ALIBABA CLOUD

阿里云

API 网关

运维监控

文档版本：20220513

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.API网关监控

本文主要介绍管理员如何在API网关查看API的调用情况。

概述

API网关的监控支持查看 region（地域）、分组、以及API 的监控图表，监控图表的指标主要包含请求数、流量、延时、HttpStatusCode。

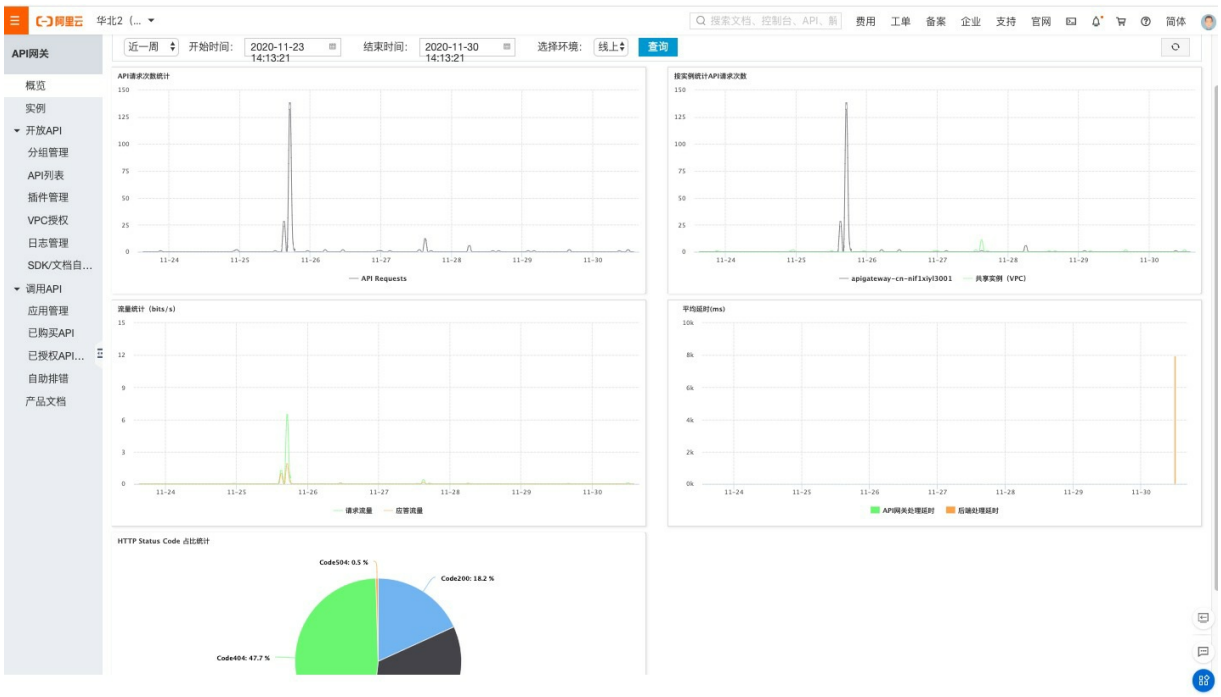
1. region监控

1.1 登录API网关控制台。

1.2 点击左侧栏的**概览**，可以看到各region的监控、API分组数量、API数量、使用中专享实例数以及10天内到期的专享实例数，点击监控图标进入即可查看相应region的监控图表。

1.3 region监控仅对最近7天内的API调用情况进行统计监控，**共享实例（经典网络）上运行的API不在统计范围内**。可根据API发布的不同环境（线上、预发、测试）查看监控图表。可监控指标包括：

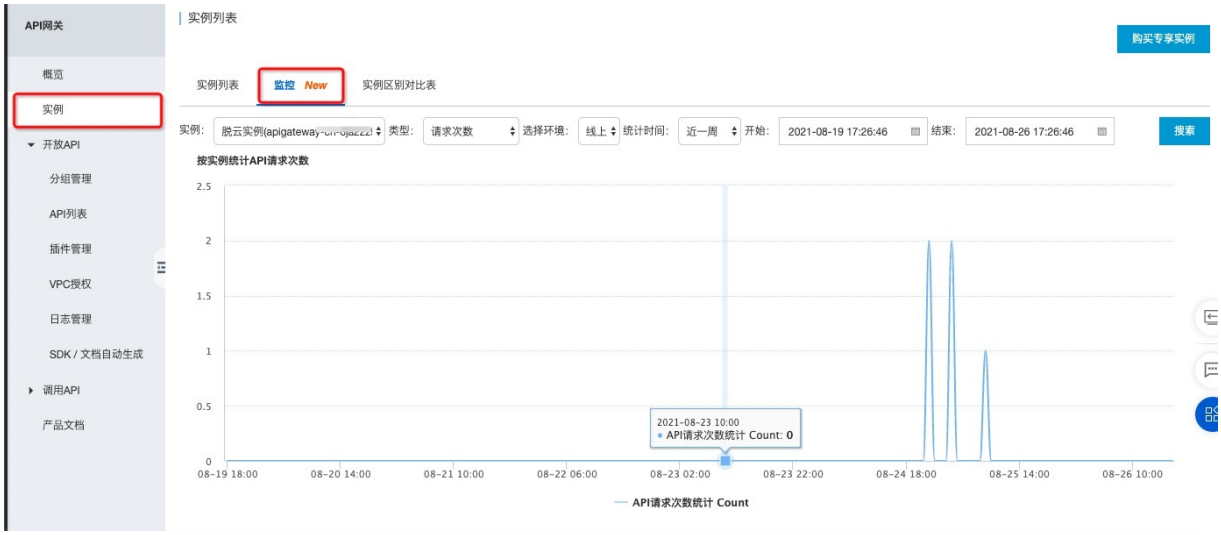
- **API请求次数统计**
- **按实例统计API请求次数**
- **流量统计**（请求流量、应答流量）
- **平均延时**（API网关处理延时、后端处理延时）
- **HTTP Status Code 占比统计**



