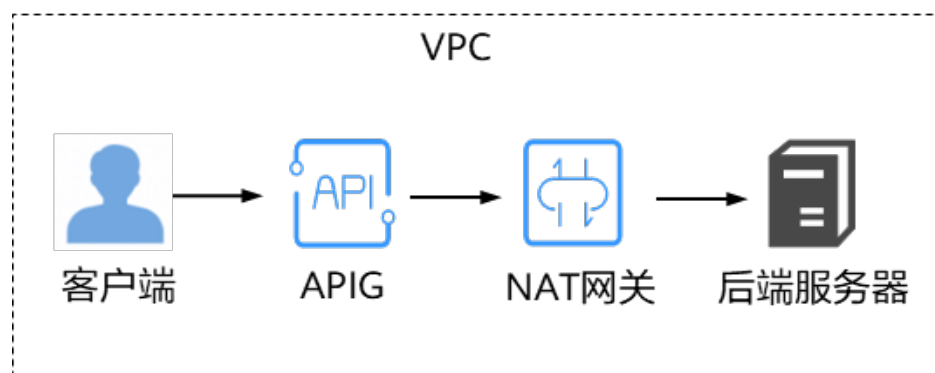


2.10 通过 NAT 网关实现 APIG 专享版 NLB 实例的公网出口访问

应用场景

APIG专享版NLB实例部署在无弹性公网IP（EIP）的私有子网中，因此访问公网后端服务需要配置公网NAT网关实现。通过配置公网NAT网关的SNAT规则，可实现实例安全、可控地访问互联网。

方案架构



客户端通过私有连接访问VPC内的APIG，APIG通过公网出口访问后端服务则经由NAT网关出站，全程保持安全隔离。

前提条件

- 已创建APIG专享版NLB系列规格实例。如果未创建，请[创建APIG实例](#)。NLB系列规格实例受限使用，如需使用，请[提交工单](#)申请扩展。

- 已创建API。如果未创建，请[创建API](#)。

创建 NAT 网关

为解决私有子网内NLB实例的公网访问需求，需创建公网NAT网关并配置SNAT规则，以此为NLB实例提供安全可控的公网出口，实现对公网后端服务的访问。

步骤1 进入[购买公网NAT网关](#)页面。

步骤2 在“购买公网NAT网关”页面，请根据下表参数说明配置参数，其余参数保持默认配置即可。

表 2-33 公网 NAT 网关参数说明

参数	配置说明
区域	选择公网NAT网关所在的区域，与APIG实例所属区域保持一致。
规格	选择公网NAT网关的规格，根据实际情况选择，建议选择“中型”及以上。
名称	填写公网NAT网关的名称。根据规划自定义，此处填写“public-nat-01”。
虚拟私有云	公网NAT网关所属的VPC，选择NLB实例所属VPC。 VPC仅在购买公网NAT网关时可以选择，后续不支持修改。
子网	公网NAT网关所属VPC中的子网，选择NLB实例所属子网。 <ul style="list-style-type: none">• 子网至少有一个可用的IP地址。• 子网仅在购买公网NAT网关时可以选择，后续不支持修改。• 本子网仅为系统配置NAT网关使用，NAT网关对整个VPC生效，需要在购买后继续添加规则，才能够连通Internet。
企业项目	企业项目与NLB实例的负载均衡的VPC企业项目一致。

步骤3 单击“立即购买”，在“规格确认”页面，您可以再次核对公网NAT网关信息。

确认无误后，单击“提交”，开始创建公网NAT网关。

步骤4 添加SNAT规则。

1. 在公网NAT网关页面，单击已创建的NAT网关名称。
2. 在“SNAT规则”页签中，单击“添加SNAT规则”。
请根据下表参数说明配置参数，其余参数保持默认配置即可。

表 2-34 SNAT 参数说明

参数	说明
使用场景	在使用SNAT访问公网的场景下，此处选择“虚拟私有云”。 表示虚拟私有云中的云主机使用SNAT规则访问公网。
网段	通过配置虚拟私有云子网中的某个网段，使该网段中的云主机通过SNAT方式访问公网。 此处默认“使用已有”，下拉选择子网网段。
公网IP类型	用来访问公网的IP，此处默认“弹性公网IP”，并选择一个弹性公网IP。

3. 单击“确定”

----结束

验证

本实践通过直接调用 API 的访问地址（URL）进行测试，验证实例与公网后端服务的连通性。

在APIG的“调试”页面向已创建的API的完整URL发送请求，其中该API的后端服务地址配置为目标业务系统的公网IP。成功收到响应即表明公网出口链路畅通，实例可正常访问外部公网服务。

3 API 认证

3.1 使用 FunctionGraph 服务实现 APIG 的自定义认证

应用场景

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。

操作流程



1. **编写自定义认证函数**
创建一个函数作为用户自己的认证服务。
2. **创建自定义认证**
在APIG中创建一个自定义认证，将函数服务接入APIG。
3. **创建自定义认证的API**
创建一个自定义认证方式的API。
4. **设置错误响应**
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。
5. **映射后端参数**
添加系统参数，将函数返回的context信息传到后端。
6. **验证**
调用API，观察是否成功返回函数的context信息。

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[创建用于前端自定义认证的函数](#)。

根据下表参数说明，在函数工作流页面创建一个函数。

表 3-1 函数信息配置

参数	配置说明
选择创建方式	默认“创建空白函数”。
函数类型	默认“事件函数”。
区域	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。
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	选择Python 3.6。

函数创建完成后，进入函数详情。在“代码”页签，将以下代码复制到index.py中（如果您使用的是专享版网关，并且实例支持authorizer_context_support_num_bool特性，那么context中的value的类型可以为boolean类型或number类型）。

```
# -*- 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 dXN****cmQ=:
        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",
                    "authorizer_success": "false"
                }
            })
        }
}
```

创建自定义认证

在API网关控制台的“API策略 > 自定义认证”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

* 认证名称

* 类型 前端 后端

* 函数地址 [添加](#)

* 版本或别名

* 缓存时间(秒)

* 宽松模式

身份来源

参数位置	参数名	操作
+ 添加身份来源		

是否发送body

用户数据
0/2,048

注意： 用户数据会明文展示所输入信息，请防止信息泄露。

创建自定义认证的 API

在API网关控制台的“API列表”页面，创建API，具体步骤请参见[创建API](#)。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。

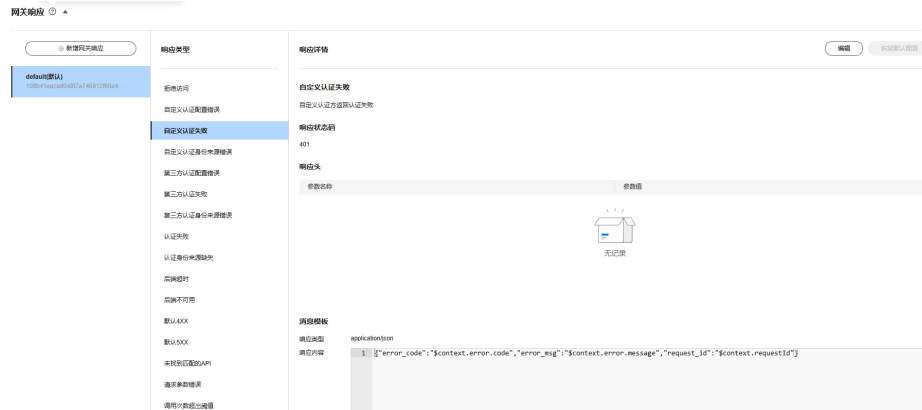
设置错误响应

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（如果您使用的是专享版网关，并且实例支持authorizer_context_support_num_bool特性，那么context中的value的类型可以为boolean类型或number类型），需要修改网关响应模板。在API所在分组中，“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（引用变量为boolean类型或number类型时，变量不需要加双引号）：

