API 网关

最佳实践

文档版本 02

发布日期 2024-04-03

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 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 使用 API 网关专享版开放云容器引擎 CCE 工作负载 1
1.1 方案概述 1
1.2 资源规划 2
1.3 操作流程 3
1.4 实施步骤 3
2 使用 API 网关专享版开放本地数据中心的服务能力 13
3 使用函数服务开发自定义认证 17
4 API 网关专享版跨 VPC 开放后端服务 21
4.1 方案概述 21
4.2 资源规划 22
4.3 操作流程 22
4.4 实施步骤 23
5 API 网关专享版对接 Web 应用防火墙 WAF 33
6 API 网关专享版流量控制 2.0 策略 37
6.1 方案概述 37
6.2 操作流程 38
6.3 实施步骤 39
7 API 网关专享版双重认证 42
7.1 方案概述 42
7.2 操作流程 43
7.3 实施步骤 43
8 API 网关专享版支持 http 到 https 自动重定向 48
8.1 方案概述 48
8.2 操作流程 48
8.3 实施步骤 49
9 基于 API 网关专享版实现 gRPC 服务的路由转发 51
9.1 方案概述 51
9.2 操作流程 51
9.3 实施步骤 52
10 使用 API 网关专享版与客户端进行认证 55

10.1 方案描述.....55
10.2 操作流程.....55
10.3 实施步骤.....56

1 使用 API 网关专享版开放云容器引擎 CCE 工作负载

1.1 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

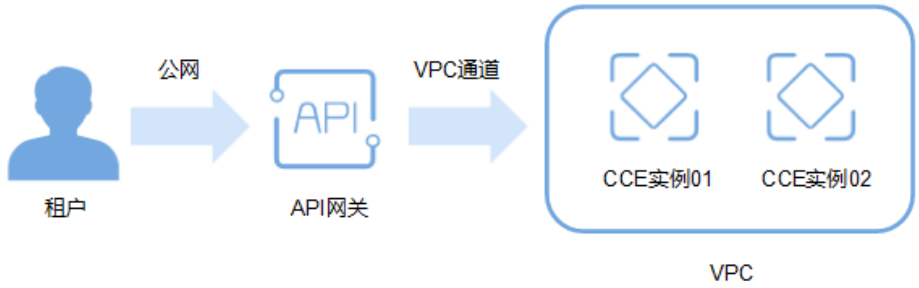
  在API网关中直接创建负载通道，通过负载通道访问CCE工作负载中的实例地址，动态监测工作负载下实例IP地址变化。开放API时使用负载通道访问后端服务，通过API的形式将云容器应用的服务能力开放出来。

- 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 1-1 通过 API 网关访问 CCE 工作负载（由实例组成）



版权所有 © 华为云计算技术有限公司

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。

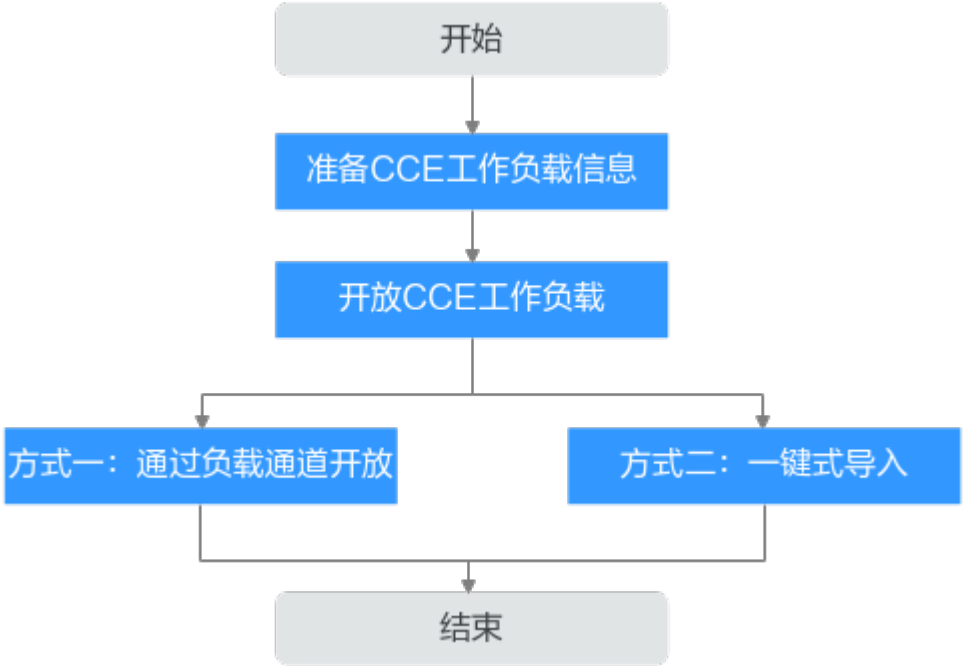
1.2 资源规划

表 1-1 资源和成本规划

资源	数量
云容器引擎CCE	1
API专享版实例	1

版权所有 © 华为云计算技术有限公司

1.3 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购买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。

1.4 实施步骤

准备 CCE 工作负载信息

步骤1 购买集群。

1. 登录云容器引擎控制台，在“集群管理”页面购买CCE集群（VPC网络模型）或Turbo集群。此处选择CCE集群，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. 登录API网关控制台，在左侧导航栏中“实例管理”。

版权所有 © 华为云计算技术有限公司

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《**CCE 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**Pod标签与注解**。

   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

方式一：通过创建负载通道开放 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 1-2 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。建议您按照一定的命名规则填写负载通道名称，方便您快速识别和查找。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。

版权所有 © 华为云计算技术有限公司

参数	配置说明
通道类型	此处选择“微服务”。

b. 微服务配置。

表 1-3 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	选择已购买的集群。
命名空间	选择已购买集群中的命名空间，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 1-4 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 1-5 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。

版权所有 © 华为云计算技术有限公司

参数	配置说明
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”。
   b. 配置前端信息后，单击“下一步”。

表 1-6 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	此处选择**已创建的API分组**。
URL	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）

版权所有 © 华为云计算技术有限公司

c. 配置后端信息后，单击“下一步”。

表 1-7 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。
URL	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，根据错误信息提示修改。

4. 发布API。

   在“API运行”页签中，单击“发布”，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域名管理。

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 1-2 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

版权所有 © 华为云计算技术有限公司

方式二：通过导入云容器引擎 CCE 工作负载开放 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 1-8 工作负载信息配置

参数	配置说明
所属分组	默认为“生成新的分组”。
集群	选择已购买的集群。
命名空间	选择已购买集群中的命名空间，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 1-9 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”。
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。

版权所有 © 华为云计算技术有限公司

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。

2. 发布API。

在“API运行”页签中，单击“发布”，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域名管理。

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 1-3 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

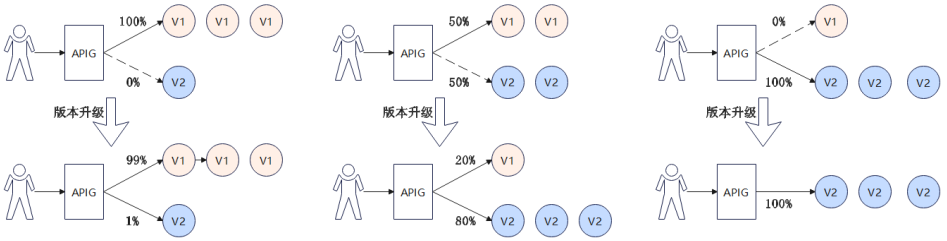
（可选）配置工作负载标签实现灰度发布

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

版权所有 © 华为云计算技术有限公司

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 1-4 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 1-10 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”

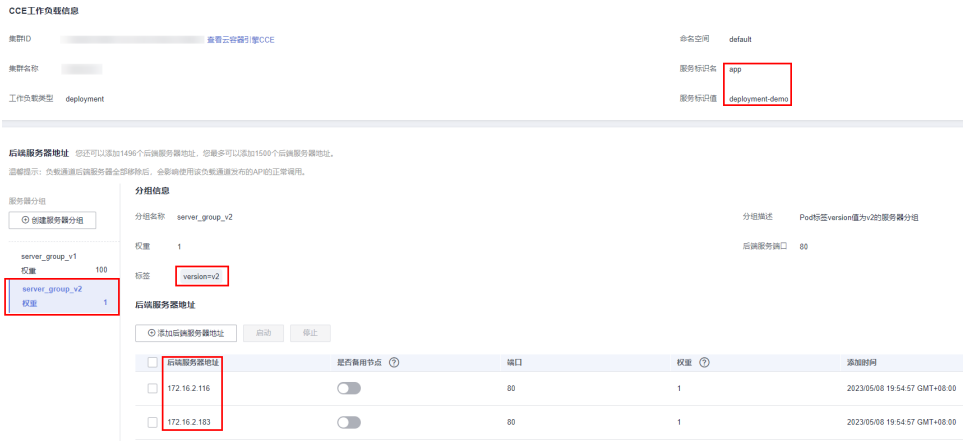
版权所有 © 华为云计算技术有限公司

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 1-5 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”分组的新版本上。