2. 实例监控（仅专享实例）

2.1 登录API网关控制台。

2.2 点击左侧栏的实例，选择监控，即可进入实例监控页。



2.3 实例监控仅对最近7天内的API调用情况进行统计监控，可根据API发布的不同环境（线上、预发、测试）查看监控图表。可监控指标包括：

- **实例请求次数统计**
- **实例流量查询**（请求流量，应答流量）
- **平均延时**（API网关处理延时、后端处理延时）
- **HTTP Status Code 分布**
- **并发连接数**

- 活跃连接数：实例每秒活跃连接数。（有ESTABLISHED状态的连接。因为如果您采用的是长连接的情况，一个连接会同时传输多个文件请求。）
- 非活跃连接数：实例没秒非活跃连接数。（表示除ESTABLISHED状态的其它所有状态的连接数。）
- 最大并发连接数：所有建立的连接数量

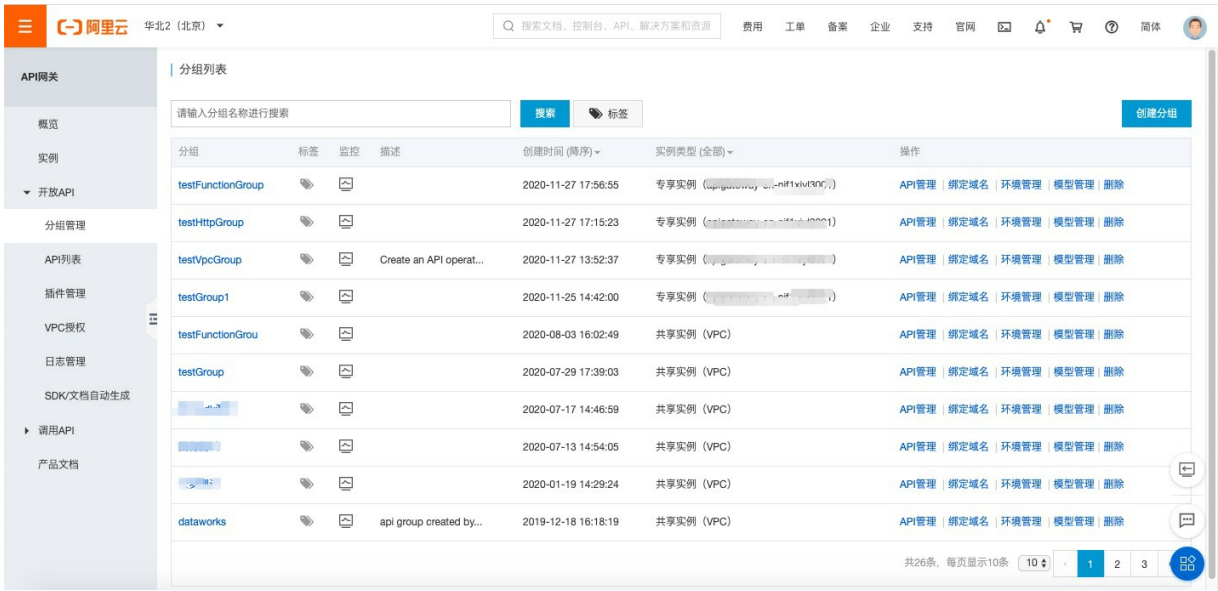
- **数据包数**
  - 流入数据包数：实例每秒接到的TCP数据包数量。
  - 流出数据包数：实例每秒发出的TCP数据包数量。
- **丢弃数据包数**
  - 丢弃流入数据包：每秒丢弃的流入TCP数据包的数量。
  - 丢弃流出数据包：每秒丢弃的流出TCP数据包的数量。
- **新建连接数**（实例每秒新建连接数CPS）
- **丢弃连接数**（每秒丢弃的连接数）

