API 网关

FAQ

文档版本 03

发布日期 2024-03-28

华为云计算技术有限公司

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 热门咨询

API 创建

- 不使用VPC通道（负载通道）时，后端服务地址可以是什么？
- 后端服务地址是否一定要配置为ECS的地址？
- 后端服务是否支持绑定私网ELB地址？
- 后端服务地址支持填写私有地址（子网IP）吗？
- API网关可以绑定内网域名吗？

API 调用

- API调用失败的可能原因有哪些？
- API调用返回错误码如何处理？
- "The API does not exist or has not been published in the environment."如何解决？
- No backend available，怎么解决？
- 后端服务调用失败“Backend unavailable”或超时“Backend timeout”原因分析

API 认证鉴权

- 是否支持HTTPS的双向认证？
- “无认证”方式的API该怎么鉴权与调用？

API 控制策略

- 是否支持对请求并发次数做自定义控制？
- API调用是否存在带宽限制
- 怎样给指定的用户开放API
- 配置了身份认证的API，如何在特殊场景下（如指定IP地址）允许不校验身份？

API 导入导出

- API导入失败是什么原因？

- **swagger导入API的扩展字段有没有模板?**

2 API 创建

2.1 无法创建 API 是什么原因?

API免费创建。如果被限制操作，可能原因为用户欠费。

计费相关的详细指导，请参考计费说明。

2.2 API 的响应码如何定义?

API响应码分两种。

- 一种是网关响应码。当请求到达网关时，由于API的流量控制、访问控制策略以及认证失败，网关直接返回的响应信息。有关网关响应的详细指导，请参考网关响应。
- 一种是后端服务响应。响应信息由后端API服务（即API的提供者）定义，API网关只做透传。

2.3 使用 VPC 通道（负载通道），后端服务的主机端口怎么填写?

填写API后端服务的端口。

有关API后端配置的详细指导，请参考创建API。

2.4 不使用 VPC 通道（负载通道）时，后端服务地址可以是什么?

可以是公网域名或者公网IP（支持云服务器的弹性IP地址）。前提需要开启公网出口，

可以是内网的IP，不可以是内网域名。

2.5 后端服务地址是否一定要配置为 ECS 的地址?

后端服务地址可以配置为ECS的弹性公网IP，也可以配置为您自己服务器的公网IP地址，还可以配置为域名。

有关API后端配置的详细指导，请参考**创建API**。

2.6 后端服务是否支持绑定私网 ELB 地址?

- 专享版支持绑定私网ELB地址。
- 共享版不支持绑定私网ELB地址，请使用VPC通道。
- 如果是公网ELB地址，可直接使用。

2.7 后端服务地址支持填写私有地址（子网 IP）吗?

专享版：支持。实例所在同一个vpc子网内IP，或者通过专线打通的本地数据中心私有地址。

不支持专享版的网段：

- 0.0.0.0/8
- 10.0.0.0/8
- 100.125.0.0/16
- 127.0.0.0/8
- 169.254.0.0/16
- 172.16.0.0/12
- 192.0.0.0/24
- 192.0.2.0/24
- 192.88.99.0/24
- 192.168.0.0/16
- 198.18.0.0/15
- 198.51.100.0/24
- 203.0.113.0/24
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

共享版：不支持。后端服务如为相同Region下的弹性云服务器，且弹性云服务器未绑定弹性IP地址，请**使用VPC通道**，不能直接填写弹性云服务器的私有地址。

2.8 API 网关是否支持多后端节点方案?

支持。

通过VPC通道（负载通道）支持多后端节点，一个VPC通道中可以添加多个云服务器。

关于VPC通道（负载通道）的详细操作，请参考负载通道。

2.9 独立域名申请后还需要做什么?

独立域名完成注册、备案后，对于共享版，您需要将其CNAME解析到API分组对应的子域名；对于专享版，您需要将其A记录解析到实例的入口地址。解析成功后，即可使用。域名与API分组为多对一的关系，即一个分组最多能绑定5个独立域名，但一个域名只能解析到1个分组。

说明

如果您使用的公网域名，需要在DNS服务公网解析内注册CNAME记录（共享版）/A记录（专享版）。

如果您使用的内网域名，需要在DNS服务内网解析内注册CNAME记录（共享版）/A记录（专享版），还需要关联后端服务所属的VPC。

2.10 API 网关可以绑定内网域名吗?

对于共享版，域名必须完成备案，并将其CNAME解析到API分组对应的子域名。不能将无法在公网访问的域名，或者将他人所有的域名绑定给API分组。

对于专享版，可以配置内网域名，域名不需要备案，并将A记录解析到实例的入口地址。

2.11 为什么分组跨域配置失败?

