API 网关

快速入门（开放 API）

MORE THAN JUST CLOUD | Alibaba Cloud

快速入门（开放 API）

概述

本文将快速引导您创建并开放API。

您需要依次完成以下步骤才能成功开放API服务：

步骤 1：创建 API 分组

API 分组是 API 的管理单元，先创建 API 分组，然后在分组下创建 API。

> 分组有 **Region** 属性，API 选定分组就选定了 **Region**，不可更改。
>
> 分组创建时，会绑定一个唯一的二级域名，您可以访问该二级域名调用该分组下测试中的 API。
>
> 若要开放 API 服务，您需要为分组绑定独立域名，独立域名需要在阿里云系统备案并且 CNAME 到该分组的二级域名上，用户访问独立域名时会调用该分组下线上的 API。
>
> 如果您的 API 支持 HTTPS 协议，您还需要为该独立域名上传 SSL 证书。

步骤 2：绑定域名和证书

域名是绑定在 API 分组上面的，API 网关通过域名来定位到一个唯一的 API 分组，再通过Path+HTTPMethod确定唯一的 API。

如果您需要开放 API 则需要为分组绑定独立域名。独立域名需要满足以下几点：

- 独立域名需要在 阿里云备案 或者在 阿里云备案接入。
- 独立域名要 CNAME 解析到该分组的二级域名上，然后操作绑定。先解析，后绑定，否则绑定操作会报错。
- 若您需要将其他分组的独立域名变更到当前分组，需要先变更解析，才能成功绑定。

若该分组下的 API 支持 HTTPS 协议，您还需要为该独立域名上 SSL 证书。不支持文件上传，需要填写证书名称、内容和私钥。

步骤 3：创建 API

API 分组创建完成您就可以创建 API 了，创建 API 是定义 API 请求的过程。您需要在创建中依次定义以下内容：

1. API 的基本信息：分组、API 名称、API 类型、API 认证方式、描述。
2. API 请求：协议、Method、Path、入参。
3. API 服务：后端服务协议、后端服务 Method、后端服务地址、后端服务 Path、服务超时时间、参数映射、系统参数、常量参数。
4. API 返回结果：返回类型及示例，目前网关对于返回结果不做处理，直接透传给请求者。后续会支持用户定制化、格式化的定义返回信息。

至此完成 API 的创建，并且具备开放的条件。操作详细说明请看 使用手册（开放API）。

步骤 4：发布 API

完成 API 创建后，需要进行调试、测试和正式上线 API。

操作步骤：

1.调试

您要把 API 发布到测试环境，然后在 API 网关控制台的调试页面上调试 API。

调试时，会跳过 **APP 鉴权** 和 **签名校验** 环节，只是调试 API 的请求链路是否正确。

如果您勾选了 Mock，就是把返回结果定义为一个常量，然后调试时不会真的去请求后端服务，而会直接返回常量结果。这种 Mock 调试模式，不要求后端服务完备。

如果未勾选 Mock，则网关会真实地请求后端服务。返回信息里可能有网关的 X-Ca 开头的返回信息，也会有底层服务真实返回的信息。

2.测试

为了模拟真实的用户请求，您可以自己创建一个 APP，操作您的 API 给这个 APP 授权。

然后按照真实的请求场景，写代码或者基于网关提供的 SDK 样例 请求 API。

您可以将 API 发布到测试或者线上环境，在绑定独立域名之前，可以直接访问二级域名来进行测试调用。请求时注意指定环境，若不指定则默认为访问线上。参见 API 调用示例。

调用API的方法，请您查看 使用手册（调用 API）。

3.发布

完成测试后，您就可以把 API 开放出去了。

要上架到 API 市场则必须将 API 发布到线上，且 API 的类型应为公开。

对外开放的 API，应在所属分组上绑定独立域名，直接访问二级域名有流控限制为1000次/天。

API 网关支持对测试/线上的 API 做版本管理，您可以发布 API、下线 API 还可以切换版本，切换版本是实时生效。

步骤 5：授权给应用

授权给应用

应用（APP）代表请求者的身份。

当您的客户或者您自己测试调用 API 时，都需要创建 APP 作为请求者的身份，然后由您操作给 APP 授权。

> 如果您的 API 已经上架云市场，购买者能够给自己的 APP 授权，不需要您再配置。

无购买行为时的授权操作需要以下几个步骤：

i. 获知待授权的 APP 的 AppID 或者 APP 所有者的阿里云邮箱账号。
ii. 在授权操作页面，选择一个或者多个准备开放调用权限的 API，选定 **测试/线上**。
iii. 选定 API 后，用 AppID 或者阿里云邮箱账号搜索到 APP。
iv. 确认授权。

注意：授权是区分环境的，同一个API、同一个APP，在两个环境需要分别授权，避免因为授权的环境和请求的环境不一致，导致报错。

步骤 6：安全服务

接下来您可以配置安全防护设置。目前 API 网关为您提供**后端服务签名密钥**和**流量控制策略**两种安全措施。

后端服务签名密钥主要是用于您后端验证网关的身份，在网关请求您后端时，保障您后端的安全。

签名密钥的 **Key** 和 **Secret** 都是您自定义的，您将创建的密钥绑定到 API 上后，相当于网关请求这个 API 时需要出示这一对 **Key** 和 **Secret**，您后端通过验证签名字符串来验证网关的身份。具体后端签名密钥的说明请参见 后端签名密钥说明文档。

流量控制策略用于您管控 API 服务的流量，详见 流量控制策略。

您还可以在控制台进行更多 API 生命周期的管理操作，如 API 下线、API 版本切换、API调 用情况监控和预警等。更多详情请您查看 使用手册（开放API）。