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



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\",\"authorizer_success\":\"false\"}
```

映射后端参数

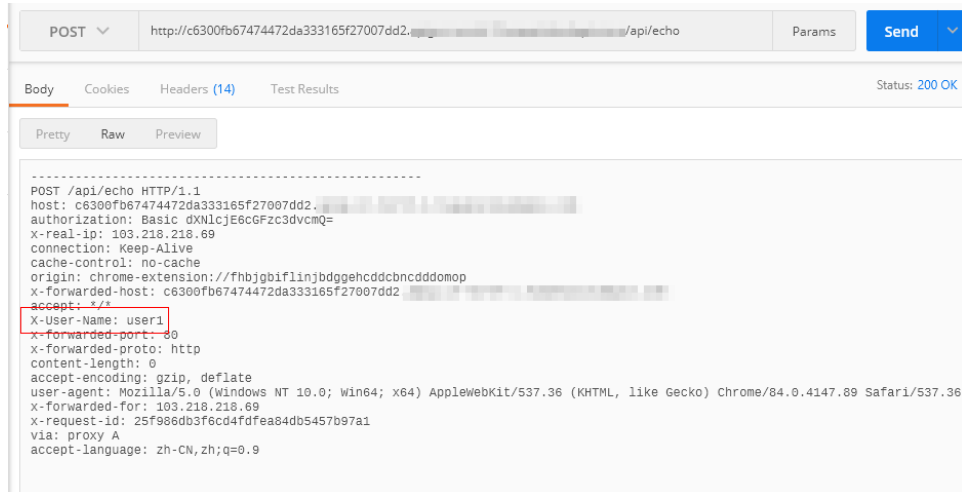
如果认证通过，函数返回的context信息，可以传到后端，配置方式如下：

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。



验证

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。



3.2 使用 APIG 的 APP 认证和自定义认证实现 API 的双重认证

应用场景

双重认证指用户根据业务需求自定义API认证策略，再结合APP认证/IAM认证，从而实现API的双重认证方式，保障API的安全性。本文以API前端认证使用APP认证和自定义认证结合场景为例，具体说明如何创建使用双重认证的API。

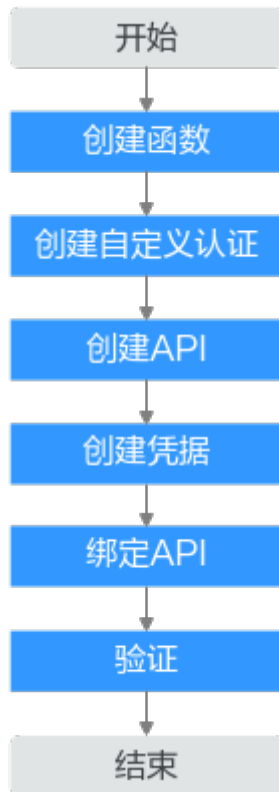
方案优势

在API网关提供的安全认证模式下，用户可根据业务需求，灵活实现自定义认证，保障API的安全性。

约束与限制

API网关支持的自定义认证依赖于函数 workflow 服务，创建自定义认证前，需要先创建函数。

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。

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”。

1. 根据下表，填写函数信息后，单击“创建函数”。

表 3-2 函数信息配置

参数	配置说明
选择创建方式	默认“创建空白函数”。
函数类型	默认“事件函数”。
区域	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。
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	选择Python 3.9。

- 函数创建完成后，进入函数详情。在“设置”页签的左侧导航栏中选择“环境变量”，根据下表参数说明，单击“编辑环境变量 > 添加环境变量”。

表 3-3 设置环境变量

参数	配置说明
键	环境变量的名称，此处添加“token”和“test”两个环境变量。token用于Header身份验证，test参数用于Query参数查询。
值	环境变量的值，token值填写为“Basic dXNlcjE6cGFzc3dvcmQ=”，test填写为“user@123”。
加密参数	开启加密参数后，环境变量的值将以“*”号加密显示，参数传输过程中键值也处于加密状态。对于敏感数据token值，开启加密参数选项。

编辑环境变量

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

- 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”。代码编写请参考[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)
```

4. 配置测试事件并调试代码，然后部署。

- a. 在下拉框中选择“配置测试事件”并配置。将以下代码设置为测试事件。测试事件的参数值与环境变量中的参数值需要保持一致。

```
{
  "headers": {
    "token": "Basic dXNlcjE6cGFzc3dvcmQ="
  },
  "queryStringParameters": {
    "test": "user@123"
  }
}
```

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 (20)

搜索

普通事件模板

空白模板

登录安全实时分析

图片分类

图片鉴黄

语音识别

* 事件名称: blank-event-czyxd3

```
1 {
2   "headers": {
3     "token": "Basic dXNlcjE6cGFzc3dvcmQ="
4   },
5   "queryStringParameters": {
6     "test": "user@123"
7   }
8 }
9 }
```

取消

创建

- b. 创建测试事件完成后，单击“测试”调试代码。如下图，表示代码调试成功。

```

1 # -*- coding:utf-8 -*-
2 import json
3 def handler(event, context):
4     testParameter = context.getUserData("test");
5     userToken = context.getUserData("token");
6     if event["headers"].get("token") == userToken and event["queryStringParameters"].get
7
8     resp = {
9         "statusCode": 200,
10        "body": json.dumps({
11            "status": "allow",
12            "context": {
13                "user": "auth success"
14            }
15        })
16    }
17 else:
18     resp = {
19         "statusCode": 403,
20         "body": json.dumps({
21             "status": "deny",
22         })
23     }
24     return json.dumps(resp)

```

执行结果 X

```

函数返回
{
  "statusCode": 200,
  "body": "{\"status\": \"allow\", \"context\": {\"user\": \"auth success\"}}"
}

日志
2022-11-04T05:29:01Z Start invoke request 216171db-0e00-4d34-9c9f-f68f1ca7ca2b; version: latest
2022-11-04T05:29:01Z Finish invoke request 216171db-0e00-4d34-9c9f-f68f1ca7ca2b; duration: 1.554ms, billing duration: 2ms, memory used: 28.524MB, billing memory: 120MB

执行摘要
请求ID: 216171db-0e00-4d34-9c9f-f68f1ca7ca2b
调用内容: 120 MB
执行时间: 1.554 ms
调用账单内存: 28.524 MB
账单时间: 2 ms

```

c. 调试成功后，单击“部署代码”。

步骤2 进入API网关控制台页面，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 3-4 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。
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 > 创建API”。

1. 根据下表参数，配置前端信息。

表 3-5 前端配置

参数	配置说明
API名称	填写API名称。
所属分组	API所属分组，此处默认“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”。

参数	配置说明
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。选择已创建自定义认证。

- 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”。

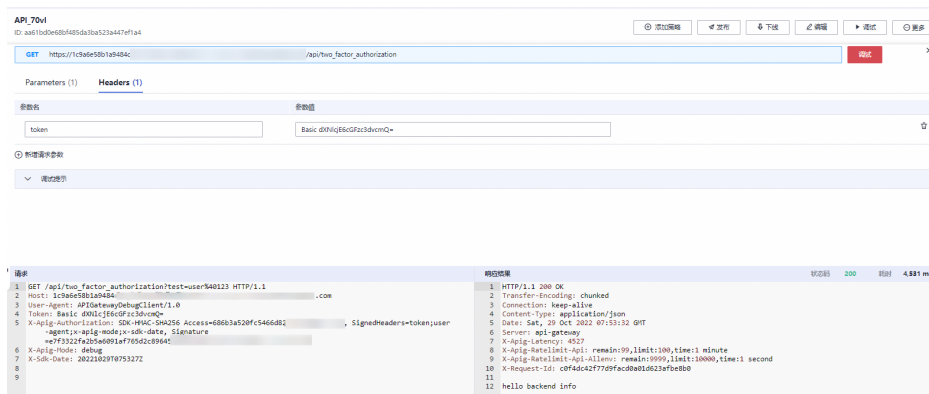
步骤5 绑定API。

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，服务器返回200认证通过。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。

```

$ curl -k -X GET "https://1c9a6e58b1a9484c8737ec22" -H "Host: 1c9a6e58b1a9484c8737ec22" -H "Authorization: SDK-HMAC-SHA256 Access=cbbbf0ee627c4024bfc188680589cb2045d4" -H "token: Basic dXNlcjE6cGFzc3dvcmQ=" -H "X-Sdk-Date: 20221029T080212Z" -H "X-Request-Id: c0f4dc42f779fac0a0102337e800"
% Total % Received % Xferd Average Speed Time Time Time Current
0 0 0 0 0 0 0 0 0 0 0 0
100 18 0 18 0 0 0 76 0 0 0 76
hello backend info

```

----结束

3.3 配置 APIG 专享版与客户端间的单向认证或双向认证

应用场景

API前端定义中的请求协议支持HTTPS时，API所属分组在绑定独立域名后，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，当SSL证书带有**CA证书**时，默认开启客户端认证即双向认证；反之，开启单向认证。

- 单向认证：客户端与服务端连接时，客户端需要校验服务端SSL证书合法性。
- 双向认证：客户端与服务端连接时，除了客户端需要校验服务端SSL证书合法性，服务端也需要校验客户端SSL证书合法性。

操作流程



APIG专享版支持单向认证和双向认证两种认证方式，两种认证方式开启认证的流程相同，下面描述单向认证流程，双向认证具体操作请参考[双向认证](#)。

1. **创建SSL证书**
SSL证书是进行数据传输加密和身份证明的证书。
2. **绑定域名**
将API所属的分组与已备案且解析的独立域名绑定。
3. **绑定证书**
将独立域名和已创建的SSL证书绑定。
4. **调用API**
验证API是否调用成功。

单向认证

步骤1 登录API网关控制台。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 创建SSL证书。

1. 在左侧导航栏选择“API管理 > API策略”。
2. 在“SSL证书管理”页签中，单击“创建SSL证书”。

表 3-6 配置单向认证的证书信息

参数	配置说明
证书名称	填写证书名称。
可见范围	此处选择“当前实例”。
证书内容	-----Start certificate----- MIICXglBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZlbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrCerTaRyG9op3OSh... -----End certificate-----
密钥	-----Start RSA private key----- MIICXglBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZlbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrCerTaRyG9op3OSh... -----End RSA private key-----
CA	单向认证无需配置CA证书。