1. 检查是否开启CORS。

   进入API详情，单击“编辑”，查看是否开启CORS。如果没开启CORS，请开启。

2. 检查是否创建OPTIONS方式的API，每个分组只需创建一个OPTIONS方式的API。

   说明

   参数配置如下：

   所属分组：选择已开启CORS的API所在分组。

   请求方法：选择OPTIONS。

   请求协议：选择与已开启CORS的API相同的请求协议。

   请求路径：选择与已开启CORS的API相同的请求路径或者与已开启CORS的API匹配的请求路径。

   匹配模式：选择前缀匹配。

   安全认证：“无认证”模式安全级别低，所有用户均可访问，不推荐使用。

   支持跨域CORS：勾选。

3 API 调用

3.1 API 调用失败的可能原因有哪些?

网络问题

调用API失败的场景分为三种：同一VPC内调用失败、不同VPC之间调用失败、公网调用失败。

- VPC内调用API失败时，请检查域名是否和API自动分配的域名一致，如果域名错误，会导致调用API失败。
- 不同VPC之间调用API失败时，请检查两个VPC的网络是否互通。如果不通，可以通过创建VPC对等连接，将两个VPC的网络打通，实现跨VPC访问实例。

  关于创建和使用VPC对等连接，请参考**VPC对等连接说明**或**API网关跨VPC开放后端服务**。
- 公网调用API失败时，可能的原因如下：
  - API没有绑定弹性公网IP（EIP），导致API缺少公网访问的有效地址，公网调用API失败。

    绑定EIP后重新调用即可，详细步骤请参考**网络环境准备**。
  - 入方向规则配置有误，导致公网调用API失败。

    配置入方向规则的详细步骤请参考**网络环境准备**。
  - 调用时未添加请求消息头“host:分组域名”，导致公网调用API失败。添加消息头后，重新调用即可。

域名问题

- 域名是否备案成功，且能正常解析。
- 域名是否绑定到正确的API分组。
- 子域名（调试域名）访问超过默认次数。API分组创建后，系统为分组自动分配一个内部测试用的子域名，此子域名唯一且不可更改，每天最多可以访问1000次。您可以通过添加独立域名来访问您开放的API。

发布问题

API是否已发布。如果修改过API，则需要重新发布；如果发布到非RELEASE环境，请求X-Stage头的值需要填写发布的环境名称。

API 认证鉴权

如果使用APP认证，App Key和Secret是否正确。

API 控制策略

- 访问控制策略是否设置正确。
- 是否超过了流量控制范围。系统默认的流控策略是单个API的访问不超过200次/秒，如果您未创建流控策略，API网关会执行默认流控策略。您可以在实例控制台“实例信息”页面中的“配置参数”页签下，通过修改“ratelimit_api_limits”参数来设置专享版API的默认流控策略。

3.2 API 调用返回错误码如何处理?

如果您直接调用自己创建的API，点此查询错误信息与解决方案。

如果您使用接口管理您的API，点此查询错误信息与解决方案。

3.3 API 调用报错“414 Request URI too large”

可能原因：URL（包括请求参数）太长，建议将请求参数放在body体中传递。

有关API调用的报错信息，请参考错误码。

3.4 "The API does not exist or has not been published in the environment."如何解决?

调用API网关中开放的API报错，请按以下顺序排查可能原因：

1. 调用API所使用的域名、请求方法、路径不正确。
   - 比如创建的API为POST方法，您使用了GET方法调用。
   - 比如访问的URL比API详情中的URL少一个“/”也会导致无法匹配上此API，例如http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test/和http://7383ea59c0cd49a2b61d0fd1d351a619.apigw.region.cloud.com/test会匹配上不同的API。
2. API没有发布。API创建后，需要发布到具体的环境后才能使用。具体操作请参考发布API。如果发布到非生产环境，检查请求“X-Stage”头是否为发布的环境名。
3. 域名解析不正确。如果API的域名、请求方法、路径正确，且已发布到环境，有可能是没有准确解析到您的API所在分组。请检查API所在的分组域名，例如您有多个API分组，每个分组有自己的独立域名，API调用时，使用了其他分组的独立域名。
4. 检查API是否使用OPTIONS跨域请求，如果使用OPTIONS跨域请求，请在API中开启CORS，并创建OPTIONS方式的API。具体操作请参考开启跨域共享。

3.5 No backend available，怎么解决?

- 检查后端服务是否可以访问，如果不能访问，请修改后端服务。
- 检查后端服务对应的ECS安全组配置，查看是否已开放您需要的端口。
- 检查后端服务地址是否使用公网IP地址，如果使用，需要在APIG控制台的“实例管理 > 查看控制台 > 实例信息”界面开启出口地址。
- 检查VPC网络中的ACL配置，查看是否有相关ACL策略限制了API网关实例与后端服务所在子网的通信。
- 如果使用VPC通道，检查VPC通道业务端口、健康检查端口、后端服务器添加是否均正常。

说明

共享APIG后端不支持配置内网ELB。

3.6 后端服务调用失败“Backend unavailable”或超时“Backend timeout”原因分析

以下原因可能导致后端服务调用失败或者超时，请逐一排查。

原因	解决方案
后端服务地址错误。	在编辑API中修改后端服务地址。 如果是域名，请确认域名能正确解析到后端服务IP地址。
后端超时时间设置不合理。 当后端服务没有在设置的后端超时时间内返回时，API网关提示后端服务调用失败。	在编辑API中增加后端超时时间。
如果“后端服务地址”在ECS（Elastic Cloud Server），ECS的安全组的出/入方向规则可能拦截了请求。	检查后端服务所在ECS的安全组，确保出/入方向端口规则和协议都设置正确。
请求协议配置错误，如后端服务为HTTP，在API网关配置为HTTPS。	创建的API与后端服务配置相同的协议。
API网关客户侧后端服务链接链路不通。	排查链接链路。