> 说明
>
> 并发连接数、数据包数、丢弃数据包数、新建连接数等指标数据仅统计公网数据。

3. 分组监控

3.1 登录API网关控制台。

3.2 左侧栏选择开放API——分组管理，在分组管理页点击监控图标进入即可查看相应分组的监控图表。



3.3 分组监控仅对最近7天内的API调用情况进行统计监控，**共享实例（经典网络）上运行的API不在统计范围内**。可根据API发布的不同环境（线上、预发、测试）查看监控图表。可监控指标包括：

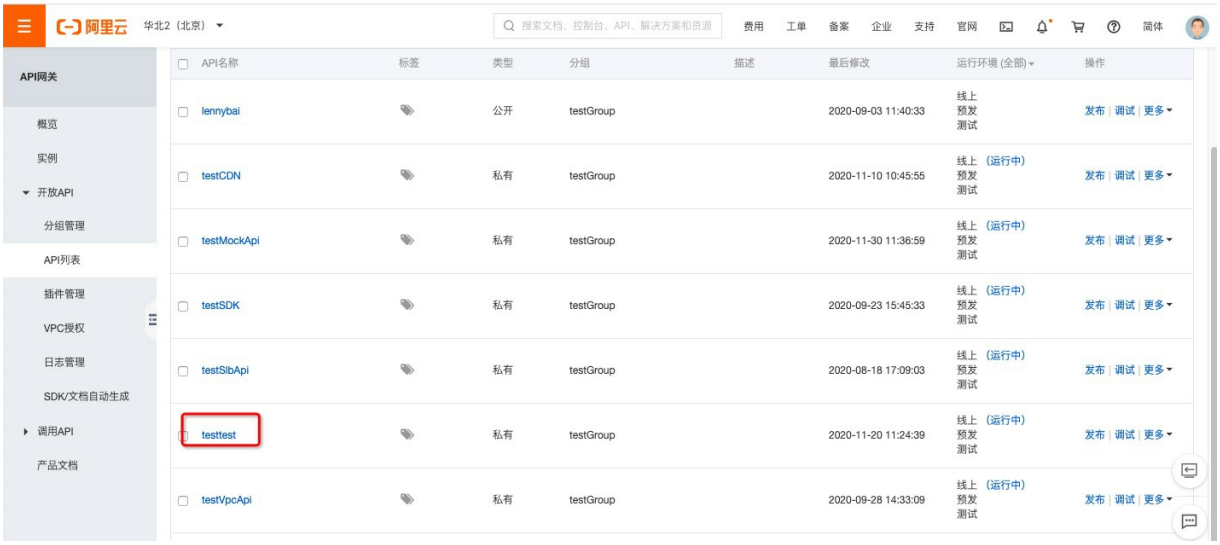
- **API请求次数统计**
- **流量统计**（请求流量、应答流量）
- **平均延时**（API网关处理延时、后端处理延时）