图 1-6 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”。

版权所有 © 华为云计算技术有限公司

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

版权所有 © 华为云计算技术有限公司

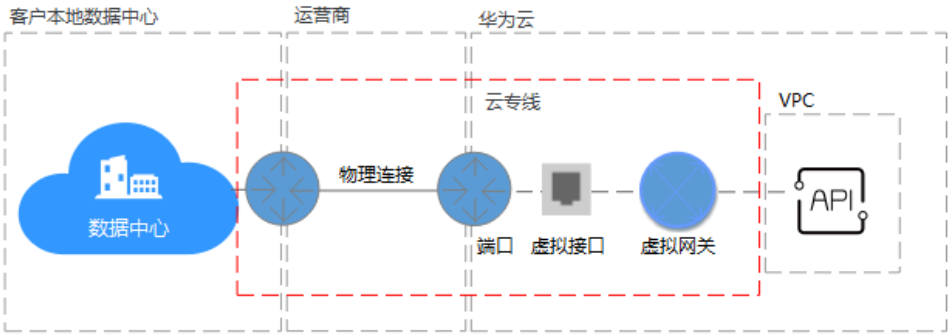
2 使用 API 网关专享版开放本地数据中心的服务能力

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（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的注意事项。

图 2-1 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。

具体请参考《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。

版权所有 © 华为云计算技术有限公司

图 2-2 创建 VPC 示例参考

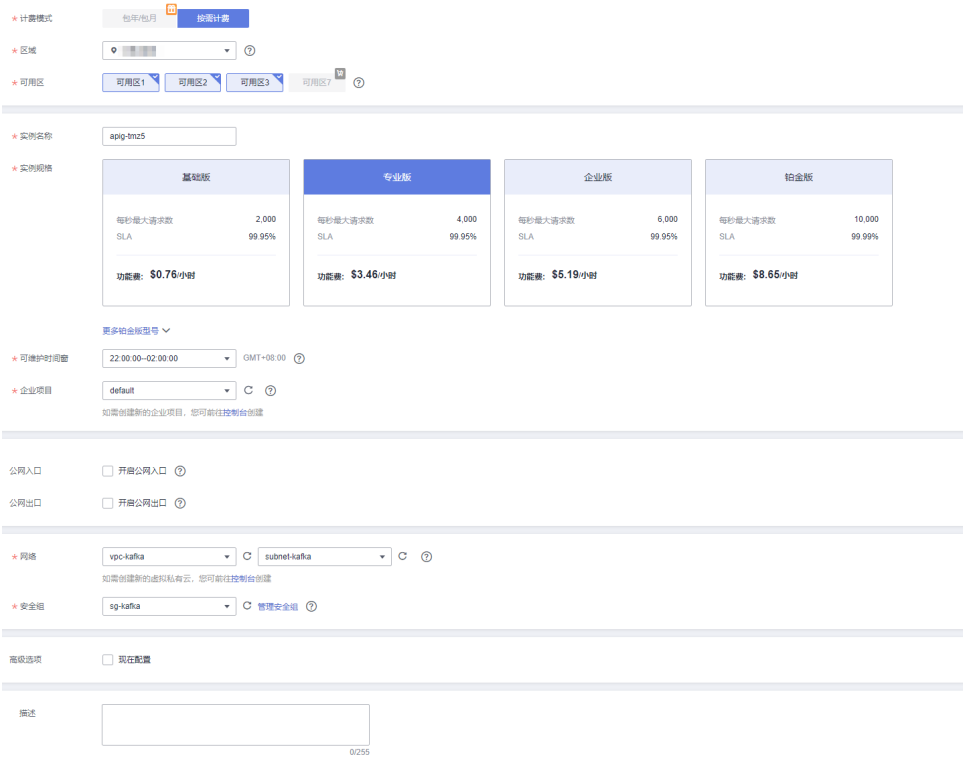
说明

- 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**购买专享版API网关**。

图 2-3 购买 API 网关专享版实例参考



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。

   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。

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。

版权所有 © 华为云计算技术有限公司

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 》的入门。

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。

版权所有 © 华为云计算技术有限公司

3 使用函数服务开发自定义认证

简介

本手册基于华为云API网关实践所编写，用于指导如何为API添加自定义认证。

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**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。

表 3-1 函数信息配置

参数	配置说明
函数类型	默认“事件函数”。
区域	与API网关相同区域。
函数名称	根据规划自定义名称。建议您按照一定的命名规则填写名称，方便您快速识别和查找。
委托名称	用户委托函数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。

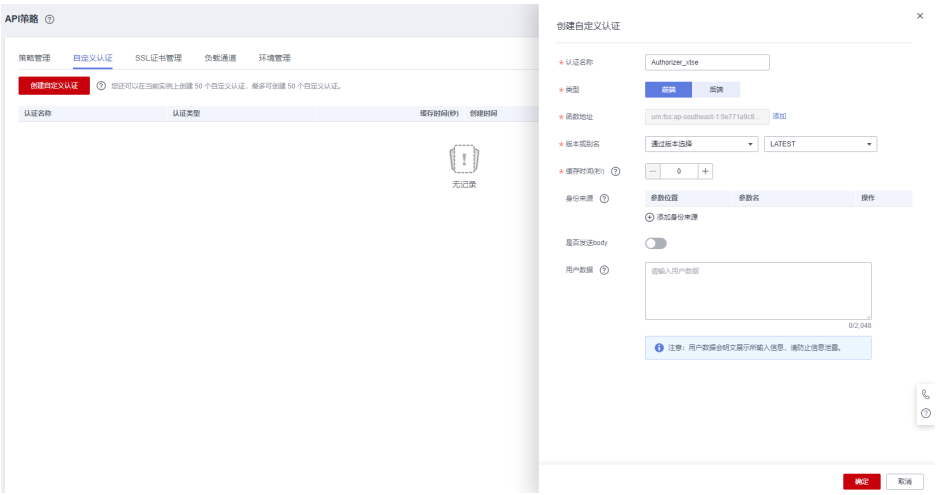
版权所有 © 华为云计算技术有限公司

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网关页面，创建自定义认证，类型选择前端，函数地址选择上一步创建的函数。



创建自定义认证的 API

创建API，具体步骤请参见**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

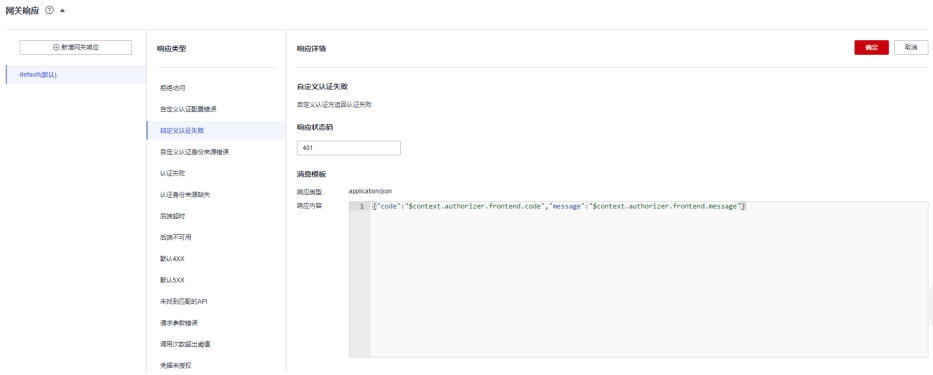
调用API如果输入错误的认证信息，则返回结果如下：

版权所有 © 华为云计算技术有限公司

```
{"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（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"}
```