3.7 后端服务调用报错域名无法解析“Backend domain name resolution failed”

APIG实例所在的VPC完成了内网域名解析，后端服务调用仍报“域名无法解析”错误。

可能原因

APIG实例所在的VPC与用户后端服务所在的VPC存在网络隔离，内网域名解析仅在用户后端服务所在的VPC下能够解析。

解决方法

- 方法一：在创建API时，使用公网域名配置“后端服务地址”。
- 方法二：在创建API时，不使用VPC通道（负载通道），使用用户后端服务IP配置“后端服务地址”，添加常量参数，在HEADER中添加Host：域名字段。
- 方法三：在创建API时，使用VPC通道（负载通道）。
  a. 创建VPC通道（负载通道）。
  b. 添加用户后端服务地址。
  c. 创建API时，使用VPC通道（负载通道），配置自定义头域。

3.8 修改后端服务的超时时间上限“backend_timeout”后未生效

问题描述

修改APIG实例参数“backend_timeout”后未生效。

可能原因

在“定义后端服务”中，“后端超时(ms)”未修改。

解决方法

登录控制台，进入目标API详情，单击“编辑”，在“定义后端服务”中配置“后端超时(ms)”。

3.9 如何切换调用环境?

默认调用“发布”环境的API。

如果您要调用其他环境的API，请添加请求消息头X-Stage，参数值填写环境名称。

3.10 调用请求包最大支持多少?

共享版：API每次最大可以转发Body体为12MB的请求包。请求body体超过12M时，API网关会拒绝该请求。这种场景，推荐考虑使用对象存储服务。

专享版：API每次最大可以转发Body体为12MB的请求包。请求body体超过12M时，根据业务需求，请在“实例概览”的配置参数中修改“request_body_size”参数。“request_body_size”表示API请求中允许携带的Body大小上限，支持修改范围1~9536 M。

3.11 使用 iOS 系统时，如何进行 APP 认证?

目前API网关为APP认证提供了Java、Python、C、PHP、Go等多种语言的SDK与demo。

当您使用iOS系统（Objective-C语言）或者其他未包含在内的语言时，请参考**APP认证工作原理**的指导进行APP认证。

3.12 新建一个华为 IAM 认证方式的 API，在配置入参时为什么无法配置 HEADER 位置的 x-auth-token?

x-auth-token在API网关内部已经被定义了，如果您再次创建此参数名，容易导致冲突。

API网关控制台中已经限定您无法创建HEADER位置的x-auth-token，您只需在调用此API时，直接在header中增加x-auth-token和其值即可。

3.13 应用（凭据）问题汇总

Q：最多支持创建多少个应用（凭据）？

每个用户最多创建50个应用（凭据）。

Q：APP认证的API，怎样实现不同的第三方之间无法知道对方调用情况?

创建多个应用（凭据），并绑定同一个API，分发给不同的第三方不一样的应用（凭据）。

Q：APP认证的API，有没有限制可以给多少个第三方使用?

没有限制。

Q：APP认证的API，是否需要自己创建应用（凭据）？

是，需要自行创建应用（凭据），并绑定API。创建完成应用（凭据）后，系统自动生成AppKey和AppSecret，将AppKey和AppSecret给第三方，就可以直接调用此API了。

Q：APP认证的API，第三方怎么调用?

您需要把AppKey和AppSecret提供给第三方，然后第三方通过SDK调用。具体SDK的调用步骤请参见**使用APP认证调用API**。

3.14 是否支持移动应用调用 API?

API支持被移动应用调用。

使用APP认证时，将移动应用的AppKey和AppSecrect替换SDK中的AppKey和AppSecrect进行APP签名。

3.15 部署在 VPC 下的应用是否可以调用 API?

默认部署在VPC下的应用可以调用API。如果域名解析失败，则参考**配置内网DNS**，在当前终端节点上配置DNS服务器。配置完成后，部署在VPC下的应用可以调用API。

配置内网 DNS

配置DNS需要配置“/etc”目录下的**resolv.conf**文件，指定DNS服务器的IP地址。

内网DNS服务器的IP地址与您所位于的区域相关，您可通过**内网DNS地址表**获取内网DNS服务器的IP地址。

新增内网DNS服务器有两种方法。

- 方法一：修改虚拟私有云的子网信息。
- 方法二：编辑“/etc/resolv.conf”文件。

说明

方法二新增的内网DNS在弹性云服务器每次重启后会失效，需要重新进行配置。因此，建议使用方法一。

方法一:

您可以按如下步骤修改虚拟私有云的子网信息，将DNS服务器地址添加到弹性云服务器对应的子网中。

步骤1 在管理控制台左上角单击 ，选择区域。

步骤2 在服务列表中，单击“计算 > 弹性云服务器”，进入弹性云服务器管理页面。

步骤3 单击待使用的弹性云服务器名称，进入弹性云服务器详情页面。

步骤4 在“网卡”页签，单击 ，查看弹性云服务器的子网名称。

步骤5 在弹性云服务器“基本信息”页面中，查看弹性云服务器的虚拟私有云名称。

步骤6 单击虚拟私有云名称，进入“网络控制台 > 虚拟私有云”页面。

步骤7 在左侧导航栏单击“子网”。

步骤8 找到**步骤4**中对应的子网，单击子网名称。

步骤9 修改该子网的“DNS服务器地址”，单击“确定”。

例如，将“DNS服务器地址”修改为“100.125.1.250”。

步骤10 重启弹性云服务器。查看“/etc/resolv.conf”文件的内容，确认其中包含待配置的DNS服务器地址，并且DNS服务器地址位于其他DNS服务器地址之前。