3. 单击“确定”创建完成。

步骤4 绑定域名。

1. 在左侧导航栏选择“API管理 > API分组”。
2. 单击API所属分组名称，进入分组详情。
3. 在“分组信息”页签中单击“绑定独立域名”。

表 3-7 配置独立域名

参数	配置说明
域名	填写已备案的域名。
支持最小TLS版本	此处选择“TLS1.2”。
支持http to https自动重定向	默认关闭。

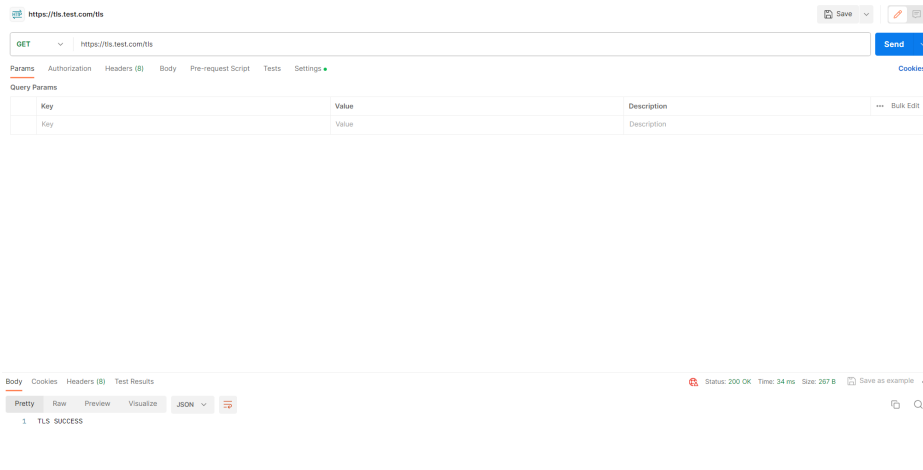
4. 单击“确定”。

步骤5 绑定证书。

1. 在已绑定独立域名所在行单击“选择SSL证书”。
2. 选择已创建的证书单击“确定”。单向认证时，确保客户端认证为关闭状态。

步骤6 调用API。

使用接口测试工具调用API，状态码为“200”表示调用成功。否则，请参考[错误码](#)章节处理。



----结束

双向认证

步骤1 在“SSL证书管理”页签中，单击“创建SSL证书”。

表 3-8 配置双向认证的证书信息

参数	配置说明
证书名称	填写证书名称。
可见范围	此处选择“当前实例”。
证书内容	填写证书内容。 -----Start certificate----- MIICXgIBAAKBgQC6ndRH5Dv5TcZiVzT6qF iaMGy61ZlbUrmBhUn61vMdvOHmtblST+fSl ZheNacv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----
密钥	填写密钥。 -----Start RSA private key----- MIICXgIBAAKBgQC6ndRH5Dv5TcZiVzT6qF iaMGy61ZlbUrmBhUn61vMdvOHmtblST+fSl ZheNacv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End RSA private key-----

参数	配置说明
CA	配置双向认证，此处需要填写CA证书内容。 CA证书配置完成后，将独立域名与此SSL证书绑定，并开启客户端认证。 -----Start certificate----- MIICXglBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZlbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrCerTaRyG9op3OSh... -----End certificate-----

步骤2 单击“确定”创建完成。

步骤3 绑定域名。

1. 在左侧导航栏选择“API管理 > API分组”。
2. 单击API所属分组名称，进入分组详情。
3. 在“分组信息”页签中单击“绑定独立域名”。

表 3-9 配置独立域名

参数	配置说明
域名	填写已备案的域名。
支持最小TLS版本	此处选择“TLS1.2”。
支持http to https自动重定向	默认关闭。

4. 单击“确定”。

步骤4 绑定证书。

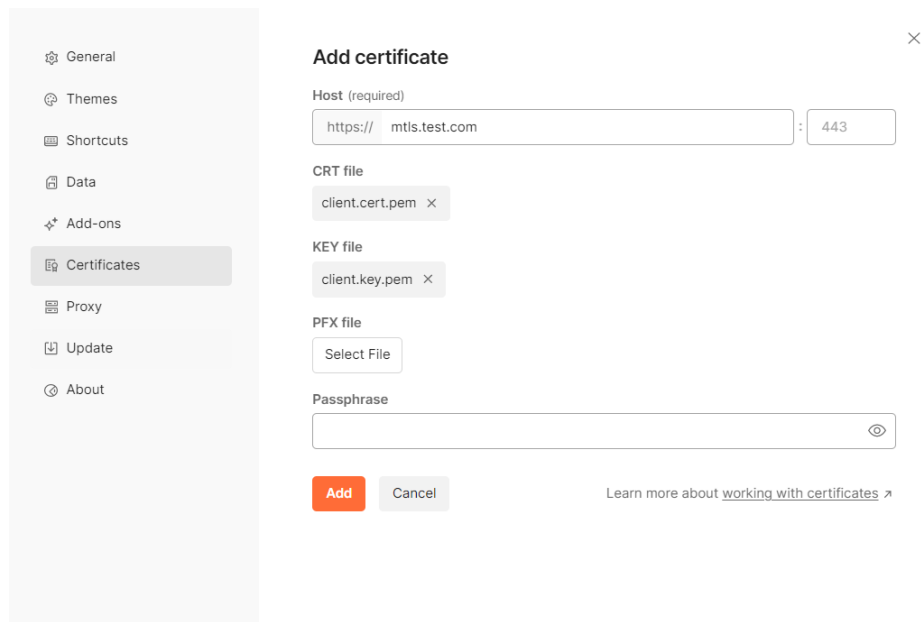
1. 在已绑定独立域名所在行单击“选择SSL证书”。
2. 选择已创建的证书并勾选“开启客户端认证”，单击“确定”。

步骤5 调用API。

使用接口测试工具调用API，状态码为“200”表示调用成功。否则，请参考[错误码](#)章节处理。

由于开启了双向认证，因此在访问API时需要配置客户端证书。

如果使用Postman调用API，则需要在Setting界面的Certificates配置项中添加Client certificates，上传客户端证书以及密钥。



----结束

4 API 策略

4.1 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控

4.1.1 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控方案概述

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提供了传统流量控制策略，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流量控制2.0策略，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

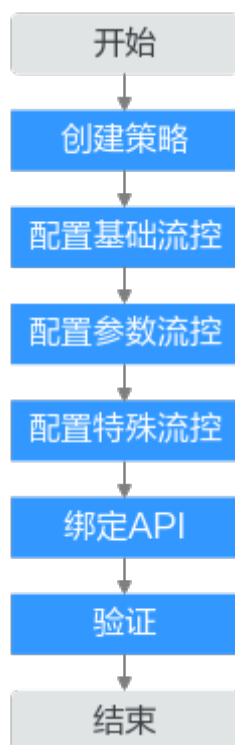
- API添加流量控制2.0策略相当于流量控制2.0策略同步绑定了API。同一个环境中，一个API只能被一个流量控制2.0策略绑定，但一个流量控制2.0策略可以绑定多个API。（使用前提是绑定的API已发布。）
- 如果API未绑定流量控制2.0策略，流控限制值为实例“配置参数”中“ratelimit_api_limits”的参数运行值。
- 如果一个API绑定传统流量控制策略后，继续绑定流量控制2.0策略，传统流量控制策略会失效。
- 参数流控的规则最多可定义100个。
- 策略内容最大长度65535。
- 如果您的实例不支持流量控制2.0，请联系技术支持。

4.1.2 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控操作流程

假设您对一个API有如下的流控诉求：

1. 默认API流量限制为100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. 对于请求头test_header的值为userA的请求，限流20次/60秒；同时对于test_header的值为userB的请求，也限流20次/60秒。对于test_header为其他取值的请求，每个值独立限流10次/60秒。
4. 对请求方法为get且请求路径为“reqPath= /list”的限制为10次/60秒。
5. 对请求路径为“reqPath= /fc”的限制为10次/60秒。
6. 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。

4.1.3 使用 APIG 专享版的流量控制 2.0 策略实现 API 的精细流控实施步骤

步骤1 创建策略。

1. 登录**API网关控制台**，创建流量控制2.0策略。
2. 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”。
3. 根据流控诉求，配置策略基本信息。

表 4-1 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。
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100次，用户流量限制为5次。

表 4-2 基础流控配置

参数	配置说明
API流量控制限制	100
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Host并定义对应的规则。
 - a. 在“定义参数”区域，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”，生效维度选择“规则限流”，API流量限制设置为10次，时长为60秒；单击  编辑条件规则，设置“条件表达式配置”中匹配条件为“Host = www.abc.com”。