2

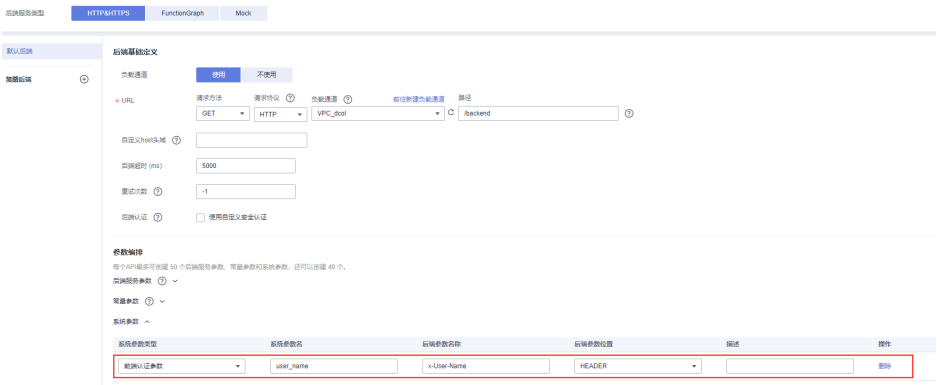
修改之后，调用API传入错误的认证信息，返回状态码为401，返回结果如下：

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

映射后端参数

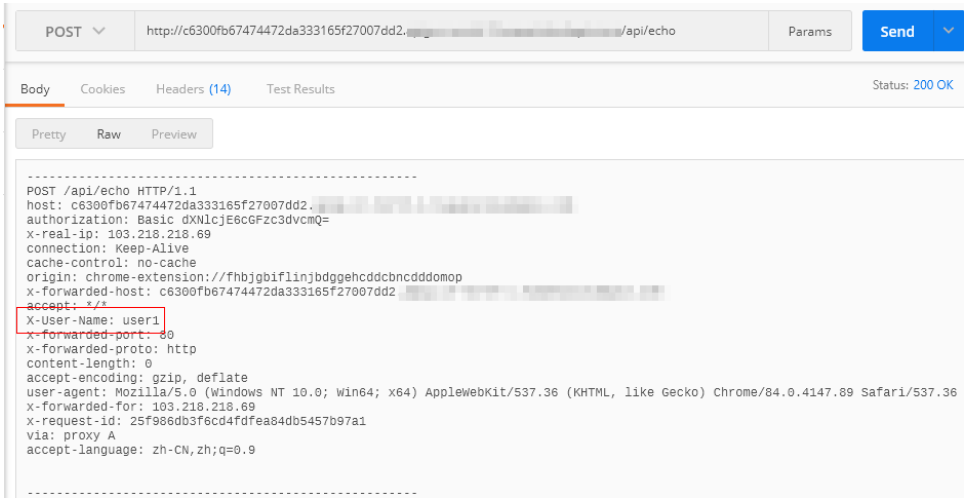
如果认证通过，函数返回的context信息，可以传到后端，配置方式如下：

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。



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。

版权所有 © 华为云计算技术有限公司



版权所有 © 华为云计算技术有限公司

4 API 网关专享版跨 VPC 开放后端服务

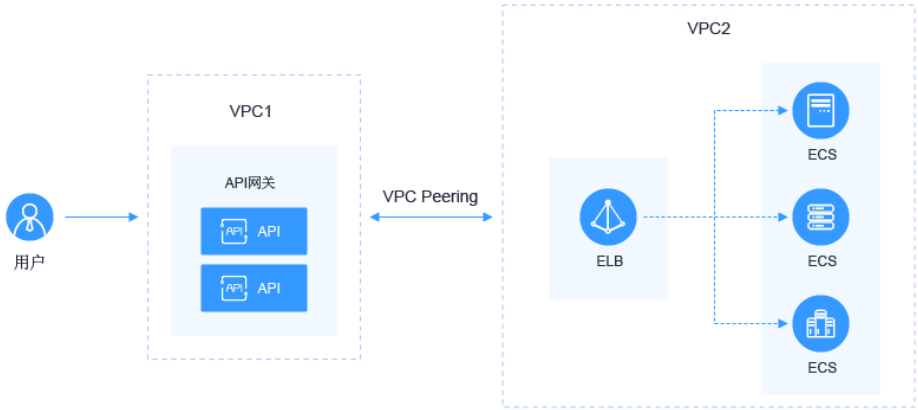
4.1 方案概述

应用场景

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

方案架构

图 4-1 API 网关跨 VPC 开放后端服务



方案优势

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

约束与限制

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

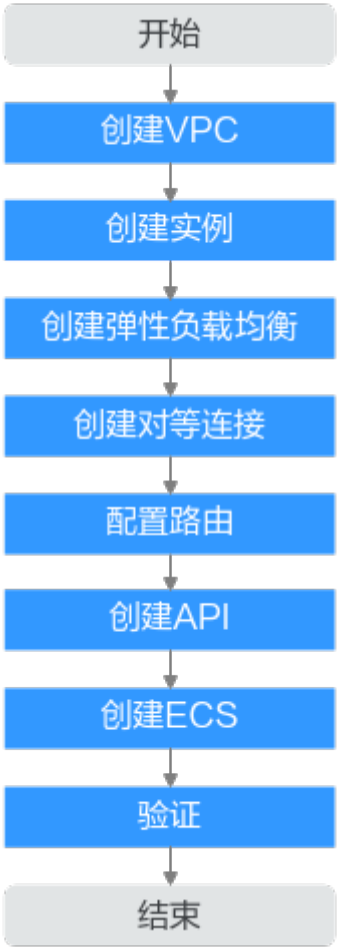
版权所有 © 华为云计算技术有限公司

4.2 资源规划

表 4-1 资源规划

资源	数量（个）
VPC	2
API专享版实例	1
ELB	1
ECS	1

4.3 操作流程



1. **创建VPC**
   创建两个VPC，VPC1为API网关所在VPC，VPC2为后端应用所在VPC。
2. **创建实例**

版权所有 © 华为云计算技术有限公司

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。

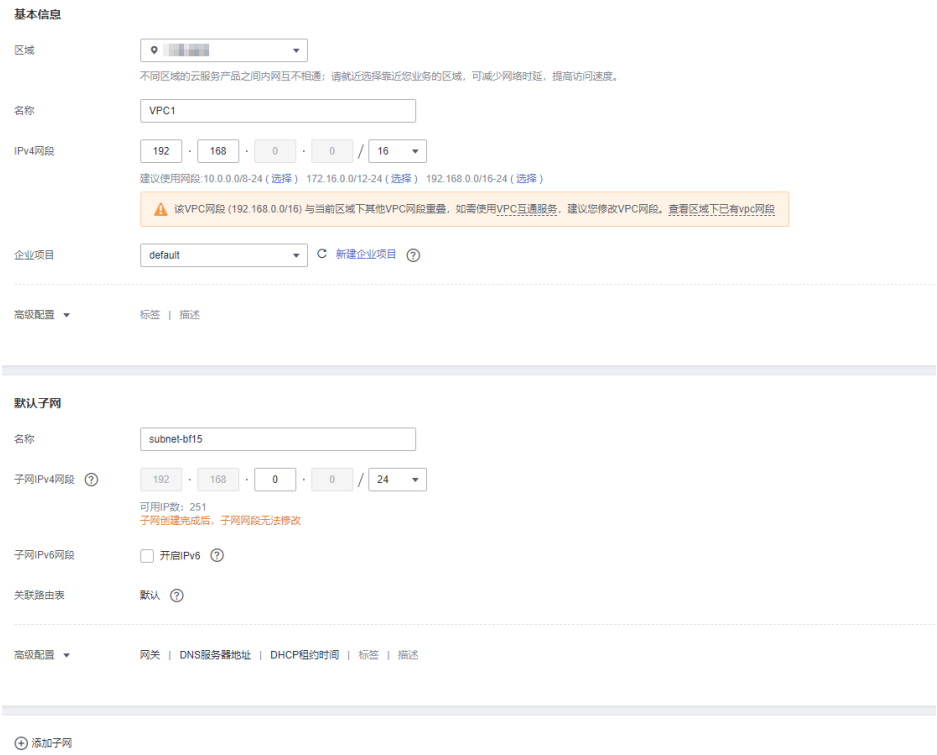
4.4 实施步骤

创建 VPC

步骤1 登录网络控制台。

步骤2 在左侧导航栏选择“虚拟私有云 > 我的VPC”。

步骤3 在“虚拟私有云”页面，单击“创建虚拟私有云”，请参考**表4-2**和**表4-3**配置信息。具体操作请参考《虚拟私有云服务用户指南》中的“创建虚拟私有云和子网”章节。



版权所有 © 华为云计算技术有限公司

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 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”。