例如，如下图所示，DNS服务器地址为“100.125.1.250”。

```
# Generated by NetworkManager
search openstacklocal
nameserver 100.125.1.250
nameserver 114.114.115.115
```

说明

对虚拟私有云的子网信息的修改会影响所有使用该子网创建的弹性云服务器。

----结束

方法二

编辑“/etc/resolv.conf”文件，新增内网DNS服务器地址。

例如，您位于“香港”，则需要在“/etc/resolv.conf”文件中新增一个IP地址为“100.125.1.250”的内网DNS服务器。

说明

- 新增的DNS服务器地址必须位于原有的DNS服务器地址之前。
- 保存“/etc/resolv.conf”文件后，DNS配置操作立即生效。

3.16 API 网关是否支持 WebSocket 数据传输?

API网关支持WebSocket数据传输。

在创建API时，请求协议中的HTTP相当于WebSocket的ws，HTTPS相当于WebSocket的wss。

3.17 API 调用是否支持长连接

支持。

注意适当使用长连接，避免占用太多资源。

3.18 策略后端有多个时，怎么匹配和执行

当您的API配置了多个策略后端，API网关会按顺序进行匹配，匹配到其中一个立即执行API请求转发，不会进行后续的匹配。

当策略后端都没有匹配成功，则按照默认后端执行API请求的转发。

3.19 API 调用对请求的响应消息体限制

API调用对请求的响应体大小没有限制。

API调用对请求的请求体大小有限制。详细指导请参考**request_body_size**。

3.20 如何通过 APIG 访问公网后端服务

通过开启公网入口访问，允许外部服务调用API。

如果您在调用API遇到网络问题，请参考**API调用失败的可能原因有哪些？**。

4 API 认证鉴权

4.1 是否支持 HTTPS 的双向认证?

专享版：支持。

- 前端双向认证。在绑定独立域名时，选择带有CA证书的**SSL证书**，默认开启客户端认证即双向认证。
- 后端双向认证。在创建API时，配置双向认证，在API网关和后端服务间启用双向认证。配置请参考**创建API**中的“TLS双向认证”参数说明。

共享版：不支持，API网关仅做HTTPS的单向认证。

4.2 “无认证”方式的 API 该怎么鉴权与调用?

“无认证”即API网关对收到的调用请求不做身份认证，您只需要按照API提供者提供的接口说明，封装规范的HTTP请求，发送给API网关即可。

说明

无认证方式下，API网关把请求内容**透传**给后端服务。因此，如果您希望在API后端服务进行鉴权，可以使用“无认证”方式，API调用方传递鉴权所需字段给后端服务，由后端服务进行鉴权。

4.3 TLS 加密协议支持什么版本?

API网关支持TLS 1.1及TLS 1.2版本，暂不支持TLS 1.0或TLS 1.3。

关于TLS版本的详细指导，请参考**绑定域名**。

4.4 API 签名认证是否支持自定义认证方式?

支持。

有关自定义认证详细指导，请参考**自定义认证**。

4.5 安全认证签名的内容是否包括 Body 体

包括。除了几个必选的请求头部参数，Body体也是签名要素之一。例如有一个使用POST方法上传文件的API，那么在签名过程中，会取这个文件的hash值，参与生成签名信息。

关于签名的详细指导，可参考：**签名认证算法详解**。

4.6 IAM 认证信息错误

IAM认证信息错误有：

- **Incorrect IAM authentication information: verify aksk signature fail**
- **Incorrect IAM authentication information: AK access failed to reach the limit,forbidden**
- **Incorrect IAM authentication information: decrypt token fail**
- **Incorrect IAM authentication information: Get secretKey failed**

Incorrect IAM authentication information: verify aksk signature fail

```
{
  "error_msg": "Incorrect IAM authentication information: verify aksk signature fail, ......
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

签名认证算法使用有问题，客户端计算的签名结果与API网关计算的签名结果不同。

解决方法

方法一：查看日志。

步骤1 获取API网关计算的canonicalRequest。

从报错信息的body中获取“request_id”，通过“request_id”查找shubao节点的error.log（error.log在CLS上查看），在error.log中获取canonicalRequest。

```
2019/01/26 11:34:27 [error] 1211#0: *76 [lua] responses.lua:170: rewrite():
473a4370fbaf69e42f9da243eb8f8c52;app-1;Incorrect IAM authentication information: verify signature
fail;SDK-HMAC-SHA256 Access=071fe245-9cf6-4d75-822d-c29945a1e06a, SignedHeaders=host;x-sdk-date,
Signature=b2ef2cddcef89cbfe22974c988909c1a94b1ac54114c30b8fe083d34a259e0f5;canonicalRequest:GE
T
/app1/

host:test.com
x-sdk-date:20190126T033427Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, client: 192.168.0.1, server:
shubao, request: "GET /app1 HTTP/1.1", host: "test.com"
```

步骤2 通过打印日志或调试中断的方式得到客户端计算的canonicalRequest，每种语言SDK中计算canonicalRequest的位置如下：

表 4-1 常见语言 SDK 中计算 canonicalRequest 的位置

语言	位置
java	libs/java-sdk-core-..*.jar中 com.cloud.sdk.auth.signer.DefaultSigner.class中的sign函数。
c	signer.c中的sig_sign函数。
c++	signer.cpp中的Signer::createSignature函数。
c#	signer.cs中的Sign函数。
go	signer.go中的Sign函数。
JavaScript	signer.js中的Signer.prototype.Sign函数。
python	signer.py中的Sign函数。
php	signer.php中的Sign函数。

例如，在调试中断位置获取的canonicalRequest。