- **HTTP Status Code 占比统计**

4. API监控

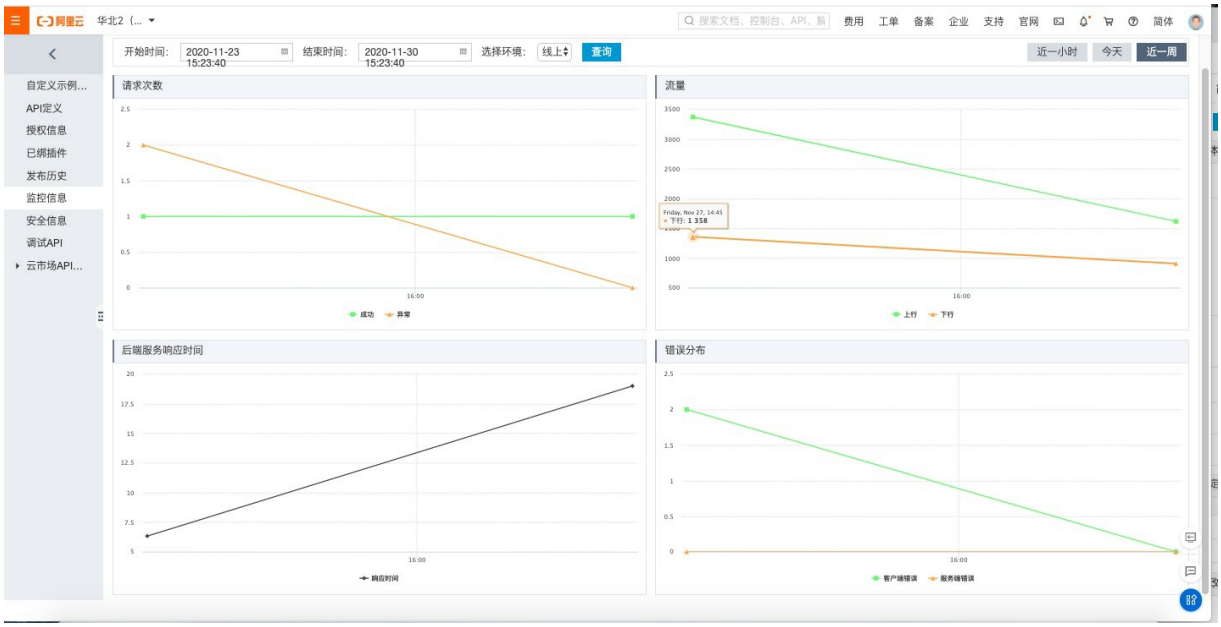
4.1 登录API网关控制台。

4.2 左侧栏选择**开放API——API列表**。点击想要查看监控的API，进入API详情页。



4.3 在左侧栏选择**监控信息**，可以根据环境（线上、测试、预发）查看该API近一周的监控数据。监控指标包括：

- **请求次数**（成功、异常）
- **流量**（上行、下行）
- **后端服务响应时间**
- **错误分布**（客户端错误、服务端错误）



说明

目前API网关监控仅支持对最近7天的调用情况进行统计监控，如您想要查看更长时间的统计，或是有其他需求，可以在日志服务中进行，具体可参考通过日志服务查看API调用日志。

2020年9月15日之后购买的专享实例可正常使用本功能， 2020年9月15日之前购买的专享实例请提交工单申请升级到新版本后可以使用。

2.配置Trace链路追踪

您可以参考本文在API网关控制台配置trace链路追踪日志上传到阿里云链路追踪平台，链路追踪 Tracing Analysis 提供了完整的调用链路还原、调用请求量统计、链路拓扑、应用依赖分析等工具，可以帮助用户提高开发诊断效率。**本功能仅支持专享实例。**