版权所有 © 华为云计算技术有限公司

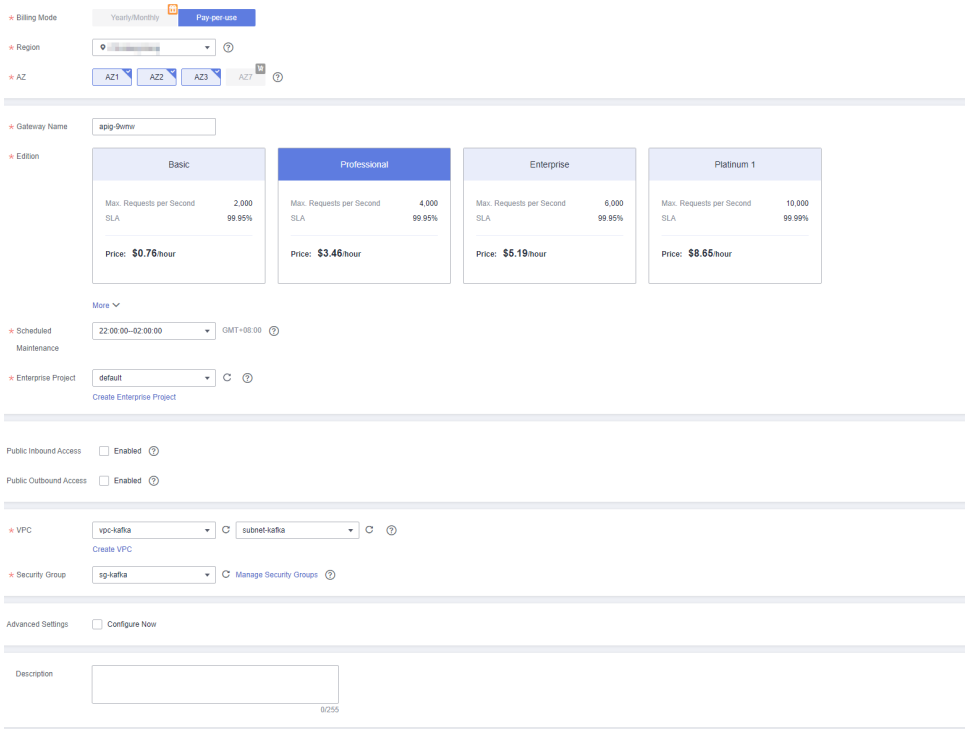


表 4-4 实例信息

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

步骤4 单击“立即购买”。

版权所有 © 华为云计算技术有限公司

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。单击“去支付”，实例开始创建，界面显示创建进度。

----结束

购买 ELB

步骤1 返回网络控制台。

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“购买弹性负载均衡”。

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。

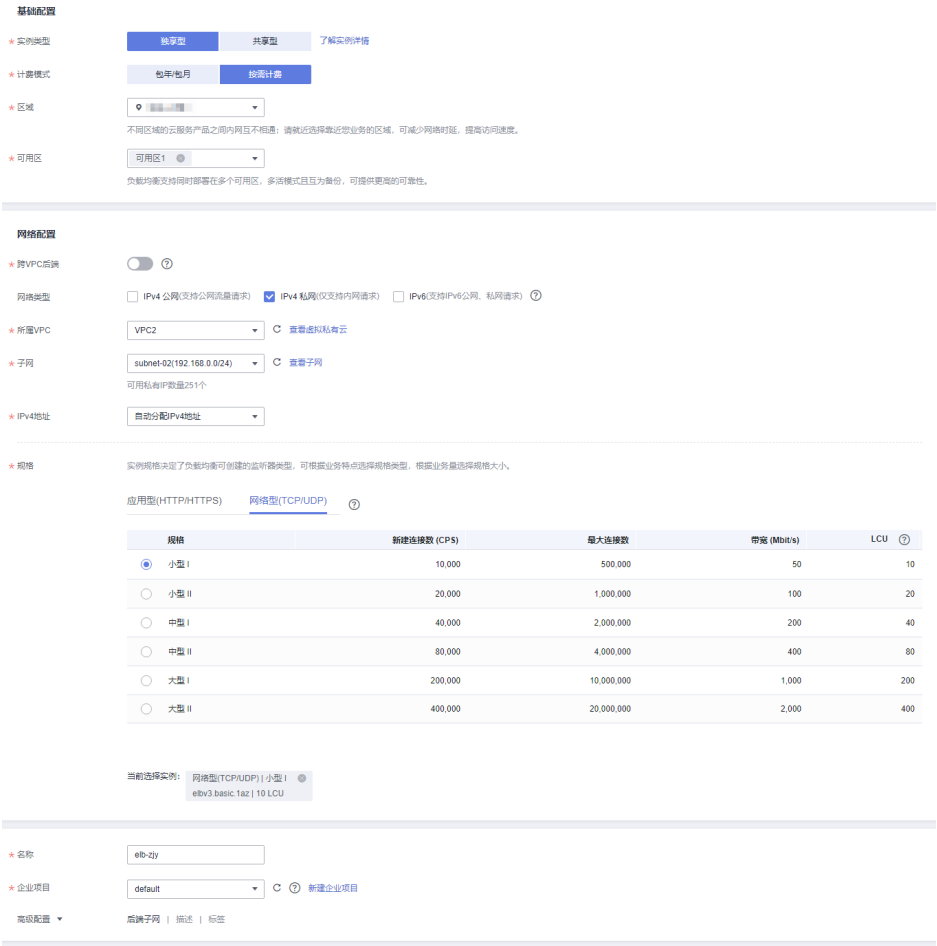


表 4-5 弹性负载均衡参数

参数	配置说明
实例类型	选择实例的规格类型。
计费模式	此处默认“按需计费”。
区域	选择实例所在的区域，且与VPC2同一区域。

版权所有 © 华为云计算技术有限公司

参数	配置说明
可用区	选择实例所在的可用区，此处选择“可用区1”。
网络类型	选择网络类型“私网”。
所属VPC	所属虚拟私有云，选择**已创建的虚拟私有云**“VPC2”。
子网	选择子网。
规格	选择“网络型”。
名称	填写弹性负载均衡的名称，根据规划自定义。建议您按照一定的命名规则填写实例名称，方便您快速识别和查找。
企业项目	选择实例所属的企业项目，此处选择“default”。

步骤5 单击“立即购买”。

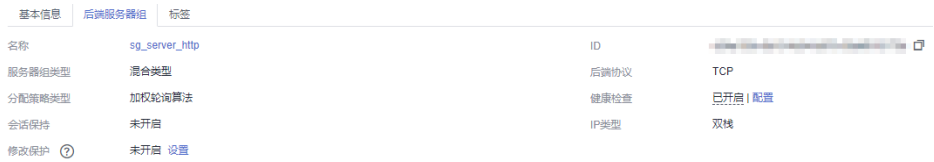
步骤6 确认信息无误后，单击“提交”。

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

图 4-3 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。

版权所有 © 华为云计算技术有限公司

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”。
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“查看路由”，进入对等对接详情页面。

步骤5 在“本端路由”页签中单击“路由表”，添加路由。

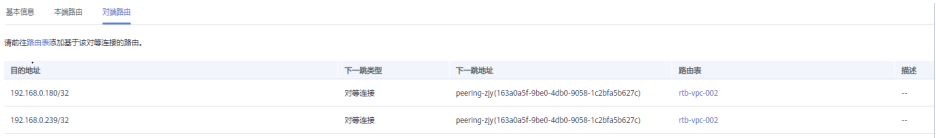
1. 在“路由”区域单击“添加路由”。
2. 在弹窗中填写路由信息。
   - 目的地址：为**ELB**详情页面，“基本信息”页签中的“服务地址”。
   - 下一跳类型：选择“对等连接”。
3. 单击“确定”。

图 4-4 本端路由

步骤6 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



----结束

版权所有 © 华为云计算技术有限公司

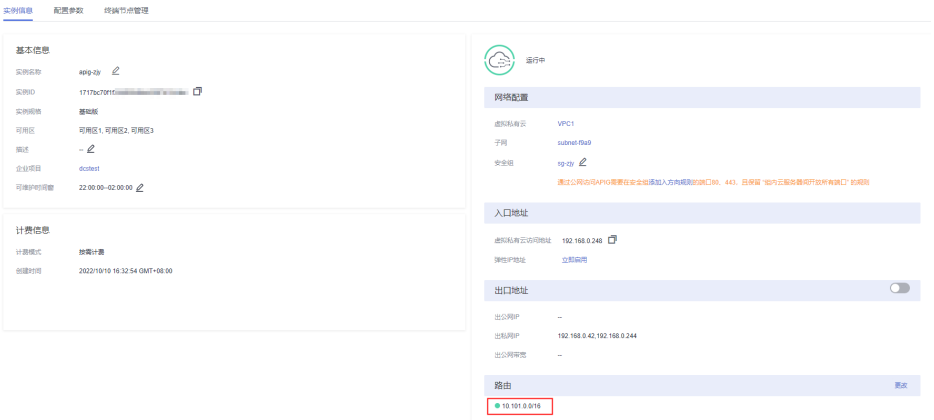
配置路由

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为购买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”。

步骤2 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”。
安全认证	选择API认证方式，此处选择“无认证”。

版权所有 © 华为云计算技术有限公司

步骤3 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：填写购买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

购买 ECS

步骤1 进入云服务器控制台。

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”。

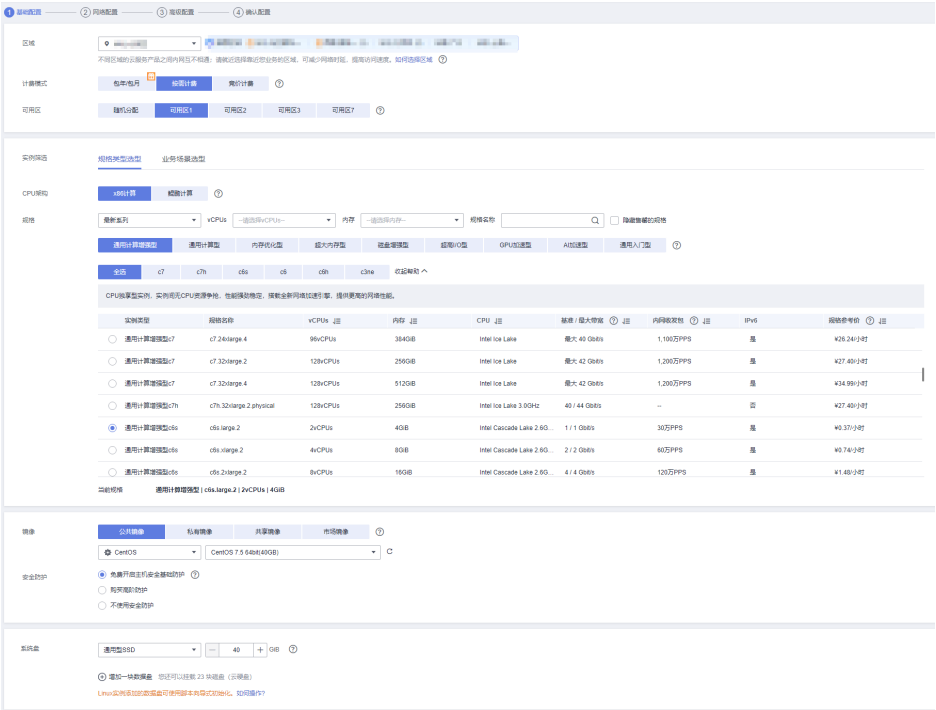


表 4-9 基础配置

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。

版权所有 © 华为云计算技术有限公司

参数	配置说明
计费模式	选择“按需计费”。
可用区	选择弹性云服务器所属可用区。
CPU架构	默认“x86计算”。
规格	根据业务规划，选择规格。
镜像	根据业务规划，选择镜像。