```
POST
/app1/

host:test.com
x-sdk-date:20190126T033950Z

host;x-sdk-date
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

步骤3 比较**步骤1**和**步骤2**中的cannonicalRequest是否一致。

- 是，请检查appsecret或sk是否正确。（常见问题：appsecret或sk中多填了空格）
- 否。
  - 第1行不同：请求方法要保持一致。
  - 第2行不同：请求路径要保持一致。
  - 第3行不同：请求参数要保持一致。
  - 第4-5行不同：请求头信息，每行都要保持一致。
  - 第7行不同：请求头参数名个数要和请求头信息行数保持一致。
  - 第8行不同：请求body要保持一致。

表 4-2 比较 API 网关和客户端计算的 canonicalRequest

行数	参数	API网关	客户端
1	请求方法	GET	POST
2	请求路径	/app1/	/app1/
3	请求参数	空	空

行数	参数	API网关	客户端
4	请求头信息	host:test.com	host:test.com
5	请求头信息	x-sdk-date:20190126T033427Z	x-sdk-date:20190126T033950Z
6	空行	-	-
7	请求头参数名列表	host;x-sdk-date	host;x-sdk-date
8	请求body的hash值	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

----结束

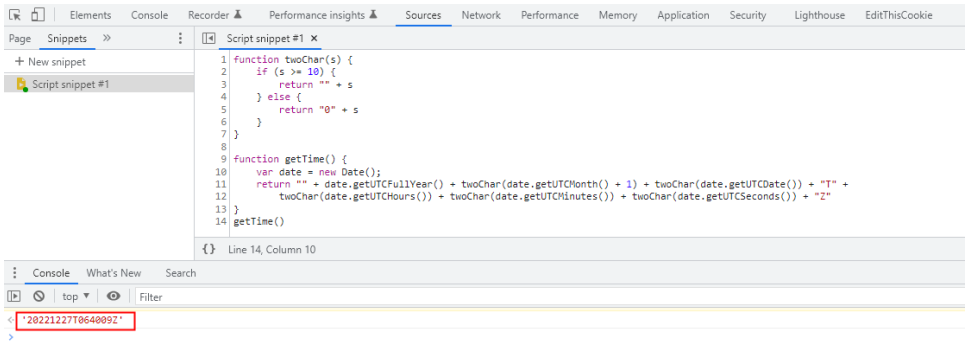
方法二：本地签名字符串比对。

步骤1 下载**js版本**，查看可视化签名SDK，获取签名字符串。

步骤2 解压压缩包，使用浏览器打开“demo.html”文件。

步骤3 获取x-sdk-date值，x-sdk-date值必须与当前时间相差在15min以内。

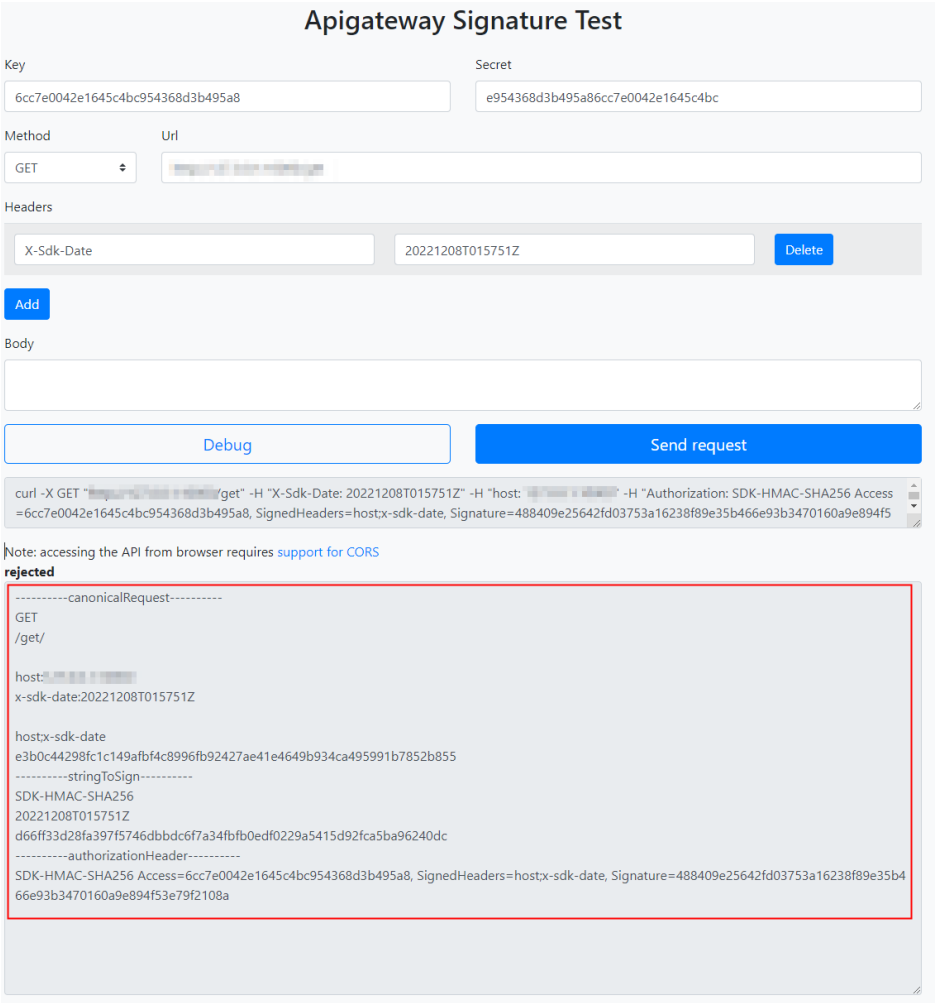
1. 在键盘中按下“F12”，并在页面中选择“Sources > Snippets > New snippet”。
2. 将以下代码复制到右侧的Script snippet中，然后在左侧右键Script snippet名称，选择“Run”后，“Console”中打印的值就是x-sdk-date值。




```
function twoChar(s) {
    if (s >= 10) {
        return "" + s
    } else {
        return "0" + s
    }
}

function getTime() {
    var date = new Date();
    return "" + date.getUTCFullYear() + twoChar(date.getUTCMonth() + 1) + twoChar(date.getUTCDate()) +
"T" +
        twoChar(date.getUTCHours()) + twoChar(date.getUTCMinutes()) + twoChar(date.getUTCSeconds()) +
"Z"
}
getTime()
```