前提条件

- API网关为专享实例
- 开通链路追踪
- 开通日志服务

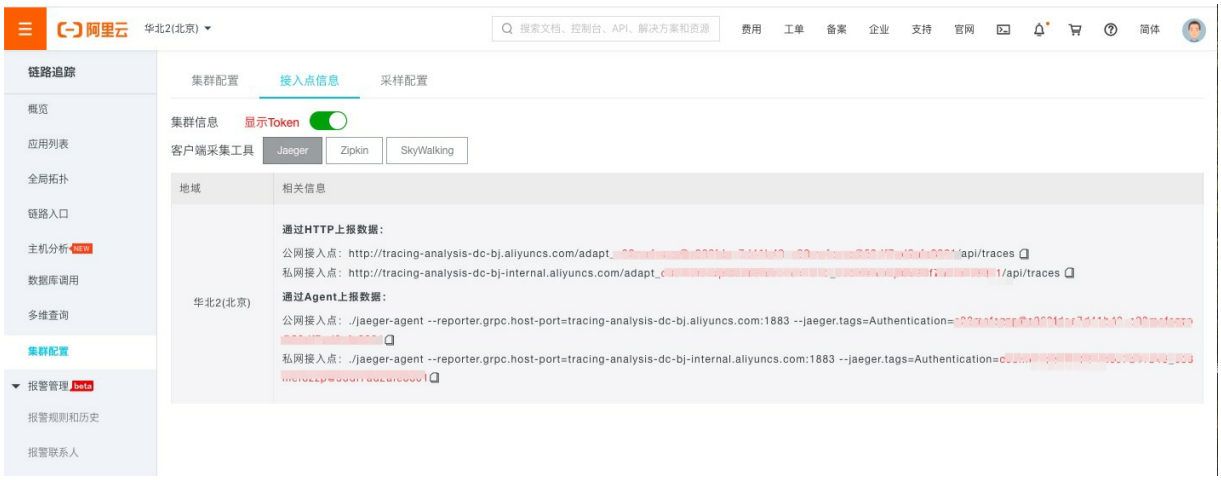
1 链路追踪授权

1.1 登录链路追踪控制台。

1.2 在概览页面上，单击立即授权，授权链路追踪读写您的日志服务。

1.3 在云资源访问授权页面上，选择所需的权限，并单击同意授权。

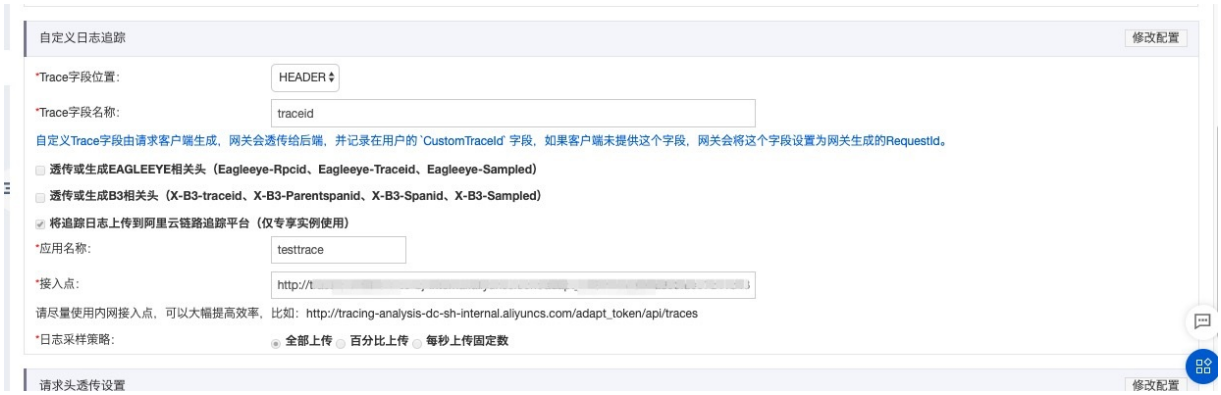
1.4 授权后可在**概览——接入流程——查看接入点信息——显示token**。即可查看到详细的接入点信息。保存**通过HTTP上传数据**中的接入点地址。



2 API网关配置Trace链路追踪

2.1 登录API网关控制台。

2.2 在左侧栏选择**开放API——分组管理**。点击进入分组详情。在分组详情页即可配置。



- Trace字段位置：指定Trace字段的位置，可选位置有Header、Query。

- Trace字段名称：自定义Trace字段的名称。自定义Trace字段由请求客户端生成，网关会透传给后端，并记录在用户的 `CustomTraceId` 字段，如果客户端未提供这个字段，网关会将这个字段设置为网关生成的RequestId。
- 透传或生成EAGLEEYE相关头（Eagleeye-Rpcid、Eagleeye-Traceid、Eagleeye-Sampled）：勾选配置后，若客户端传了EAGLEEYE相关头，网关会将相关头透传给后端服务，若没有传，网关将会生成相关头并传给后端服务。（共享实例和专享实例均可使用）
- 透传或生成B3相关头（X-B3-traceid、X-B3-Parentspanid、X-B3-Spanid、X-B3-Sampled）：勾选配置后，若客户端传了B3相关头，网关会将相关头透传给后端服务，若没有传，网关将会生成相关头并传给后端服务。（共享实例和专享实例均可使用）
- 将追踪日志上传到阿里云链路追踪平台（仅专享实例使用）：
  - 应用名称：自定义链路追踪的应用名称。
  - 接入点：填写1.4中的接入点地址，同region建议使用内网接入点，可以大幅提高效率。
  - 日志采样策略：支持全部上传、按百分比上传、每秒上传固定数，根据需要选择即可。

API网关配置Trace链路追踪后的请求可以在链路追踪控制台查看到请求链路。

关于链路追踪的使用可参考查看接口调用情况

> **说明**
>
> 2020年12月3日之后购买的专享实例可正常使用本功能， 2020年12月3日之前购买的专享实例请提交工单申请升级到新版本后可以使用。

3.使用 RAM 管理 API

API 网关结合阿里云访问控制（RAM）来实现企业内多职员分权管理 API。API 提供者可以为员工建立子账户，并控制不同职员负责不同的 API 管理。

- 使用 RAM 可以允许子账号，查看、创建、管理、删除 API 分组、API、插件等。但子账号不是资源的所有者，其操作权限随时都可以被主账号收回。
- 可以根据文档，利用标签鉴权实现主子账号的资源隔离。
- 在查看本文前，请确保您已经详读了RAM帮助手册和API 网关API 手册。
- **若您无此业务场景，请跳过此章节。**

第一部分：策略管理

授权策略（Policy），来描述授权的具体内容，授权内容主要包含效力(Effect)、资源(Resource)、对资源所授予的操作权限（Action）以及限制条件（Condition）这几个基本元素。

1. 系统授权策略

API 网关已经预置了两个系统权限，AliyunApiGatewayFullAccess和AliyunApiGatewayReadOnlyAccess，可以到 RAM 的在 RAM 控制台-策略管理 进行查看。

- AliyunApiGatewayFullAccess：管理员权限，拥有主账号下包含 API 分组、API、流控策略、应用等所有资源的管理权限。
- AliyunApiGatewayReadOnlyAccess：可以查看主账号下包含 API 分组、API、流控策略、应用等所有资源，但不可以操作。

2. 自定义授权策略

您可以根据需要自定义管理权限，支持更为精细化的授权，可以为某个操作，也可以是某个资源。如：API GetUsers 的编辑权限。可以在 RAM 控制台-策略管理-自定义授权策略查看已经定义好的自定义授权。