步骤4 网络配置后，单击“下一步：高级配置”。

表 4-10 网络配置

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

步骤5 高级配置后，单击“下一步：确认配置”。

表 4-11 高级配置

参数	配置说明
云服务器名称	填写弹性云服务器名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
登录凭证	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。

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“立即购买”。

----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。

版权所有 © 华为云计算技术有限公司

步骤2 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3 填写请求参数，单击“调试”。

状态码显示“200”表示调试成功。

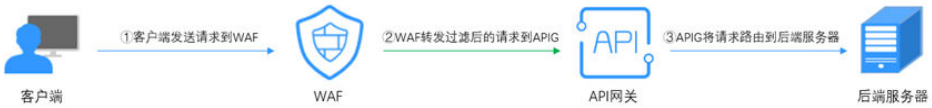
----结束

版权所有 © 华为云计算技术有限公司

5 API 网关专享版对接 Web 应用防火墙 WAF

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

图 5-1 后端服务器访问原理



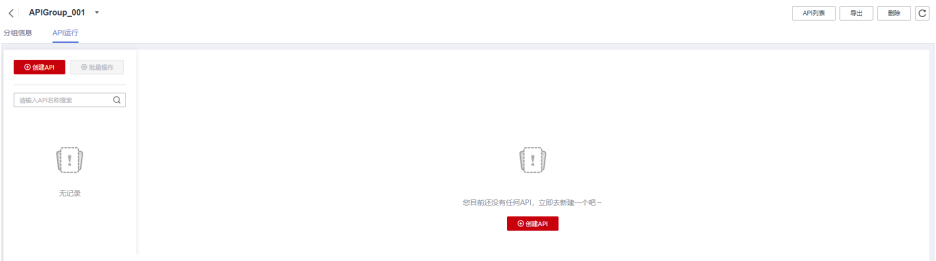
方案一（推荐）：WAF 侧注册对外访问域名并配置证书，通过 APIG 实例的分组调试域名访问后端服务