步骤4 将x-sdk-date添加到Headers中，并填写其余参数，单击“debug”获取签名字符串。



非get\delete\head请求，需要携带body体，需要在上图Body框中添加body（格式与发送请求的body一致）。

步骤5 复制**步骤4**图中的curl命令，在cmd命令行中执行，curl命令执行后再进行下一步。

```
curl -X GET "http://192.168.0.1:10000/get" -H "X-Sdk-Date: 20221208T015751Z" -H "host:
192.168.0.1:10000" -H "Authorization: SDK-HMAC-SHA256 Access=6cc7e0042e1645c4bc954368d3b495a8,
SignedHeaders=host;x-sdk-date,
Signature=488409e25642fd03753a16238f89e35b466e93b3470160a9e894f53e79f2108a" -d $"
```

如果自定义authorization，则需要把curl命令里面的Authorization替换为自定义名称。

步骤6 比较本地代码中签名结果与js可视化签名结果。

例如排查java语言签名代码中的**canonicalRequest**、**stringToSign**、**authorizationHeader**值，与js可视化签名字符串是否一致。

```java
public void sign(Request request) throws UnsupportedEncodingException {
    String singerDate = getHeader(request, X_SDK_DATE);
    SimpleDateFormat sdf = new SimpleDateFormat( pattern: "yyyyMMdd'T'HHmmss'Z'");
    sdf.setTimeZone(TimeZone.getTimeZone("UTC"));

    if (singerDate == null) {
        singerDate = sdf.format(new Date());
        request.addHeader(X_SDK_DATE, singerDate);
    }
    addHostHeader(request);

    String messageDigestContent = calculateContentHash(request);

    String[] signedHeaders = getSignedHeaders(request);

    final String canonicalRequest = createCanonicalRequest(request, signedHeaders, messageDigestContent);

    final byte[] signingKey = deriveSigningKey(request.getSecrect());

    String stringToSign = createStringToSign(canonicalRequest, singerDate);
    byte[] signature = computeSignature(stringToSign, signingKey);
    String signatureResult = buildAuthorizationHeader(signedHeaders, signature, request.getKey());

    request.addHeader(AUTHORIZATION, signatureResult);
}
```

----结束

Incorrect IAM authentication information: AK access failed to reach the limit,forbidden

```
{
  "error_msg": "Incorrect IAM authentication information: AK access failed to reach the limit,forbidden." .....
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

- aksk签名计算错误。请参考**Incorrect IAM authentication information: verify aksk signature fail**解决方法。
- ak对应的sk不匹配。
- aksk频繁出现鉴权出错，连续错误5次以上，被锁定5分钟（5分钟内鉴权失败，误以为是异常的鉴权请求）。
- token鉴权时，token过期。

Incorrect IAM authentication information: decrypt token fail

```
{
  "error_msg": "Incorrect IAM authentication information: decrypt token fail",
  "error_code": "APIG.0301",
  "request_id": "******"
}
```

可能原因

用户的API所属IAM认证，TOKEN解析失败。

解决办法

- 检查获取token的方法，token是否正确。

- 检查获取token的环境与调用的环境是否一致。

Incorrect IAM authentication information: Get secretKey failed

```
{
"error_msg": "Incorrect IAM authentication information: Get secretKey failed,ak:******,err:ak not exist",
"error_code": "APIG.0301",
"request_id": "******"
}
```

可能原因

用户的API所属IAM认证，使用AK/SK签名方式访问，但是AK不存在。

解决方法

检查AK填写是否正确。

4.7 APP 认证信息错误

APP认证信息错误有：

- **Incorrect app authentication information: app not found, appkey xxx**
- **Incorrect app authentication information: verify signature fail, canonicalRequest**
- **Incorrect app authentication information: signature expired**

Incorrect app authentication information: app not found, appkey xxx