第二部分：授权策略

授权策略是一组权限的集合，它以一种策略语言来描述。通过给用户或群组附加授权策略，用户或群组中的所有用户就能获得授权策略中指定的访问权限。

示例：

```
{
  "Version": "1",
  "Statement": [
    {
  "Action": "apigateway:Describe*",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

此示例表示：允许所有的查看操作。

Action（操作名称列表）格式为：

```
 "Action":"<service-name>:<action-name>"
```

其中：

- **service-name** 为：阿里云产品名称，请填写 **apigateway**。
- **action-name** 为：API 接口名称，请参照下表，支持通配符*。

  "Action": "apigateway:Describe*" 表示所有的查询操作。

  "Action": "apigateway:*" 表示 API 网关所有操作。

第三部分：Resource（操作对象列表）

Resource 通常指操作对象， API 网关中的 API 分组、流控策略、应用都被称为 Resource，书写格式：

```
acs:<service-name>:<region>:<account-id>:<relative-id>
```

其中：

- **acs**：Alibaba Cloud Service 的首字母缩写，表示阿里云的公有云平台。
- **service-name** 为：阿里云产品名称，请填写 apigateway。
- **region**：地区信息，可以使用通配符*号来代替，*表示所有区域。
- **account-id**：账号 ID，比如1234567890123456，也可以用*代替。
- **relative-id**：与 API 网关相关的资源描述部分，这部分的格式描述支持类似于一个文件路径的树状结构。

示例：

```
acs:apigateway:$regionid:$accountid:apigroup/$groupId
```

书写：

```
acs:apigateway:*:*:apigroup/cbd157704e624ab58a204fd3e0b5ad79
```

请结合 API 网关的API 手册来查看下表：

action-name	接口描述	资源(Resource)
CreateApiGroup	创建分组	acs:apigateway:$regionid:$accountid:apigroup/*
ModifyApiGroup	修改分组	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DeleteApiGroup	删除分组	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeApiGroups	查询分组列表	acs:apigateway:$regionid:$accountid:apigroup/*
CreateApi	创建API	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DeployApi	发布API	acs:apigateway:$regionid:$accountid:apigroup/$groupId
AbolishApi	下线API	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DeleteApi	删除API	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeApis	查询API列表	acs:apigateway:$regionid:$accountid:apigroup/*
CreatePlugin	创建插件	acs:apigateway:$regionid:$accountid:plugin/*
ModifyPlugin	修改插件	acs:apigateway:$regionid:$accountid:plugin/$pluginId
DeletePlugin	删除插件	acs:apigateway:$regionid:$accountid:plugin/$pluginId
AttachPlugin	将插件绑定到API上	acs:apigateway:$regionid:$accountid:plugin/$pluginId

action-name	接口描述	资源(Resource)
DetachPlugin	将插件和API解绑	acs:apigateway:$regionid:$accountid:plugin/$pluginId
DescribePluginsByApi	查询API上绑定的插件列表	acs:apigateway:$regionid:$accountid:plugin/$pluginId
CreateApp	创建应用	acs:apigateway:$regionid:$accountid:app/*
ModifyApp	修改应用	acs:apigateway:$regionid:$accountid:app/$appId
DeleteApp	删除应用	acs:apigateway:$regionid:$accountid:app/$appId
DescribeAppAttributes	查询应用列表	acs:apigateway:$regionid:$accountid:app/$appId
SetApisAuthorities	给APP授权API访问权限	acs:apigateway:$regionid:$accountid:apigroup/$groupId
DescribeAuthorizedApps	查询API授权列表	acs:apigateway:$regionid:$accountid:apigroup/$groupId
SetVpcAccess	添加VPC授权	acs:apigateway:$regionid:$accountid:vpcaccess/*
RemoveVpcAccess	删除VPC授权	acs:apigateway:$regionid:$accountid:vpcaccess/*
DescribeVpcAccesses	查询VPC授权	acs:apigateway:$regionid:$accountid:vpcaccess/*
DescribeInstances	查询专享实例列表授权	acs:apigateway:$regionid:$accountid:instance/$instanceId

部分场景示例

授权所有API的查询操作：

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:Describe*",
                      "Resource":"acs:apigateway:$regionid:$accountid:apigroup/*",
                      "Effect": "Allow"
            }
          ]
}
```

授权打了标签 `version:v1` 的分组查询操作：

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:Describe*",
                      "Resource":"acs:apigateway:$regionid:$accountid:apigroup/*",
                      "Effect": "Allow",
                "Condition": {
                       "StringEquals": {
                            "apigateway:tag/version": "v1"
                       }
                }
             }
          ]
}
```

授权某个分组下所有API的管理操作：