推荐原因：API分组通过域名方式对外提供服务，具备更强的可扩展性。

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

图 5-2 新建 API 分组并记录调试域名

图 5-3 新建 API

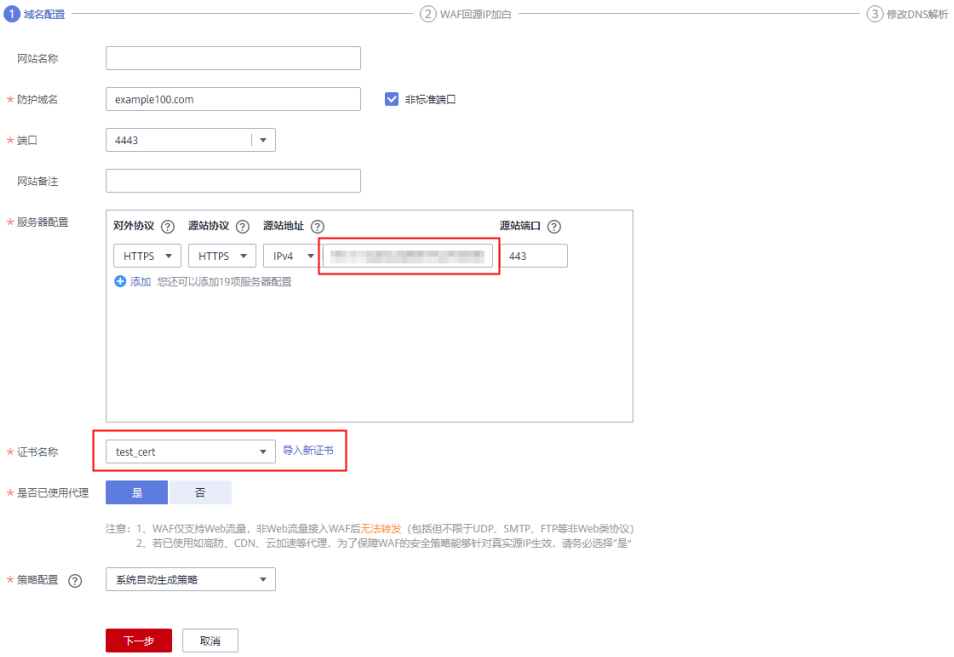


步骤2 在WAF侧添加防护域名时，配置“源站地址”填写为API分组的域名，并添加证书。详细操作步骤请参考**网站接入WAF**。

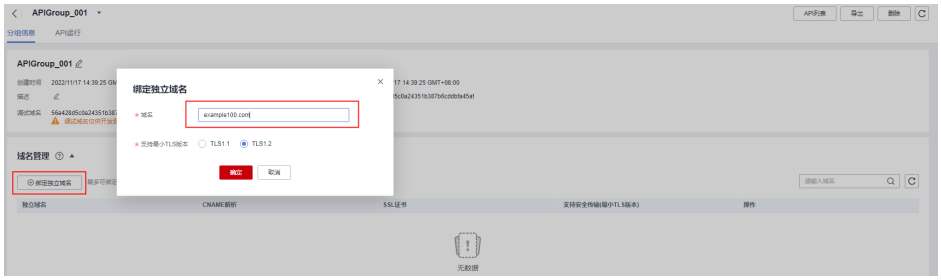
版权所有 © 华为云计算技术有限公司

说明

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



步骤3 在APIG实例中，为API分组绑定已创建的防护域名。

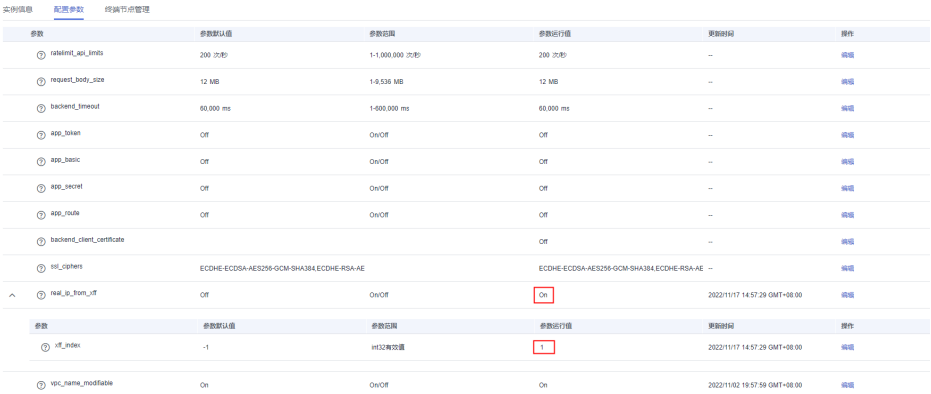


步骤4 在APIG实例中，将“real_ip_from_xff”开关打开，并设置参数运行值为“1”。

说明

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

版权所有 © 华为云计算技术有限公司



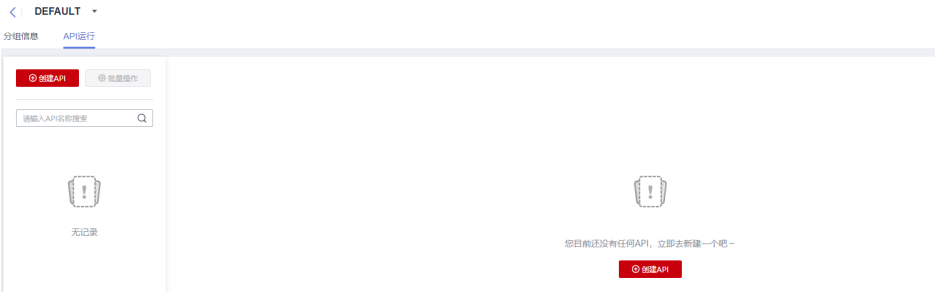
----结束

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

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

- 虚拟私有云访问地址为VPC内网地址。
- 弹性IP地址为公网地址。

步骤2 在DEFAULT分组中添加API。

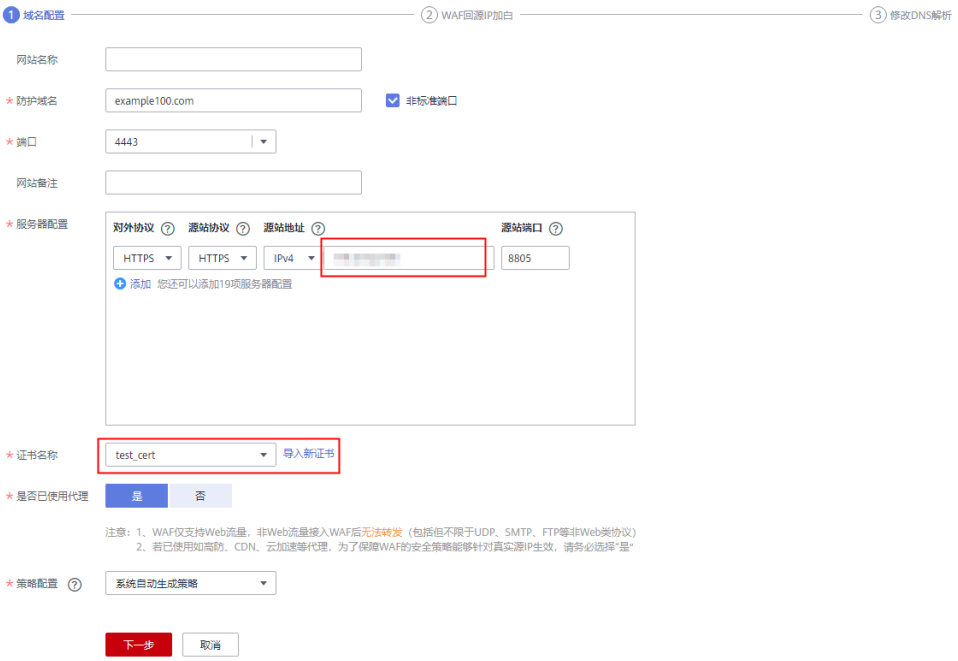


步骤3 在WAF侧添加防护域名时，配置“源站地址”为API网关实例的**入口地址**，并添加证书，以及复制WAF回源IP段。详细操作步骤请参考**网站接入WAF**。

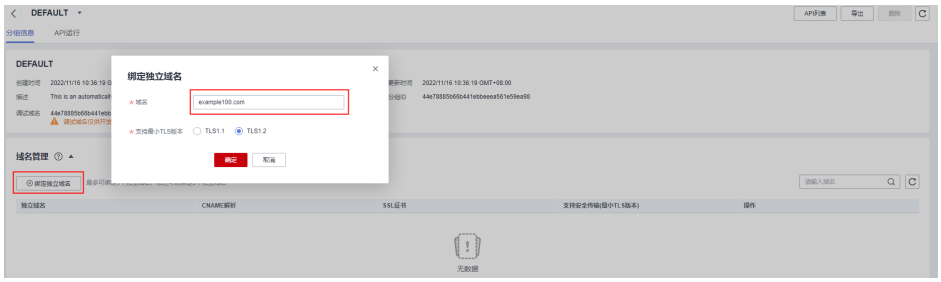
说明

- 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。

版权所有 © 华为云计算技术有限公司



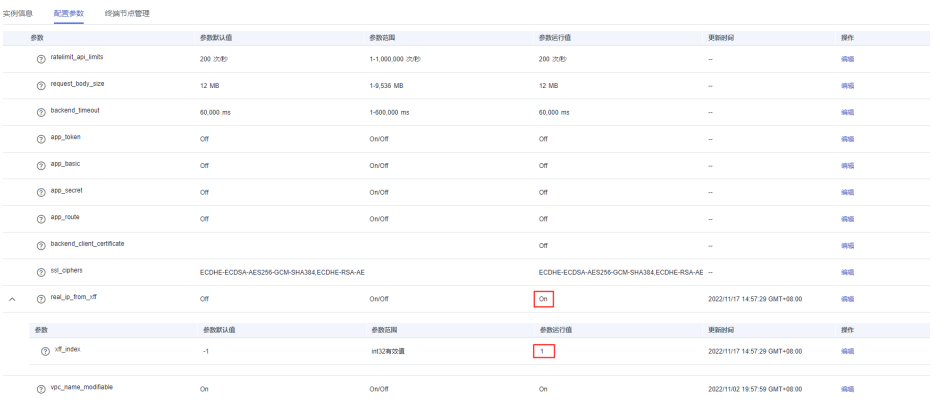
步骤4 在APIG实例中，为DEFAULT分组绑定已创建的防护域名。



步骤5 在APIG实例中，将“real_ip_from_xff”开关打开，并设置参数运行值为“1”。

说明

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



----结束

版权所有 © 华为云计算技术有限公司

6 API 网关专享版流量控制 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。）

版权所有 © 华为云计算技术有限公司

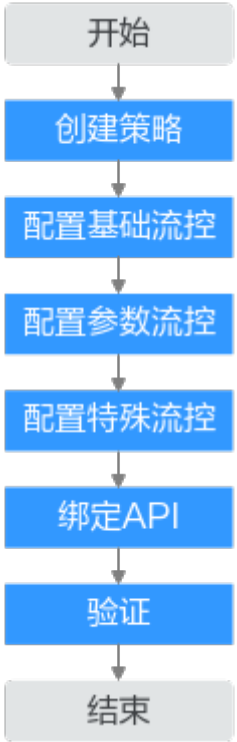
- 如果API未绑定流量控制2.0策略，流控限制值为实例“配置参数”中“ratelimit_api_limits”的参数运行值。
- 如果一个API绑定传统流量控制策略后，继续绑定流量控制2.0策略，传统流量控制策略会失效。
- 参数流控的规则最多可定义100个。
- 策略内容最大长度65535。
- 如果您的实例不支持流量控制2.0，请联系技术支持。

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。

版权所有 © 华为云计算技术有限公司

4. **配置特殊流控**

   开启特殊流控配置开关，特殊凭据与特殊租户流量控制的使用场景。

5. **绑定API**

   流量控制2.0策略绑定到API。

6. **验证**

   通过相应的请求URL调用API，验证流量控制2.0策略是否生效。

6.3 实施步骤

步骤1 创建策略。

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

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”。

版权所有 © 华为云计算技术有限公司

b. 在“定义规则”区域，单击“添加规则”，API流量限制设置为10次，时长为60秒；单击 编辑规则，设置“条件表达式配置”中匹配条件为“Host = www.abc.com”。

c. 单击“确定”，生成参数header为Host对应的匹配规则“Host = www.abc.com”，表示在60s内，对于请求头域中Host参数等于“www.abc.com”的API，且API调用次数达到10，参数流控生效。

2. 根据3、4，定义参数Path对应的多重规则。

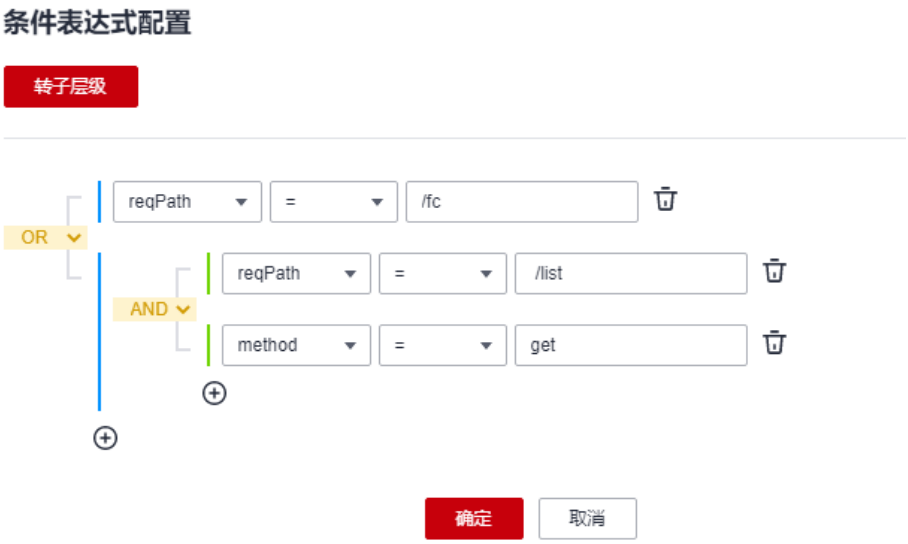
a. 在“定义规则”区域，单击“添加规则”，API流量限制设置为10次，时长为60秒；单击 编辑规则，设置“条件表达式配置”中的匹配条件。

b. 依次添加三个条件表达式，请求路径为“reqPath= /fc”和“reqPath= /list”，请求方法为“method=get”。

c. 单击“转子层级”，进一步划分子层级约束条件。

d. 两个请求路径“reqPath”条件表达式为互斥关系，故将“AND”关系改为“OR”，表示请求路径为“reqPath= /fc”或者“reqPath= /list”。

e. 将“reqPath= /list”和“method= get”两个匹配条件进行约束，选中二者，单击“确定转子层级”，匹配条件默认为“AND”关系。



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

版权所有 © 华为云计算技术有限公司

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

版权所有 © 华为云计算技术有限公司

7 API 网关专享版双重认证

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

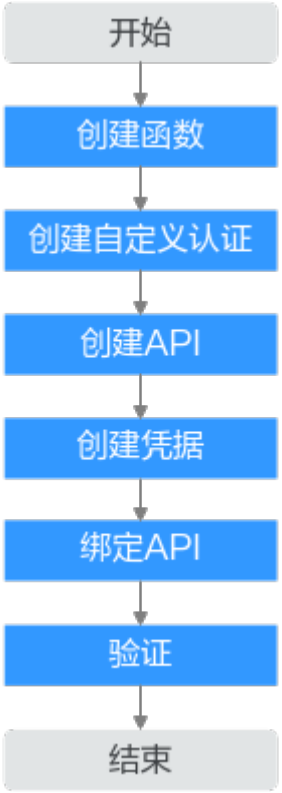
API网关在提供安全的APP认证模式下，用户可根据业务需求，灵活实现自定义认证，保障API的安全问题。