参数流控配置


定义参数	参数位置	参数
	path	reqPath
	method	method
	header	Host


⊕ 添加参数


定义规则

rule-84sg 


★ 生效维度  参数限流 **规则限流**

★ 条件规则 
Host = www.abc.com

★ API流量限制  10 次

时长  60 秒

⊕ 添加规则

- 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，对于请求头中Host参数等于“www.abc.com”的API，且API调用次数达到10，参数流控规则限流生效。
2. 根据3，定义参数test_header并定义对应的规则。
 - a. 在“定义参数”区域，单击“添加参数”，在“参数位置”列选择“header”，在“参数”列填写“test_header”。
 - b. 在“定义规则”区域，单击“添加规则”，生效维度选择“参数限流”，流控参数中选择test_header，API流量限制设置为20次，时长为60秒；单击  编辑条件规则，设置“条件表达式配置”中匹配条件为“test_header = userA” OR “test_header = userB”。

rule-q5dz

生效维度 参数限流 规则限流

流控参数 test_header 包含空值

条件规则 test_header || test_header

- test_header = userA
- OR
- test_header = userB

API流量限制 20 次

时长 60 秒

- c. 在“定义规则”区域，单击“添加规则”继续添加规则，生效维度选择“参数限流”，流控参数中选择test_header，API流量限制设置为10次，时长为60秒；单击编辑条件规则，设置“条件表达式配置”中匹配条件为“test_header != userA” AND “test_header != userB”。

rule-ah38

生效维度 参数限流 规则限流


流控参数 test_header 包含空值

条件规则 test_header && test_header

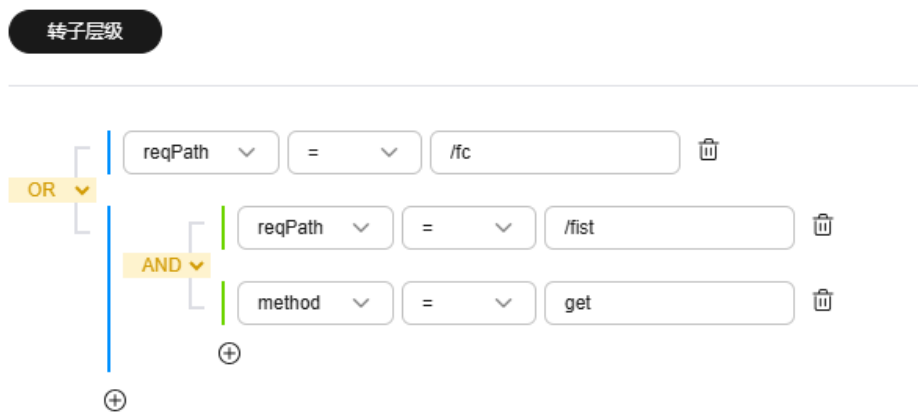
- test_header != userA
- AND
- test_header != userB

API流量限制 10 次

时长 60 秒

- d. 单击“确定”，生成关于请求头test_header的参数限流，表示对于值userA和userB，每个独立限流20次/60s；对于其他取值，每个独立限流10次/60秒。
3. 根据4、5，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”，生效维度选择“规则限流”，API流量限制设置为10次，时长为60秒；单击  编辑条件规则，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



- 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，参数流控规则限流生效。

步骤4 特殊流控配置。

根据6，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 4-3 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

4.2 使用 APIG 专享版的 JWT 认证策略实现身份认证和密钥轮转

应用场景

JWT (JSON Web Token) 是一种基于JSON的轻量级令牌，通过数字签名实现信息的安全传递，广泛应用于身份认证、信息交换等场景。

JWT常用于身份认证的令牌，利用无状态特性实现高效跨场景身份验证。用户通过认证服务器生成JWT，客户端通过在请求中携带Token来访问受保护的资源。网关收到请求后，验证JWT的有效性（签名、有效期等），并可以从Payload中直接提取用户身份和权限信息。

JWT的安全性依赖于签名密钥，密钥轮转（定期或按需更换签名密钥）是保障JWT安全的关键实践。长期使用同一密钥会增加泄露概率（如密钥被恶意窃取、内部人员滥用），定期轮转密钥可降低风险；此外，若发现密钥可能泄露，也可以立即触发应急轮转，终止旧密钥的有效性，防止攻击者利用泄露密钥伪造令牌。

方案优势

API网关的JWT认证策略支持从Header、Query、Cookie多种位置设置Token，通过校验Token实现身份认证。同时支持识别Payload中的claim并将身份信息提取出来，传递给后端。此外，用户还可以通过设置JWKS_URI远程服务地址，通过定期更换该地址返回的公钥，实现无缝密钥轮转。

约束与限制

- 请求中携带的Token应当符合[RFC 7519规范](#)；JWT认证策略配置的公钥应当是符合[RFC 7517规范](#)的JSON格式字符串。
- 由于JWT并不会对数据进行加密，请勿将敏感数据设置在Token中。此外为了避免Token泄露，建议您不要对请求协议为HTTP的API使用JWT认证。
- 网关会校验Token中的nbf（生效时间）和exp（过期时间）字段，如果校验失败会拒绝请求。
- Token校验支持的加密算法包含RS256、RS384、RS512、ES256、ES384和ES512。使用RSA算法时，建议密钥长度大于等于3072位。
- 当选择“定时拉取”的公钥设置方式时，必须保证JWKS_URI和APIG实例网络互通。网关内部的定时任务会每隔5min请求JWKS_URI，将返回的响应体作为公钥，并且当次请求的结果会覆盖上次请求的结果。如果要实现公私钥轮转，建议在每次轮换时，留出一段宽限时间，令JWKS_URI返回新公钥和本次轮转被替换的旧公钥，使得新旧私钥签发的Token在这段时间均有效。

- 网关会根据Token和JWKS公钥中的kid进行匹配验签。如果JWKS中只存在一个JWK则kid可以为空，否则不可以为空；JWKS中任意两个JWK的kid不可以相同。如果未设置kid，则公私钥替换后，之前签发的Token无法校验通过。
- 更多约束与限制，请参考[配置API的JWT认证](#)。

操作流程



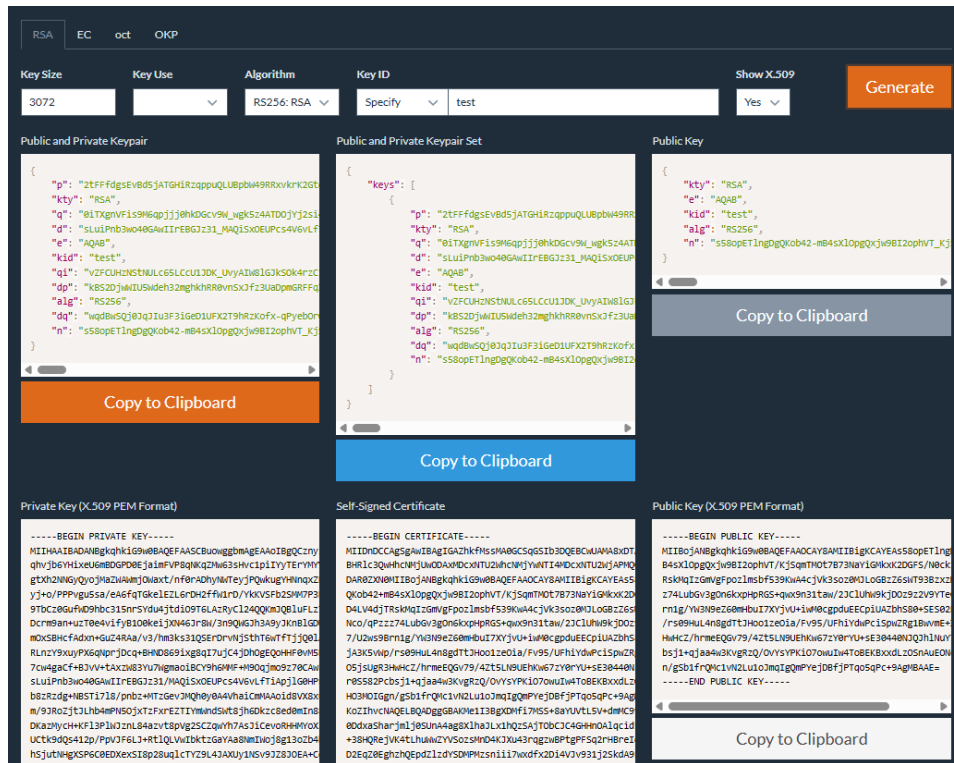
1. **生成密钥对和签发Token**
通过在线生成或者本地生成密钥对和签发Token。
2. **搭建远程JWKS服务地址**
搭建并维护一个返回JWK公钥的在线服务，供网关访问获取公钥。
3. **创建JWT认证策略**
配置一个JWT认证策略，设置JWKS_URI。
4. **绑定API**
将JWT认证策略绑定API。
5. **验证身份认证是否生效**
通过改变请求携带的Token来测试API是否被JWT认证策略所保护。
6. **实现密钥轮转**
通过更换远程JWKS服务返回的公钥实现密钥轮转。
7. **验证密钥轮转是否生效**
验证新私钥签发的token是否能通过认证。

使用 JWT 认证策略实现身份认证和密钥轮转实施步骤

步骤1 生成密钥对和签发Token。

JWT的签发和验证依赖密钥对，您可以通过[在线生成](#)或者[本地生成](#)等方式来生成密钥对，并利用私钥签发Token。请您妥善保管私钥，避免泄露。

- 在线生成
 - a. 登录[JWK密钥生成平台](#)，“Key Size”选择“3072”，“Algorithm”选择“RS256”算法，输入自定义的Key ID，“Show X.509”选择“Yes”，单击“Generate”生成JWK及其对应的X.509格式的密钥。



- b. 登录[JWT生成平台](#)，“Algorithm”选择“RS256”算法，在header对应的json结构体中添加上一步自定义的kid（Key ID）字段，并在公钥和私钥位置处填入上一步生成的公钥和私钥，左下方框会自动生成对应的JWT。

Algorithm: RS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtZCI6InRlc3QifQ.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG91IiwiaWF0IjoiYyJjHj8QbplTIXymYz79riJb_VzbE0lWXcQHkxliuITJAFQJSq_EU1LGyz4QLHaxn5pr9qu01UrCU2gtD16ZzGh89Zuhji4I7GxEfYh3L9eFJDKJjPEBvI0-tI01jhdeoEI0xrSPF1JDnxoMb_9BsLtjyJiU2qvc0X_dUSW2koV7T8w
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{  "alg": "RS256",  "typ": "JWT",  "kid": "test"}
```

PAYLOAD: DATA