```
{
          "Version": "1",
          "Statement": [
            {
                      "Action": "apigateway:*",
                      "Resource": [
                              "acs:apigateway:$regionid:$accountid:apigroup/$groupId",
                              "acs:apigateway:$regionid:$accountid:app/$appId",
                              "acs:apigateway:$regionid:$accountid:vpcaccess/*"
                      ],
                      "Effect": "Allow"
            }
          ]
}
```

备注：以上示例中，变量部分可以根据需要配置成*。

4.通过标签对资源进行管理

本文主要介绍通过标签(Tag)功能对API网关资源进行标记，利用资源上的Tag来批量描述资源，从而实现对特定类型的资源进行分组查询和管理。

每个标签(Tag)是由两个部分组成，Key和Value。同时，标记资源的时候需要指定资源类型，不同类型资源之间的标签是隔离的，不同region之间的标签也是隔离的。目前API网关支持对以下几种资源打标签：分组，API，插件，应用。这四种资源对应的参数ResourceType取值分别为：apiGroup，api，plugin，app。

1. 标签使用场景

1. 对大量资源进行分组管理，方便批量的查询和处理资源。
2. 结合阿里云的RAM系统的权限管理能力，提供主子账户的资源隔离的功能。本文3.1节将对此用法进行详细说明。

2. 使用Tag的限制：

- 一个资源上面已有的Tag不能超过20个
- 一个资源上Tag的Key不能相同，如果添加一个已有key的Tag，会使用该Tag新的Value覆盖旧的Value
- Key长度<=64 个 Unicode 字符，Value长度<=128 个 Unicode 字符
- Key和Value区分大小写
- 键（key）不支持以aliyun、acs: 开头； 不允许包含http:// 和 https:// ；不允许为空字符串
- 值（value）不允许包含http:// 和 https:// 。允许为空字符串

3. 权限控制

3.1 主子账户的资源隔离

简单介绍下RAM，阿里云账号本身是主账号，可以创建多个子账号，这些子账号可以被授权管理主账号的资源，授权操作参见相关文档：使用 RAM 管理 API。

主账号可以使用Tag对资源进行分类，对子账号授权时按照文档权限策略基本元素将资源的标签指定为授权语句的限制条件（Condition）部分，进而对所属资源进行子账号的隔离。例如，公司有多个部门，我们为每个部门创建一个管理员（子账号），然后授权每个子账号只能操作带有自己部门标签的资源。授权示例如下：

示例1：

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": "dep1"
        }
      }
    }
  ]
}
```

被授权的子用户，就只能操作带有depart:dep1标签的资源，即可管理部门1的所有资源。**在这个子账号查询资源列表的时候，必须带有Tag.1.Key=depart、Tag.1.Value=dep1的过滤条件鉴权才会通过，才允许查询。**

示例2:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": ["dep2", "dep3"]
        }
      }
    }
  ]
}
```

被授权的子用户，能操作带有depart:dep2或者depart:dep3 标签的资源，即可管理部门2和部门3的所有资源。

示例3:

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "apigateway:*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "apigateway:tag/depart": "dep2",
         "apigateway:tag/Enviroment": "test"
        }
      }
    }
  ]
}
```

被授权的子用户，只能操作同时被depart:dep2 和 Enviroment:test 标签标记的资源，即可管理部门2的测试环境资源。

分组，插件，应用三种资源支持子账号按照标签授权访问，API的授权完全从属于所属分组的授权规则，不支持通过API上已标记的标签进行授权。

3.2 标签相关操作的鉴权说明

对于使用标签(Tag)授权的资源，对不同类型的API有不同的限制表现，具体的限制如下：

创建类接口

对于创建类接口，鉴权时会判断接口中使用的所有资源是不是有权限，同时，也会通过标签参数判断是否有即将创建出来的资源的权限。因此，对于带有标签授权的子账号，创建API分组、应用、插件这类资源的时候，请求参数中也必须带有相关Tag参数，否则子用户没有权限创建。示例如下：

子账号被授予如下的权限时，则该子账号只能创建带有标签 `depart:dept1` 的分组。

```
{
    "Effect": "Allow",
    "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/*",
     "Condition": {
           "StringEquals": {
                "apigateway:tag/depart": "dep1"
            }
      }
}
```

操作类接口

对于操作类接口（如DeleteApp），是针对某一个资源的操作，子账号是否有权限完全依赖这个资源是否带有指定的标签。 如果应用上带有授权语句中所有规定的标签，则允许子账号操作。

查询类接口

对于查询类操作，由于所有的鉴权行为都是前置行为（即判断结果只区分是否通过，而不会判断一个集合中有哪些通过），所以不会对结果集合进行“有权限过滤”。使用了标签鉴权的子账号，必须在查询中带有指定有权限的标签进行查询，才能查到有权限的应用。当查询条件指定资源id 的情况下，账号是否有权限依赖这个资源是否带有指定的标签。