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。

版权所有 © 华为云计算技术有限公司

7.2 操作流程



1. **创建函数**

   创建自定义的前端函数，使用函数服务开发自定义认证。

2. **创建自定义认证**

   创建自定义认证，类型选择“前端”，函数地址选择上一步创建的函数。

3. **创建API**

   安全配置中的安全认证选择APP认证，并勾选“支持双重认证”，选择上一步创建的自定义认证。

4. **创建凭据**

   使用APP认证的API，需要在API网关中创建一个凭据，生成凭据ID和密钥对（Key、Secret）。

5. **绑定API**

   将创建的凭据绑定API后，才可以使用APP认证调用API。

6. **验证**

   调用API，验证双重认证是否设置成功。

7.3 实施步骤

步骤1 登录函数工作流控制台，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**。

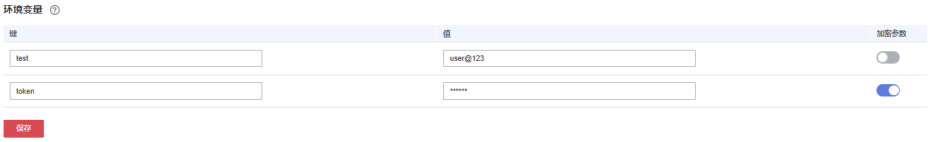
版权所有 © 华为云计算技术有限公司

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。



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

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

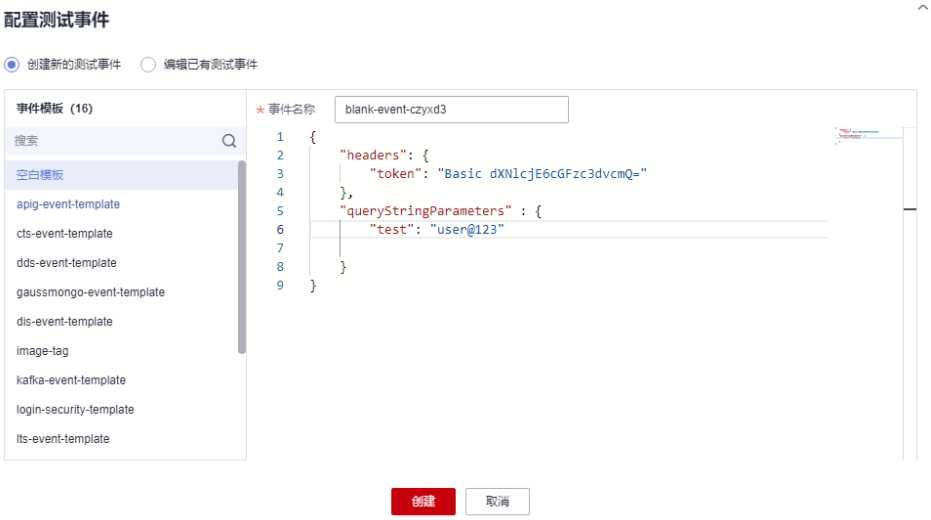
4. 配置测试事件并调试代码，然后部署。

   a. 在下拉框中选择“配置测试事件”并配置。

版权所有 © 华为云计算技术有限公司

说明

测试事件的参数值与环境变量中的参数值保持一致。



b. 创建测试事件完成后，单击“测试”调试代码。

c. 单击“部署”。

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

在“自定义认证”页签中，创建自定义认证。

表 7-2 自定义认证配置

参数	配置说明
认证名称	根据规划自定义名称。建议您按照一定的命名规则填写名称，方便您快速识别和查找。
类型	此处选择“前端”。
函数地址	单击“添加”，选择已创建函数。
版本或别名	默认“通过版本选择”。
缓存时间(秒)	30
身份来源	第一个身份来源参数位置选择“Header”，参数名填写“token”；第二个身份来源参数位置选择“Query”，参数名填写“test”。

版权所有 © 华为云计算技术有限公司

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

1. 根据下表参数，配置前端信息。

表 7-3 前端配置

参数	配置说明
API名称	填写API名称，建议您按照一定的命名规则填写，方便您快速识别和查找。
所属分组	默认“DEFAULT”。
URL	请求方法：接口调用方式，此处选择“GET”。 请求协议：选择API请求协议，此处选择“HTTPS”。 子域名：API分组创建后，系统为分组自动分配一个内部测试用的调试域名，此调试域名每天最多可以访问1000次。 路径：接口请求路径。此处填写“/api/two_factor_authorization”。
网关响应	API网关未能成功处理API请求，从而产生的错误响应。 默认的网关响应为“default”。
安全认证	选择API认证方式，此处选择“APP认证”。
支持双重认证	勾选后，开启双重认证。选择**已创建自定义认证**。