```
{  "sub": "1234567890",  "name": "John Doe",  "admin": true,  "iat": 1516239622}
```

VERIFY SIGNATURE

```
RSASHA256(  base64UriEncode(header) + "." +  base64UriEncode(payload),  -----BEGIN PUBLIC KEY-----  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuL3V/XDwSb8+  1D32F63S  -----BEGIN PRIVATE KEY-----  MIIEvwIBADANBgkqhkiG9w0BAQEF  AASCBAkkggS1AgEAAoIBAQC4vdX9  cPDlvz7U  PfyXrdKJVuiWXXLwQjcmMHSrYdJ  )
```

- **本地生成**

您可以利用JWT相关的开源代码仓，在本地运行代码来生成密钥对和签发Token。下方代码为生成密钥对和签发Token的Python代码示例。

```
import jwt
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import serialization
from jwcrypto.jwk import JWK
import datetime

private_key = rsa.generate_private_key(
    public_exponent=65537,
    key_size=3072
)
pem_private = private_key.private_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PrivateFormat.PKCS8,
    encryption_algorithm=serialization.NoEncryption()
)
public_key = private_key.public_key()
pem_public = public_key.public_bytes(
    encoding=serialization.Encoding.PEM,
    format=serialization.PublicFormat.SubjectPublicKeyInfo
)
jwk_public = JWK.from_pem(pem_public)
jwk_public_dict = jwk_public.export(as_dict=True)
test_kid = "test"
jwk_public_dict['kid'] = test_kid
payload = {
    "sub": "1234567890",
    "name": "John Doe",
    "iat": datetime.datetime.utcnow(),
}
token = jwt.encode(
    payload,
    pem_private,
    algorithm="RS256",
    headers={"kid": test_kid}
)
```

```
print("==== Public Key (JWK Format) =====")
print(jwk_public_dict)
print("\n==== Private Key (PEM Format) =====")
print(pem_private.decode('utf-8'))
print("\n==== JWT =====")
print(token)
```

步骤2 搭建远程JWKS服务地址。

根据**步骤1**中生成的密钥对搭建和维护一个返回公钥的在线服务。API网关会每隔5min访问该服务来获取公钥，并将其缓存。此外，密钥轮转需要多个kid不同的公私密钥对。

以下是返回两个JWK公钥的远程服务Python代码示例：