```
{
  "error_msg": "Incorrect app authentication information: app not found, appkey
01177c425f71487ea362ba84dc4abe5e1",
  "error_code": "APIG.0303",
  "request_id": "a5322eb89048eb41d705491a76a05aca"
}
```

可能原因

appkey配置错误。

解决方法

步骤1 在API网关控制台页面的左侧导航栏中选择“API管理 > 凭据管理”。

步骤2 单击对应的凭据名称，进入凭据详情。

步骤3 查看“Key”值，并重新配置appkey。

----结束

Incorrect app authentication information: verify signature fail, canonicalRequest

```
{
  "error_msg": "Incorrect app authentication information: verify signature fail, canonicalRequest:GET|/test/||
host:d7da6fe436fb48f2af3c5c2e5b203df7.example.com|x-sdk-date:20230527T015431Z||host;x-sdk-date|
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855",
  "error_code": "APIG.0303",
  "request_id": "cb141a91c945e68950a14a8eff5d62dc"
}
```

可能原因

签名认证算法使用有问题，客户端计算的签名结果与API网关计算的签名结果不同。

解决方法

请参考**Incorrect IAM authentication information: verify aksk signature fail**。

Incorrect app authentication information: signature expired

```
{
  "error_msg": "Incorrect app authentication information: signature expired, signature
time:20230527T000431Z,server time:20230527T020608Z",
  "error_code": "APIG.0303",
  "request_id": "fd6530a01c09807640189e65e837b8ad"

}
```

可能原因

客户端签名时间戳x-sdk-date与APIGW服务器时间相差超过15min。

解决办法

检查客户端时间是否正确。

5 API 控制策略

5.1 API 流量控制

5.1.1 是否支持对请求并发次数做自定义控制?

不支持。

流控策略只控制单位时间内调用次数，无请求并发次数控制。

5.1.2 每个子域名（调试域名）每天最多可以访问 1000 次，如果账号为企业账号，是否还有这个限制?

有。

每个子域名（调试域名）每天最多可以访问1000次的限制同样适用于企业账号。

有关子域名（调试域名）的详细指导，请参考绑定域名。

5.1.3 API 调用是否存在带宽限制

共享版API网关按照流控策略以及单个请求的最大Body体（12M）进行管控，没有直接限制带宽。

专享版API网关存在带宽限制，在创建实例时可以选择公网入口以及出口带宽。

5.1.4 流量控制策略不生效怎么办?

如果流控策略的API流量限制或源IP流量限制不生效，检查API是否绑定流控策略。

如果流控策略的用户流量限制不生效，检查API的安全认证方式是否为APP认证或IAM认证。

如果流控策略的应用（凭据）流量限制不生效，检查API的安全认证方式是否为APP认证。

5.2 API 访问控制

5.2.1 怎样给指定的用户开放 API

可以采用以下两种方式：

- 创建API时可选取APP认证方式，APP key和APP Secret分享给指定的用户。
- 使用访问控制策略，按照IP地址或者账号名，只允许符合允许策略的用户调用API。

5.2.2 配置了身份认证的 API，如何在特殊场景下（如指定 IP 地址）允许不校验身份？

认证方式不能基于某个特殊场景进行选择性认证。

- 方案1：创建API时选择无认证方式，然后利用“访问控制策略”功能进行IP白名单过滤，使得所有调用都不需要校验身份。
- 方案2：考虑拆分成2个API，其中一个使用身份认证（IAM认证或APP认证），另一个使用“无认证”并设置访问控制策略，以确保安全。

5.2.3 访问控制策略的 IP 地址是否取的客户端的 IP 地址？

访问控制策略的IP地址不一定取客户端的IP地址。

APIG的访问控制是根据$remote_addr的值进行校验。$remote_addr代表客户端的IP，它的值是服务端根据客户端的IP指定的，当客户端访问APIG时，如果中间没有任何代理，那么就会把remote_addr设为客户端IP；如果使用了某个代理，那么客户端会先访问这个代理，然后再由这个代理转发到APIG，这样就会把remote_addr设为这台代理机的IP。

6 API 发布

6.1 对 API 的修改是否需要重新发布?

需要。

API发布后，如果再次编辑API参数，需要重新发布才能将修改后的信息同步到环境中。

关于API重新发布的详细指导，请参考**发布API**。

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

API发布到非RELEASE环境可以访问，添加x-stage请求消息头后即可访问。

例如：