2. 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”。

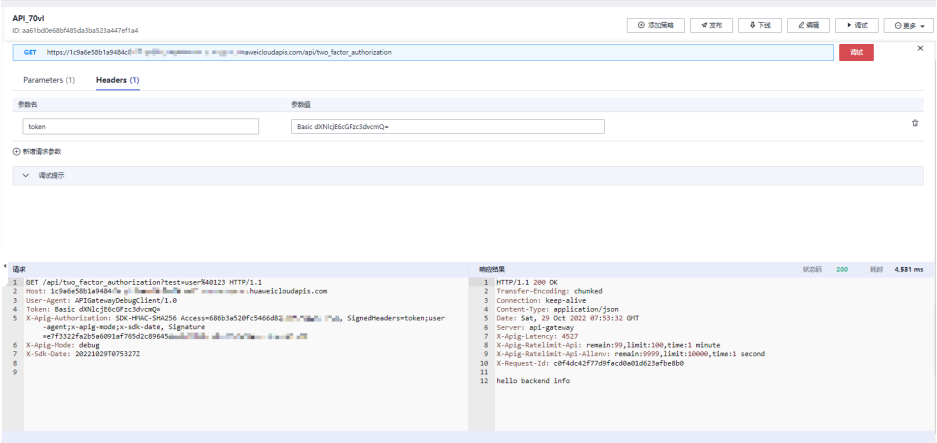
步骤5 绑定API。

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。

版权所有 © 华为云计算技术有限公司



- 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://1C[redacted]/api/two_factor_authorization?test=user%
40123" -H "token: Basic dXNlcjE6cGFzc3dvcmQ=" -H "Host: 1c9a6e58b1a9484c8737ec
[redacted].huaweicloudapis.com" -H "X-Sdk-Date: 20221029T08021
2Z" -H "Authorization: SDK-HMAC-SHA256 Access=cbbbf0ee627c4024bfc18[redacted]1
, SignedHeaders=host;token;x-sdk-date, Signature=37666681767904819ad3f8d6b37a5
8680589cb2045d[redacted]4"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Curren
t
                                 Dload  Upload   Total   Spent    Left  Speed
100    18    0    18    0     0     76      0 --:--:-- --:--:-- --:--:--    76
hello backend info
```

----结束

版权所有 © 华为云计算技术有限公司

8 API 网关专享版支持 http 到 https 自动重定向

8.1 方案概述

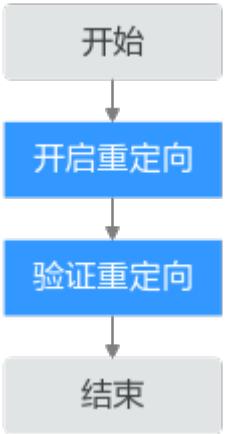
应用场景

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。

8.2 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”。

版权所有 © 华为云计算技术有限公司

2. **验证重定向**

   验证重定向功能是否生效。

8.3 实施步骤

说明

前提条件

- 已创建API或新创建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，在左侧导航栏选择“API管理 > API分组”。

步骤2 单击分组名称，进入API所属分组的详情页面。

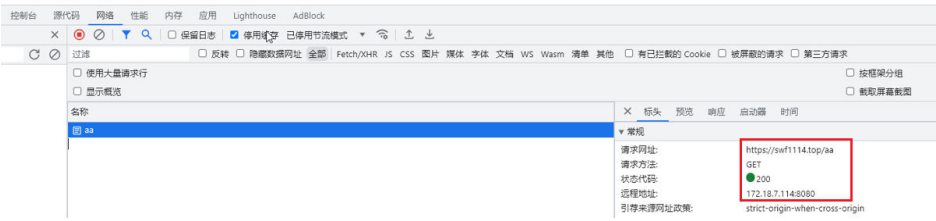
步骤3 在“分组信息”页签的“域名管理”区域，找到已绑定的独立域名，在“支持http to https自动重定向”列开启重定向功能。

----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。

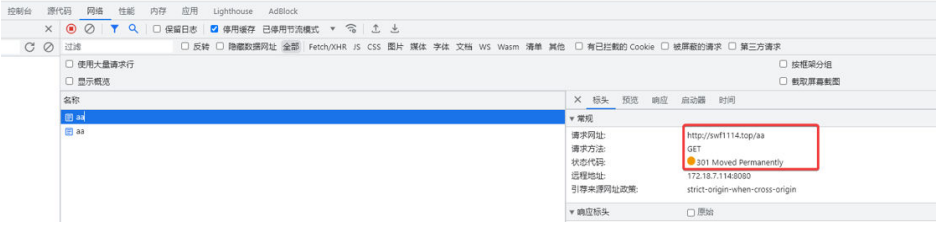
1. 在浏览器的地址栏中输入“https://*API请求路径*”后回车。
2. 在键盘上按F12。
3. 在“网络”页签中状态码显示“200”表示调用成功。



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。

版权所有 © 华为云计算技术有限公司



----结束

版权所有 © 华为云计算技术有限公司

9 基于 API 网关专享版实现 gRPC 服务的路由转发

9.1 方案概述

应用场景

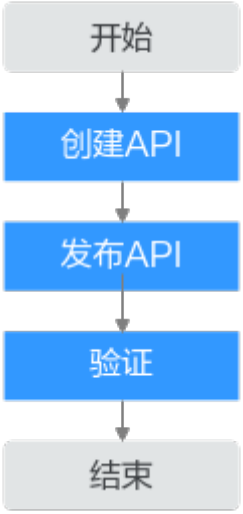
gRPC是RPC（远程过程调用）的一种，只需定义每个API的Request和Response，剩下的gRPC框架就可以完成。它的典型特征就是使用protobuf（protocol buffers）作为其接口定义语言（Interface Definition Language，缩写IDL），同时底层的消息交换格式也是使用protobuf。

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，不支持第三方认证、自定义认证策略。

9.2 操作流程



版权所有 © 华为云计算技术有限公司

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。

9.3 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服务接口的文件，通常在gRPC中使用。它基于Protobuf语言，用于描述数据的结构和交互方式，充当客户端和服务端之间通信的合同。

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。

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 配置前端信息后，单击“下一步”。

表 9-1 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，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”。

版权所有 © 华为云计算技术有限公司

参数	配置说明
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”。

步骤6 配置后端信息后，单击“下一步”。

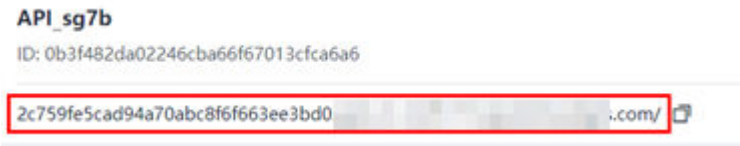
表 9-2 后端配置

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	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“/”。

步骤7 单击“完成”。

说明

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



----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”。

步骤2 选择API的发布环境，并填写发布说明。

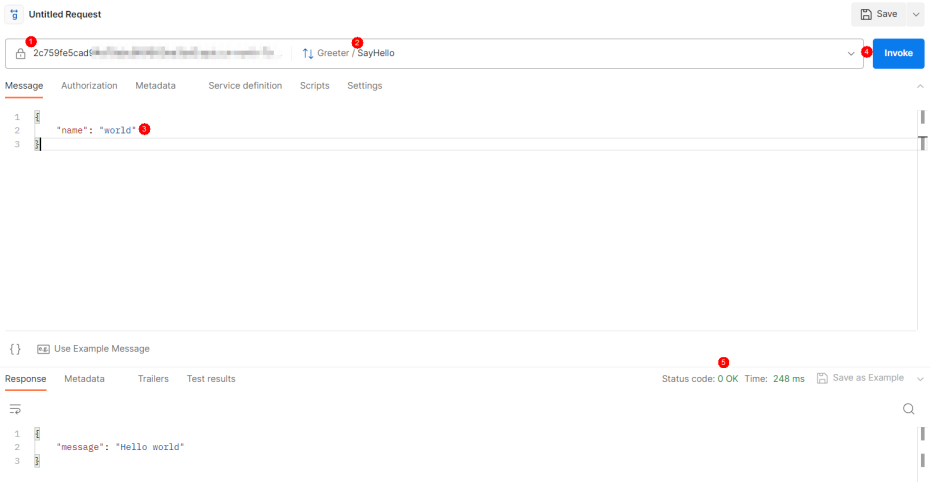
步骤3 单击“确定”，API发布成功后，“发布”按钮左上角的红色感叹号消失。

----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。

版权所有 © 华为云计算技术有限公司



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

版权所有 © 华为云计算技术有限公司

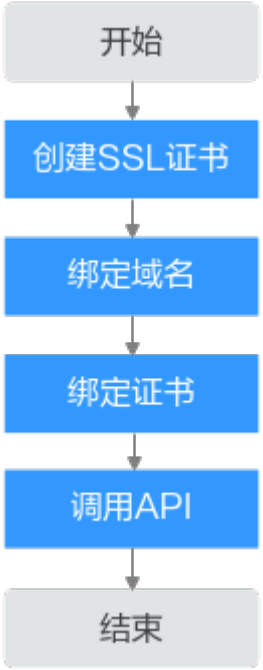
10 使用 API 网关专享版与客户端进行认证

10.1 方案描述

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。

10.2 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。

版权所有 © 华为云计算技术有限公司

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**
   将独立域名与已创建的SSL证书绑定。
4. **调用API**
   验证API是否调用成功。

10.3 实施步骤

单向认证

步骤1 进入API网关控制台页面。

步骤2 根据实际业务在左侧导航栏上方选择实例。

步骤3 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 10-1 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，建议您按照一定的命名规则填写，方便您快速识别和查找。
可见范围	此处选择“当前实例”。
证书内容	-----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----
密钥	-----Start RSA private key----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+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。

版权所有 © 华为云计算技术有限公司

3. 在“分组信息”页签中单击“绑定独立域名”。

表 10-2 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。

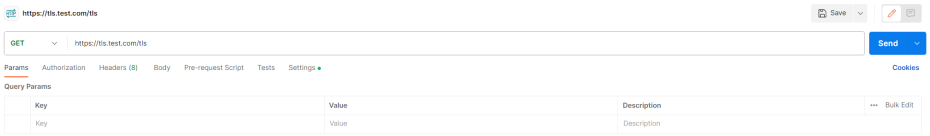
1. 在已绑定独立域名所在行单击“选择SSL证书”。
2. 选择已创建的证书单击“确定”。

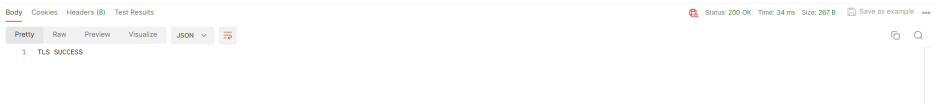
须知

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。





----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”。

版权所有 © 华为云计算技术有限公司

表 10-3 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，建议您按照一定的命名规则填写，方便您快速识别和查找。
可见范围	此处选择“当前实例”。
证书内容	填写证书内容。 -----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End certificate-----
密钥	填写密钥。 -----Start RSA private key----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+fSl ZheNAcv2hQR4aqJLi4wrcerTaRyG9op3OSh... -----End RSA private key-----
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，只要独立域名绑定此SSL证书，默认开启客户端认证。** -----Start certificate----- MIICXgIBAAKBgQC6ndRHy5Dv5TcZiVzT6qF iaMGy61ZIbUrmBhUn61vMdvOHmtblST+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 10-4 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”。

版权所有 © 华为云计算技术有限公司

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. 选择已创建的证书单击“确定”。

须知

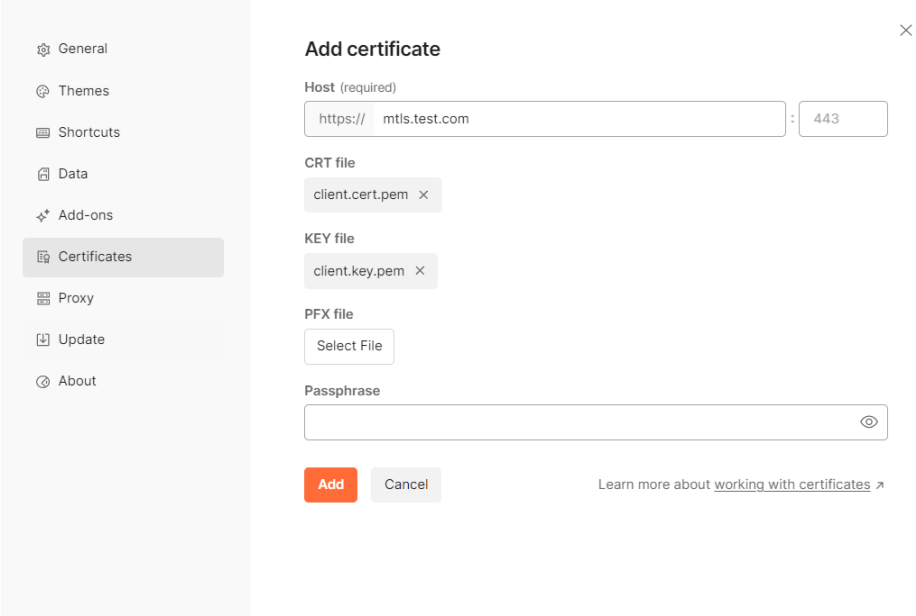
绑定证书后，自动开启双向认证。

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。

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的Certificates中添加Client certificates，上传客户端证书以及密钥。



----结束

版权所有 © 华为云计算技术有限公司