```
from flask import Flask, request, abort, Response, jsonify, url_for
import json
import time
app = Flask(__name__)
@app.route("/jwks", methods=["GET"])
def echo():
    return jsonify({
        "keys": [
            {
                "kty": "RSA",
                "e": "AQAB",
                "kid": "test-kid-1",
                "alg": "RS384",
                "n": "oZaD8Tu7VKC1hnOvCa-DiouYKdHGaiokIWIlu-
vfvM0JHJdfFLOxJ4BVTksySZcWdv854_81hrYVpylz_YjC8YHfQHmbtOjRQjcYHzQqoZTiZnS-
NRjk4tjzYFOsc1F3oijZutxyeZctCgTn-gUyXlhXzKHsum-
G4I0xWbBZzCGE7l0IMBHi6snrhWdz9eHwUSZviOYpKoYBf88FtBhHJTIt2_VLlrXRwwwP_joEMT56vKvX0dTpKE4H
HMENWT4-p8lVycJvtfPdZeg8hAgqfT4O0DHvfOpxAkSkVJpvJs3MA-VbYYRmZufM8TDI9jlyMffKlxxEbzLgpBp-
oy41mbOI-VSjPynaBRRz1XV0GLEUIz_ri9Or8M29fQqb_h01o5dLC5X06OzRZ--
VENf53mnXwdUwesROexMF4_5JCJ7-
Pefi0b6DTIQiPYd0lvKajzN1jwP4WfdzZE5E5FsX84gbkbn2G3aLgU2EPPoX7LPZTdlWMr5jF4FjT73HF0cr",
            },
            {
                "kty": "RSA",
                "e": "AQAB",
                "kid": "test-kid-2",
                "alg": "RS256",
                "n": "lRv_mMn0hRIAlMjrcGnyFTIasr7rqwdK2GrQ5rNF76ZGrl-NVGpVTRq0lzcYzyOmLiFGfu1E-
Tgs4aPwMyOVy1rXlXIKYOShGblElrtsFgd6b-xr09WKZcyTnnV16wH68WjpELDFUNJ48GNU-
c7co2UroQhUZ4Rh8dHlHl89-bayYMwBFMmVfVcimGf4xPut0weldDm-
bdU3RR1qJfjmnAyEA37qYynl7YTVGRBGM4kLnWn3sJIMDDd8v8AJMTHhWyi_DS5K7azkbQQMDd5hPKn_yU_
-700N5fUqIWELSlj1L85qPdpQ62j109ShcFpVAXKvg64qGesxlDzbgV6D3NWN_7wuGZS-exEi-gVJgMo-
V1pNTMacRuooAK-VX6N-
ds9nSMXb8P825XcFvGT1NecI5E7VcmqEvHjKcTEuGVWlTqLujfM9szOC4wAHMfmFCXhiEAKfwq6kK39uM6hwk
kUm_-HYUL_YbOWNRJ-hOtc7ooNMy4EXgDhLgK1"
            }
        ]
    }), 200
if __name__ == '__main__':
    app.run(port=8080)
```

步骤3 创建JWT认证策略。

1. 登录**API网关控制台**，创建JWT认证策略。
2. 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“JWT认证”。
3. 公钥设置方式选择“定时拉取”，“JWKS_URI”填入搭建的JWKS服务地址，其余参数设置默认。**请确保API实例与JWKS服务地址网络保持互通。**
4. 单击“确定”，JWT认证策略创建成功。

步骤4 绑定API。

1. 单击已创建的策略名称，进入策略详情。
2. 在“关联API”区域，单击“绑定API”，选择API分组、发布环境和需要绑定的API，单击“确定”。

步骤5 验证身份认证是否生效。

调用绑定JWT认证策略的API，如果请求携带了指定私钥生成的token，则请求通过JWT认证访问后端，否则返回认证失败。

步骤6 实现密钥轮转。

每次密钥轮转时，用户需要将远程JWKS服务地址返回的公钥更换为新的公钥，请求也需要携带新私钥签发的token来访问API。为了避免旧私钥签发的token在密钥轮转时立即失效导致认证失败，用户需要在密钥轮转后的一段“宽限期”（根据旧私钥失效时间确定），设置远程JWKS服务同时返回旧公钥和新公钥。

例如，如果上一个轮转周期内远程JWKS服务返回旧公钥的kid为“test-kid-1”，则密钥轮转时远程JWKS服务应当同时返回旧公钥（kid为“test-kid-1”）和新公钥（kid为“test-kid-2”），这样新旧私钥签发的token在这一段时间内均能通过JWT认证。当旧私钥签发的token均失效后，再让远程JWKS服务只返回新公钥（kid为“test-kid-2”）。

步骤7 验证密钥轮转是否生效。

根据**步骤6**，调用绑定JWT认证策略的API，密钥轮转后，请求携带新私钥生成的token能通过JWT认证访问后端；此外，在“宽限期”内，如果请求携带了旧私钥或者新私钥生成的token，均能通过JWT认证访问后端。

----结束

5 API 安全

5.1 使用 WAF 对 APIG 进行安全防护

应用场景

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。

方案架构

图 5-1 后端服务器访问原理



方案优势

方案一：API分组通过域名方式对外提供服务，具备更强的可扩展性。

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

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。

1. 登录[API网关控制台](#)，在左侧导航栏中选择“API管理 > API分组”。
2. 单击“创建分组 > 直接创建”，填写分组名称完成创建。
3. 单击已创建分组名称，进入分组详情。
4. 在“分组信息”页签中，查看调试域名并记录。该调试域名唯一且不可修改，每天最多可以访问1000次。
5. 在“API运行”页签中，单击“创建API > 创建API”，即可添加API。

步骤2 在WAF侧添加防护域名。进入WAF控制台，单击“网站设置 > 添加防护网站”，即可配置防护域名。配置“源站地址”时，需要填写API分组的域名，并添加证书。添加域名后，还需执行放行回源IP、本地验证、修改域名DNS解析设置。详细操作步骤请参考[网站接入WAF（云模式）](#)。

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。

基础信息

防护域名 [?]

[快速添加云内域名](#)

请确保域名已经过ICP备案 (https://beian.xinnet.com/)，WAF会检查域名备案情况，未备案域名将无法添加。

网站名称(可选)

网站备注(可选)

防护端口

[查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务配置 [?]

对外协议	源站协议	源站地址	源站端口	操作
<input type="text" value="HTTPS"/>	<input type="text" value="HTTPS"/>	<input type="text" value="IPv4"/> <input type="text" value=""/>	<input type="text" value="443"/>	删除

[添加地址](#) 您还可以添加49个源站地址

国际证书

证书选择 [导入新证书](#)

代理情况 [?]

七层代理 四层代理 无代理

配置参数

步骤3 在APIG实例中，为API分组绑定已创建的防护域名。

1. 进入APIG控制台，在左侧导航栏中选择“API管理 > API分组”。
2. 单击已创建的分组名称。
3. 在“分组信息”页签中的“域名管理”区域，单击“绑定独立域名”。
4. 在弹窗中添加已创建的防护域名即可。

步骤4 在APIG实例中，将“real_ip_from_xff”开关打开，并设置参数。