```
r.Header.Add("x-stage", "RELEASE")
```

您也可以参考**调用API**章节中的示例。

6.3 API 发布到不同环境后，会调用不同的后端服务吗?

使用环境变量，或者在后端服务定义不同的参数，可以实现API发布到不同环境时，调用不同的后端服务。

有关环境变量的详细指导，请参考**创建环境变量**。

6.4 API 调试的时候，如何指定环境?

不能指定。

API网关控制台提供的调试功能，用的是特定的debug环境，调试完成后需先发布到对应环境，之后可使用代码或者postman等工具，并添加请求消息头X-Stage，才能访问指定环境。

7 API 导入导出

7.1 API 导入失败是什么原因?

可能原因1：单次导入的API数量超出上限。当前单次最高能导入300个API，如超出此数量，请分批导入，或提交配额修改工单，调整API单次导入上限。

可能原因2：参数错误，需要检查和修正。建议先在API网关控制台界面创建一个API，将其导出作为API文件的模板。

可能原因3：YAML文件格式问题，需要检查和修正。

可能原因4：本地proxy网络限制，更换网络环境。

可能原因5：定义API请求中，不允许在Header定义“X-Auth-Token”字段。

7.2 swagger 导入 API 的扩展字段有没有模板?

模板在开发中。

您可以先配置好1~2个API，再导出作为模板。

8 API 安全

8.1 怎样保护 API?

- 使用身份认证

  创建API时，为API调用增加身份认证，如使用IAM认证或API网关提供的APP认证，防止API被恶意调用。

- 设置访问控制策略

  从IP地址（或地址区间）以及账号等不同维度，设置白名单/黑名单。

- 将API绑定流控策略，通过流控策略保护API。

  API网关默认API流量控制为每秒200次，如果您的后端服务不能支撑单个API 200次/秒的调用请求，可设置流量控制策略，将限额调低。

8.2 怎样保证 API 网关调用后端服务器的安全?

通过以下方法确保API网关调用后端服务器的安全：

- 为API绑定签名密钥。

  在绑定签名密钥后，API网关到后端服务的请求增加签名信息，后端服务收到请求后计算签名信息，验证计算后的签名信息与API网关的签名信息是否一致。

- 使用HTTPS对请求进行加密。

  需要确保已有相应的SSL证书。

- 使用后端认证：

  您可以对后端服务开启安全认证，只受理携带正确授权信息的API请求。在创建API的定义后端服务阶段，可以开启后端认证。

8.3 能否针对 VPC 通道（负载通道）内的 ECS 私有 IP 进行访问控制

不支持。

9 其他

9.1 API、环境、应用（凭据）之间的关系?

API可以被发布到不同的环境中。比如RELEASE和BETA两个环境，分别代表线上和测试环境。

应用（凭据）指代一个API调用者的身份。创建应用（凭据）时，系统会自动生成用于认证该身份的应用（凭据）key&secret。将指定的API授权给指定应用（凭据）后，该应用（凭据）的持有者才可以调用已发布到环境中的指定API。

同一个API发布到不同的环境时，可以为之定义不同的流控策略并授权给不同的应用（凭据）。举例，API v2版本在测试过程中，可以发布到BETA环境，并授权给测试应用（凭据），而API v1版本是稳定版本，可以在RELEASE环境中，授权给所有用户或应用（凭据）使用。

9.2 怎样使用 API 网关?

API网关提供了以下方式来管理/调用API：

- Web化的服务管理平台，即管理控制台。

  如果您已注册云服务，可直接登录管理控制台，单击管理控制台左上角 ☰，然后单击“API网关 APIG”。

  有关管理控制台的功能描述以及操作使用指导，请参考《API网关用户指南》。
- 基于Java、Go、Python、Javascript、C#、PHP、C++、C、Android等多种语言的SDK包。

  您可以通过下载SDK包来调用API，具体操作请参考《API网关开发指南》。

9.3 API 网关支持哪些 SDK 语言?

API网关当前支持Java、Go、Python、C#、javascript、PHP、C++、C和Android的SDK。

关于SDK的详细指导请参考**《API网关开发指南》**。

9.4 API 网关是否支持通过 POST 方法上传文件?

API网关支持通过POST方法上传文件。

共享版：API每次最大可以转发Body体为12MB的请求包。

专享版：在实例配置参数中，配置“request_body_size”参数。“request_body_size”表示API请求中允许携带的Body大小上限，支持修改范围1~9536 M。

说明

目前仅支持对请求体透传。

9.5 如何获取 API 网关错误返回信息?

当API请求到达网关后，网关返回请求结果信息。查看返回结果的Body信息如下。

```
{
    "error_code": "APIG.0101",
    "error_msg": "API not exist or not published to environment",
    "request_id": "acbc548ac6f2a0dbdb9e3518a7c0ff84"
}
```

- “error_code”表示错误码。
- “error_msg”表示报错原因。

9.6 API 网关如何开放部署在华为云上的服务?

- 如果部署在华为云上的服务绑定了公网IP地址，在API网关中创建API时，使用**公网IP地址:端口号**作为后端服务地址。如果此服务已绑定域名，则优先使用域名作为后端服务地址。创建API的详细步骤请参见**创建API**。

- 如果部署在华为云上的服务无公网IP地址，则将此服务的访问方式设置为VPC内网访问，在API网关中创建API时，通过VPC通道访问部署在VPC内的此服务。创建VPC通道和API的详细步骤请参见**创建负载通道**和**创建API**。

9.7 API 网关共享版是否可以升级到专享版?

暂不支持一键升级，但可以平滑迁移，您可以参考以下方案：

1. 新购买专享版实例。
2. 导出共享版中的API。
3. 将API导入到专享版。
4. 重新绑定域名，并修改DNS解析记录至专享版实例的公网访问入口。

9.8 API 网关控制台所有按钮均无法单击

请检查账号是否欠费，并进行续费处理。

计费相关指导，请参考**计费说明**。