1. 在APIG控制台的左侧导航栏中，选择“实例管理”。
2. 在“配置参数”页签中，根据实际的真实IP排序设置“xff_index”参数。

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需要据此指定用户的真实IP。

例如，如果WAF在HTTP头部记录的X-Forwarded-For值为：“客户端的真实IP，代理服务器1-IP，代理服务器2-IP，代理服务器3-IP，……”，则“xff_index”的值设置为“0”，表示获取X-Forwarded-For的第一个IP；如果WAF在HTTP头部记录的X-Forwarded-For值为：“代理服务器1-IP，客户端的真实IP，代理服务器2-IP，代理服务器3-IP，……”，则“xff_index”的值设置为“1”，表示获取X-Forwarded-For的第二个IP。

----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。

1. 登录**API网关控制台**，在左侧导航栏中选择“实例管理”。
2. 单击实例名称或“查看控制台”。
3. 在“基础信息”页签中，查看入口地址。
 - 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。

1. 在APIG控制台的左侧导航栏中，选择“API管理 > API分组”。
2. 单击“DEFAULT”分组名称。
3. 单击“创建API > 创建API”，即可添加API。

步骤3 在WAF侧添加防护域名。进入WAF控制台，单击“网站设置 > 添加防护网站”，即可配置防护域名。配置“源站地址”为API网关实例的**入口地址**，并添加证书。添加域名后，还需执行放行回源IP、本地验证、修改域名DNS解析设置。详细操作步骤请参考[网站接入WAF（云模式）](#)。

- 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。

基础信息

防护域名 [?]

example100.com [快速添加云内域名](#)

请确保域名已经过ICP备案（<https://beian.xinnet.com/>），WAF会检查域名备案情况，未备案域名将无法添加。

网站名称(可选)

您可以自定义域名名称

网站备注(可选)

您可以填写备注信息

防护端口

4443 [查看可添加端口](#)

标准端口为HTTP对外协议80和HTTPS对外协议443

服务器配置 [?]

对外协议	源站协议	源站地址	源站端口	操作
HTTPS	HTTPS	IPv4 [IP Address]	443	删除

[添加地址](#) 您还可以添加49个源站地址

国际证书

证书选择 test_cert [导入新证书](#)

代理情况 [?]

七层代理 四层代理 无代理

高级配置

步骤4 在APIG实例中，为DEFAULT分组绑定已创建的防护域名。

1. 在APIG控制台的左侧导航栏中，选择“API管理 > API分组”。

2. 单击“DEFAULT”分组名称。
3. 在“分组信息”页签中的“域名管理”区域，单击“绑定独立域名”。
4. 在弹窗中添加已创建的防护域名。

步骤5 在APIG实例中，将“real_ip_from_xff”开关打开，并设置参数。

1. 在APIG控制台的左侧导航栏中，选择“实例管理”。
2. 在“配置参数”页签中，根据实际的真实IP排序设置“xff_index”参数。

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需要据此指定用户的真实IP。

例如，如果WAF在HTTP头部记录的X-Forwarded-For值为：“客户端的真实IP，代理服务器1-IP，代理服务器2-IP，代理服务器3-IP，……”，则“xff_index”的值设置为“0”，表示获取X-Forwarded-For的第一个IP；如果WAF在HTTP头部记录的X-Forwarded-For值为：“代理服务器1-IP，客户端的真实IP，代理服务器2-IP，代理服务器3-IP，……”，则“xff_index”的值设置为“1”，表示获取X-Forwarded-For的第二个IP。

----结束

5.2 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击

5.2.1 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击方案概述

应用场景

当用户在公网中调用APIG上公开的业务API时，会存在DDoS攻击风险，为防范DDoS攻击，华为云提供了DDoS防护服务。下文讲述如何对接DDoS高防服务来进行抵御DDoS攻击。DDoS攻击详情请参见[常见DDoS攻击类型](#)。

方案架构



方案优势

- 所有Region都可以配置。
- 可指定保底带宽和弹性带宽。

约束与限制

- 对接高防后，如果开启了WEB基础防护或者CC防护，APIG将无法透传真实源IP。
- 需修改域名的IP，必须使用高防IP。
- 需依赖公网DNS进行域名切换。
- 业务带宽需收费。
- 域名切换有短暂时间间隔，可能会导致网络中断。

5.2.2 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击资源规划

表 5-1 资源规划

资源	数量（个）
DDoS高防实例	1
已备案域名	1
API分组	1
API	1

5.2.3 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击操作流程



1. **购买DDoS高防**
购买DDoS高防实例，为对接做准备。

2. **接入域名**
添加域名和证书。
3. **注册公网域名**
将防护域名注册到DNS服务上。
4. **绑定防护域名**
将防护域名绑定到API分组上。
5. **创建API**
在绑定域名的分组上创建一个API。
6. **验证**
调用API，调用成功表示对接DDoS成功。

5.2.4 使用 DDoS 防护服务为 APIG 抵御 DDoS 攻击实施步骤

前提条件

已创建API分组，详细操作请参见《[用户指南](#)》。

操作步骤

- 步骤1** 登录[DDoS防护控制台](#)，在左侧导航栏中选择“DDoS高防 > 概览”，单击“购买DDoS高防”。

根据业务需求，配置参数信息。详情请参考[DDoS高防操作指南](#)。

实例类型
DDoS原生防护1.0 DDoS原生防护2.0 **DDoS高防** DDoS管理中心
针对源站在中国的用户提供的DDoS防护服务，避免源站遭受大流量DDoS攻击

接入类型
接入 IP接入
当前使用中国内地（大陆）地区的云服务对外提供网站服务，需要申请备案 接入指引

接入描述
接入域名：DNS解析指向
带宽类型：多线BGP
保护资源：互联网上所有公网IP

防护区域
中国大陆 中国大陆外

线路资源
BGP

IP类型
IPv4 IPv6
防护IPv6网站需要选择IPv6实例，防护IPv6网站需要选择IPv6实例，只支持公网类型的地址。

资源区域
华北 华东

业务防护带宽
10 Gbps 20 Gbps 30 Gbps 40 Gbps 50 Gbps 60 Gbps 70 Gbps 80 Gbps 90 Gbps 100 Gbps 200 Gbps 300 Gbps 400 Gbps 500 Gbps 600 Gbps

防护防护带宽
10 Gbps 20 Gbps 30 Gbps 40 Gbps 50 Gbps 60 Gbps 70 Gbps 80 Gbps 90 Gbps 100 Gbps 200 Gbps 300 Gbps 400 Gbps 500 Gbps 600 Gbps 700 Gbps 800 Gbps
1000 Gbps

业务带宽
100 Mbps 500 Mbps 1,000 Mbps 2,000 Mbps 自定义
此带宽为防护的源站或源站的干净业务流量带宽，**免费赠送100Mbps**，建议此业务带宽规格大于等于源站出口带宽，否则可能会造成业务受影响。

弹性业务带宽
不月租 按月计费

业务QPS
3,000
业务QPS指正常业务HTTP(S)请求请求速率峰值

防护峰值
60
默认防护峰值，防护峰值数量本实例可防护的防护峰值的数量

单击“立即购买”，确认产品信息无误后，单击“去支付”。

- 步骤2** 在左侧导航栏选择“DDoS高防 > 域名接入”，单击“添加域名”。详情请参考[配置防护域名](#)。

1. 填写域名信息。

添加用户网站的防护域名和域名绑定的证书。如果没有域名，可通过域名注册商申请；证书可通过[云证书管理服务](#)申请。

📖 说明

填写的域名须备案，如果没有备案，请参考[域名备案](#)。

2. 选择实例与线路。
选择已购买的实例，单击“提交并继续”。
3. 单击“下一步”。
4. 单击“完成”。

步骤3 确认已开启CNAME自动调度和安全防护。

域名	CNAME	实例与线路	源站IP/域名	业务类型	安全防护	企业项目	操作
www.zwf1112.top	85f124619e14b930mmmmcafe.dns.	CNAME接入状态：正常 实例选择信息：查看详情 CNAME自动切换：🔄	🔗 编辑 删除	网站类 HTTP/WebSocket	流量安全防护：开 WEB鉴权防护：🔗 CC防护：🔗	default	编辑 删除

步骤4 进入DNS控制台，在左侧导航栏中选择“公网域名”，单击“创建公网域名”。

填写防护域名并选择企业项目，单击“确定”。

步骤5 进入APIG控制台，在共享版API网关的左侧导航栏中选择“开放API > API分组”，单击已创建的API分组名称。

步骤6 在“域名管理”页签中，绑定防护域名。

步骤7 在“API列表”页签中新建API。详情请参考[《用户指南》](#)。

步骤8 如果源站已配置防火墙或安装安全软件，为了防止高防回源IP被源站拦截或限速，需要将高防回源IP段添加到源站的防火墙或其它防护软件的白名单中，即放行高防回源IP段，以确保高防的回源IP不受源站安全策略影响。

身份认证和访问控制

- APIG提供API级别的认证鉴权，包括[APP认证](#)、[IAM认证](#)和[自定义认证](#)。
 - 在IAM认证场景下，使用Token认证方式调用API时，token过期时间由IAM服务决定。详情请参考[获取IAM用户Token（使用密码）](#)。
 - 在APP认证/IAM认证场景下，使用AK/SK认证方式调用API时，签名有效期为15分钟。
- APIG提供API级别[访问控制策略](#)，用户可以设置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。
- APIG支持实例级别[访问控制策略](#)，用户可以配置黑白名单来禁止/允许某个IP地址访问实例。

DDoS 防护

- 流量控制：
 - APIG提供API级别的[流量控制策略](#)和[流量控制2.0插件策略](#)，用户可以通过为API配置流控策略进行流量控制。
 - APIG提供实例级别的[流量控制](#)，通过配置ratelimit_api_limits参数设置API全局默认流控值。
- APIG提供实例级别的[请求大小控制](#)，通过配置request_body_size参数设置请求中允许携带的Body大小上限。
- APIG支持对接WAF和DDoS防护服务来进行抵御攻击。具体操作请参考[使用WAF对APIG进行安全防护](#)和[使用DDoS防护服务为APIG抵御DDoS攻击](#)。

数据传输安全

- APIG支持创建HTTP/HTTPS协议的API，默认使用HTTPS。
- APIG支持TLS 1.1和TLS 1.2，推荐使用TLS1.2。具体操作请参考[配置API的调用域名](#)章节中的“支持最小TLS版本”参数说明。
- APIG默认支持安全的[加密套件](#)，通过配置ssl_ciphers参数按需选择其中的加密套件。
- APIG支持TLS双向认证，包括APIG网关和客户端之间的双向认证（配置请参考[配置APIG专享版与客户端间的单向认证或双向认证](#)）和APIG网关和后端服务之间的双向认证（配置请参考[创建API](#)章节中的“TLS双向认证”参数说明）。

审计日志和访问日志记录

- APIG默认使用审计日志服务（CTS）记录OpenAPI的执行日志，用户可以在CTS服务页面查看租户最近的操作日志。具体操作请参考[审计与日志](#)。
- APIG和云日志服务（LTS）集成，推荐租户在APIG页面开通日志分析功能，可以快速获取并分析API的调用日志。具体操作请参考[查看APIG的API调用日志](#)。

6 版本迁移

6.1 APIG 共享版迁移到专享版

应用场景

APIG共享版即将退市，为了避免影响用户的业务，需要将共享版上已有资源迁移到专享版上继续使用。

约束与限制

- 基于APIG共享版使用了云商店功能暂不支持迁移。
- 基于APIG共享版使用了跨用户授权功能暂不支持迁移。
- 基于APIG共享版使用了ELB通道类型的VPC通道暂不支持迁移。
- 由DataArts创建的共享版资源需要由DataArts服务提供迁移。

涉及以上特殊场景的用户，可[提交工单](#)联系技术支持工程师协助处理。

迁移可能带来的影响

1. 公网出入口的变化

专享版实例可以根据需要分别开启公网入口和公网出口，每个实例都会有单独的公网入口IP和公网出口IP，该IP与原有的共享版IP不同，如果上游和下游（服务端和客户端）的相关服务有网络安全策略的设置，需要修改相应的网络安全策略，放通对应IP的访问。

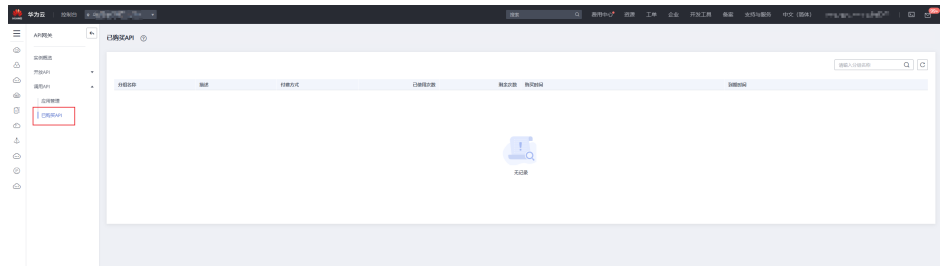
2. 内网出入口的变化

每个专享版实例都会拥有一个VPC内的入口私有IP，以及VPC内的多个出口私有IP（专享实例的基础版、专业版、企业版，以及铂金版分别有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。），上下游服务（服务端和客户端）需要酌情调整网络安全策略，保证网络可达。如果下游存在跨VPC调用的场景时，需要通过VPC终端节点对接到APIG专享版的VPC终端节点服务上，以保证网络可达。具体操作详见[实施步骤](#)。

3. 调试域名的变化

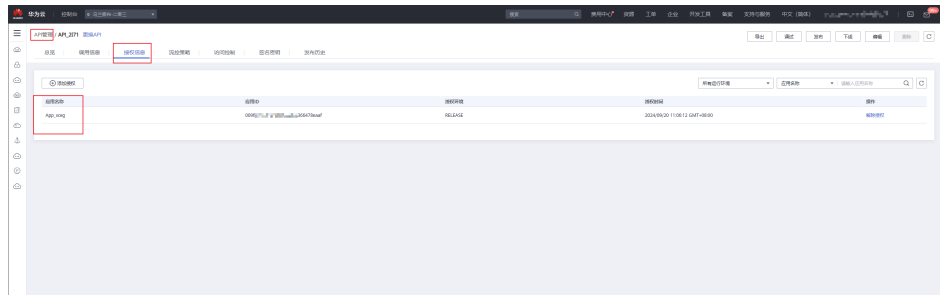
原共享版的分组调试域名{group-id}.apig.{region-id}.huaweicloudapis.com将会更新为{group-id}.apic.{region-id}.huaweicloudapis.com，如果有使用调试域名进行API调用的，则需要做相应修改。

- 在左侧导航栏中选择“调用API > 已购买API”，查看已购买的API。如果已购买API列表为空，则说明未使用云商店功能，可以迁移共享版；否则，请[提交工单](#)联系技术支持工程师协助处理。



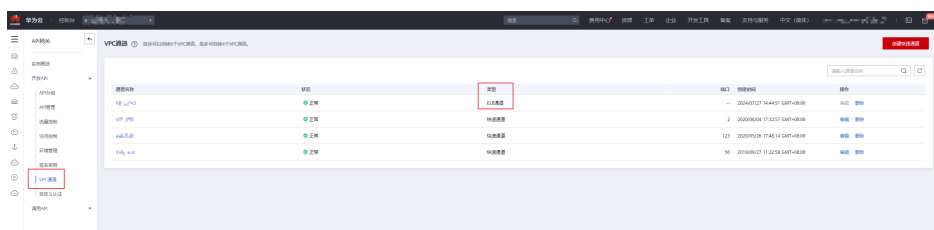
步骤2 查看API授权信息。

- 在左侧导航栏中选择“开放API > API管理”。
- 单击API名称，进入API详情页面。
- 单击“授权信息”页签，查看授权应用。如果授权的应用非用户自身的应用，则为跨用户授权场景，不支持迁移共享版，请[提交工单](#)联系技术支持工程师协助处理；否则，可以迁移共享版。



步骤3 查看VPC通道类型。

在左侧导航栏中选择“开放API > VPC通道”，查看通道类型。如果VPC通道类型为“ELB通道”，则不支持迁移共享版，请[提交工单](#)联系技术支持工程师协助处理；否则，可以迁移共享版。



步骤4 查看是否存在DataArts服务创建的资源。

在左侧导航栏中选择“开放API > API分组”，查看分组名称。如果分组名称由“dlm_default_”开头且描述中有“default api group created by dlm”字样，则表示该分组资源由DataArts服务创建。这部分资源需要联系DataArts的服务人员进行迁移，除DataArts以外的资源可以正常迁移。

迁移信息	项目ID	专享版实例ID	局点
	XXX	XXX	XXX

验证和切流

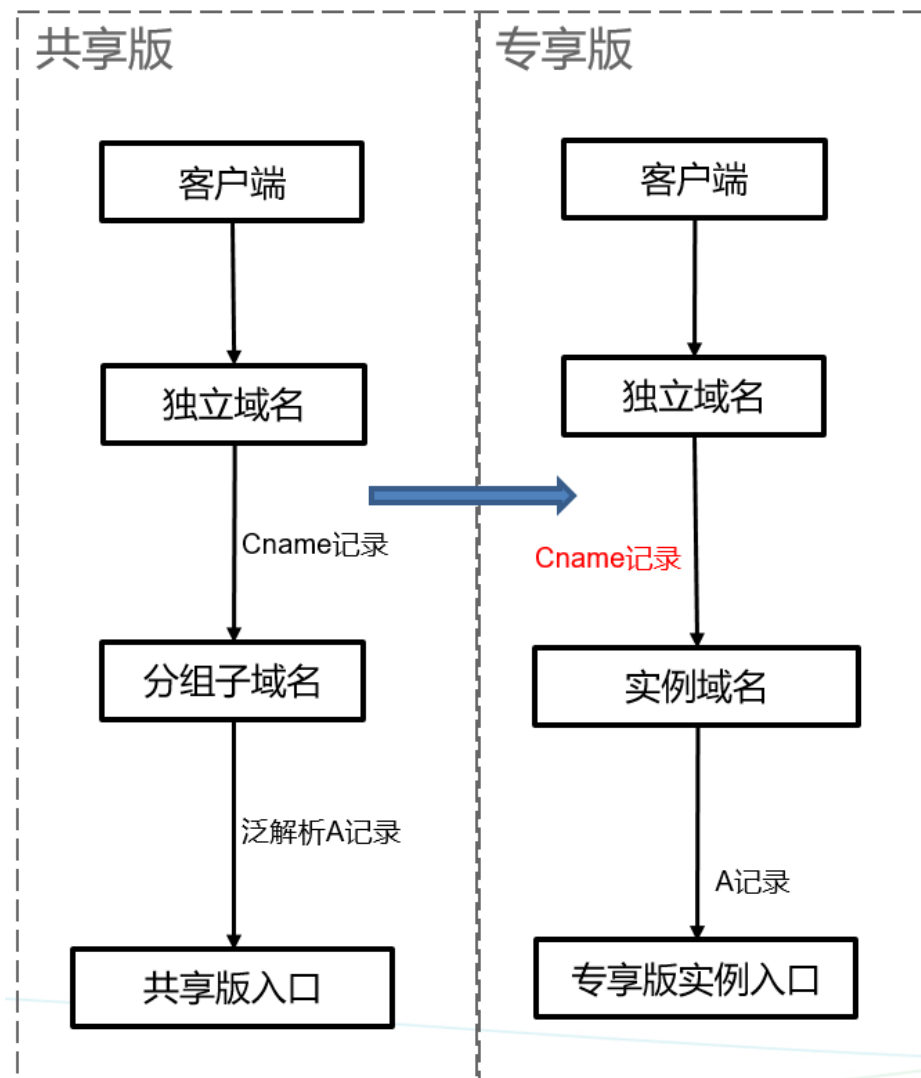
步骤1 迁移完成后，需要先在APIG专享版实例上调试验证迁移后的资源功能是否正常。

- 可以使用调试功能来测试API功能是否正常，详情参考[调试API](#)。
- 可以使用分组调试域名进行API功能测试，详情参考[调用API](#)。

步骤2 验证完毕后进行切流，切流目前主要存在以下几种场景。

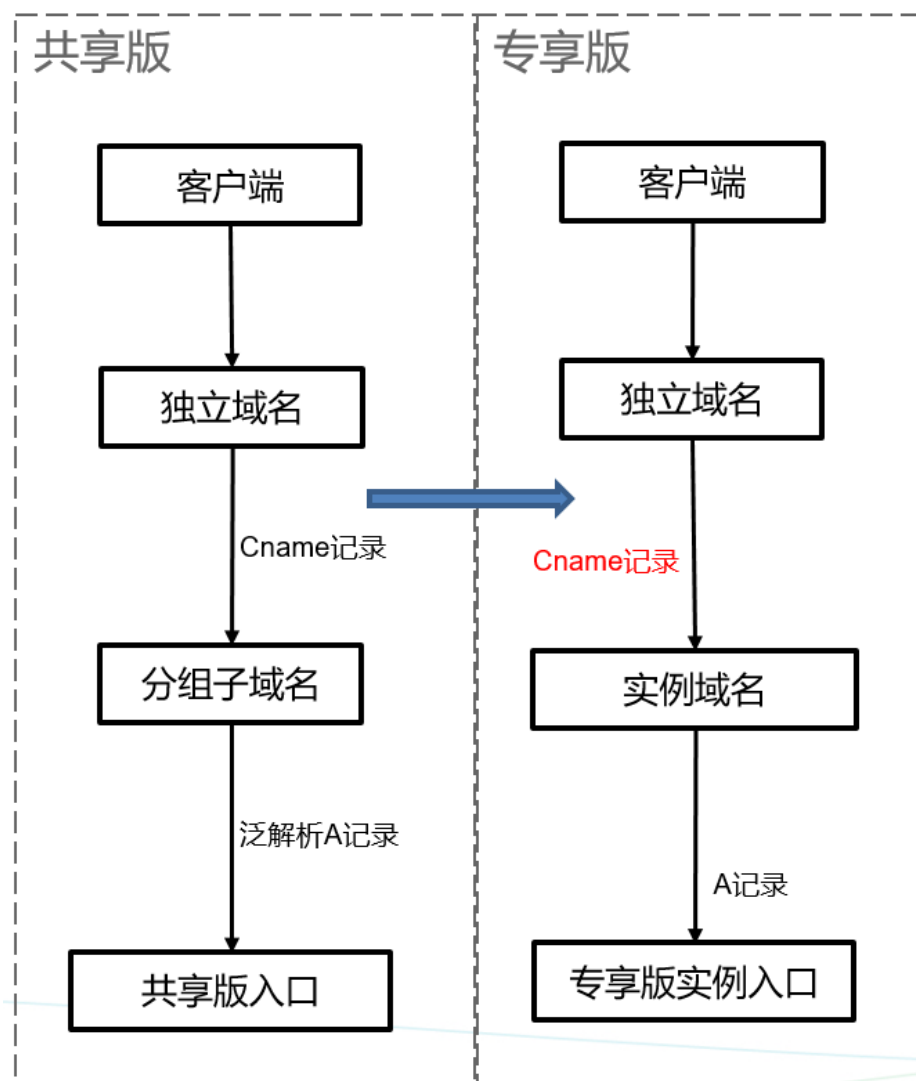
- 使用独立域名从公网访问的场景

需要将原来自定义域名的Cname记录从共享版分组子域名更改为专享版的实例域名{instance-id}.apic.{region-id}.huaweicloudapis.com。

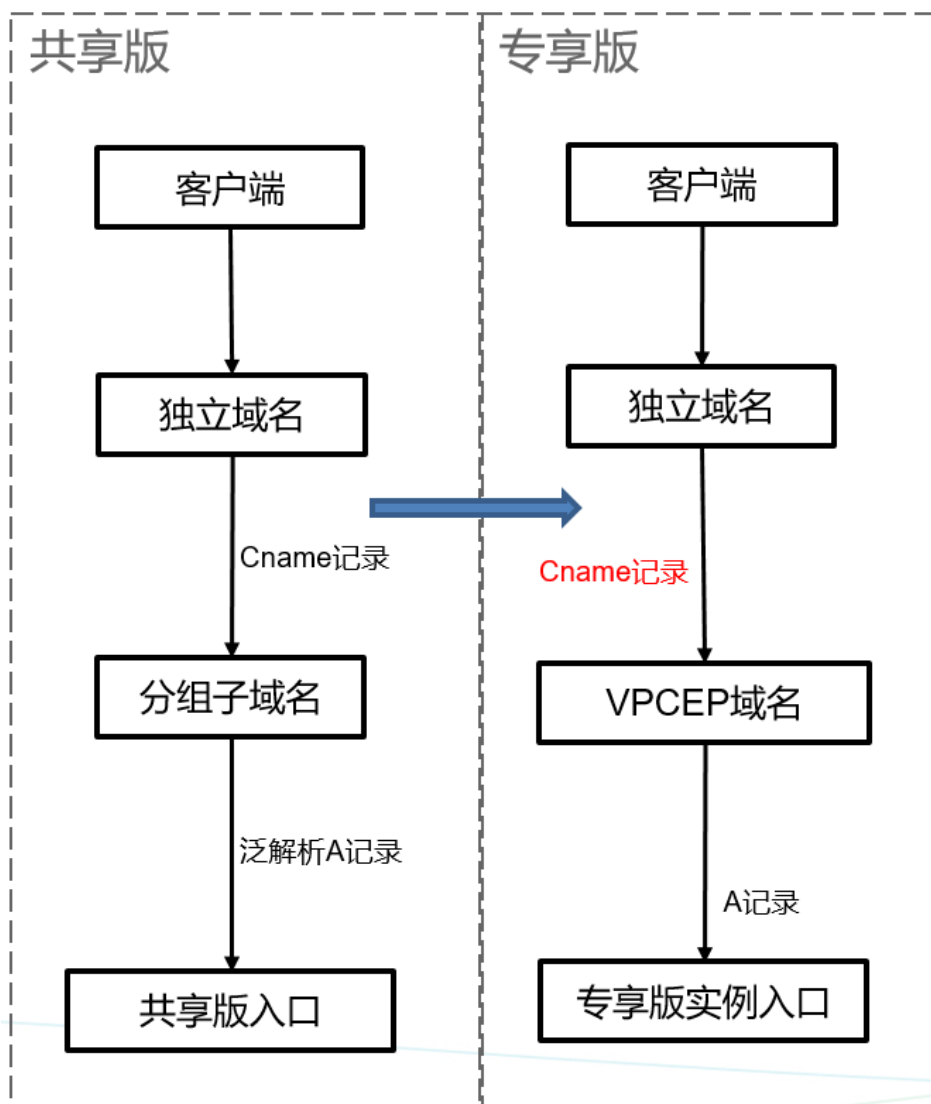


- 同VPC内使用独立域名从内网访问的场景

需要将原来的自定义域名的Cname记录从共享版分组子域名更改为专享版实例的实例域名{instance-id}.apic.{region-id}.huaweicloudapis.com。



- 跨VPC使用独立域名从内网访问的场景
 - a. 需要先使用VPC终端节点打通跨VPC的网络链路。具体操作请参考[终端节点简介](#)和[管理终端节点](#)。
 - b. 将原来的自定义域名的Cname记录从共享版分组子域名更改为[步骤2.a](#)中创建的新VPC终端节点的域名。



----结束