3.3 用户通过OpenAPI 访问资源的特殊说明

通过子账号AK根据标签条件查询资源列表时，需要配置启用标签鉴权，即设置参数 `EnableTagAuth` 为true。启用后才支持标签鉴权。这类接口列表如下：

- DescribeApiGroups
- DescribeAppAttributes

3.4 子账号访问控制台分组和API列表不展示的情况

部分用户过去使用类似下面语法的授权，老版控制台可以在列表查询中默认看到该分组。新版控制台将不再支持子账号资源列表查询对这种语法的支持。

```
{
     "Effect": "Allow",
     "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/f0b34d4c55504a34897f7390a24ce253"
}
```

子账号需要作出下面的调整才可以看到列表查询的结果。**除列表查询以外其他接口不受影响，也不需要调整任何授权配置。**

1. 在原来的授权语句基础上增加下面的授权子句，分组列表和API列表查询可以展示所有资源

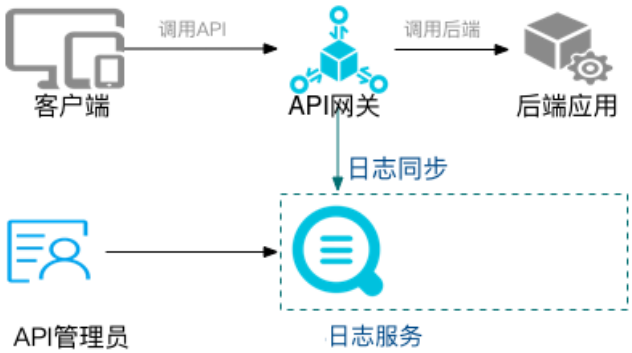
   ```
   {
        "Effect": "Allow",
        "Action": ["apigateway:DescribeApiGroups", "apigateway:DescribeApisForConsole"],
        "Resource": "acs:apigateway:*:*:apigroup/*"
   }
   ```

2. 通过主账号在控制台给对应的资源加标签 `depart:dep1` ，并在RAM控制台给需要授权的子账号对应的自定义权限权规则中增加下面的授权子句，则子账号在控制台可以通过设置标签条件查询资源列表

```
{
    "Effect": "Allow",
    "Action": "apigateway:*",
     "Resource": "acs:apigateway:*:*:apigroup/*",
     "Condition": {
           "StringEquals": {
                "apigateway:tag/depart": "dep1"
            }
      }
}
```

5.通过日志服务查看API调用日志

API网关和日志服务实现无缝集成，通过日志服务您可以进行实时日志查询、下载、多维度统计分析等，您也可以将日志投递到OSS或者MaxCompute。



- 日志服务每个月前500MB免费，具体价格请参照：日志服务定价。

1 功能简介

1.1 日志在线查询

可根据日志中任意关键字进行快速的精确、模糊检索，可用于问题定位或者统计查询。

1.2 详细调用日志

您可以检索API调用的详细日志包含如下表所示字段。其中：requestQueryString，requestHeaders, requestBody, responseHeaders, responseBody 几个字段只有VPC专享实例支持，且需要在分组详情页面配置后支持。

日志项	描述
apiGroupUid	API的分组ID
apiGroupName	API分组名称
apiUid	API的ID
apiName	API名称
apiStageUid	API环境ID
apiStageName	API环境名称
httpMethod	调用的HTTP方法

日志项	描述
path	请求的PATH
domain	调用的域名
statusCode	HttpStatusCode
errorMessage	错误信息
appId	调用者应用ID
appName	调用者应用名称
clientIp	调用者客户端IP
exception	后端返回的具体错信息
providerAliUid	API提供者帐户ID
region	区域，如：cn-hangzhou
requestHandleTime	请求时间，UTC
requestId	请求ID，全局唯一
requestSize	请求大小，单位：字节
responseSize	返回数据大小，单位：字节
serviceLatency	访问后端资源耗时总和，包括申请连接资源耗时，建立连接耗时，调用后端服务耗时，单位：毫秒
errorCode	错误码code，如：X500ER
requestProtocol	客户端请求协议：HTTP/HTTPS/WS

日志项	描述
instanceId	API服务所在的网关实例ID
initialRequestId	API网关自调用时，例如API-1调用API-2 ，那么API-2的日志中会用initialRequestId来记录API-1的requestid。
clientNonce	客户端X-Ca-Nonce头
requestQueryString	客户端请求的queryString
requestHeaders	客户端请求的header内容
requestBody	客户端请求的body内容，最多1024个字节
responseHeaders	API响应的header内容
responseBody	API响应的response内容，最多1024个
consumerAppKey	API请求的appKey
totalLatency	API请求的总延迟，单位毫秒
customTraceId	全链路日志的traceId
jwtClaims	从JWT中解析出来的Claim，可以在分组上配置
plugin	API请求命中的插件列表及相关上下文

2 使用日志服务查看API日志

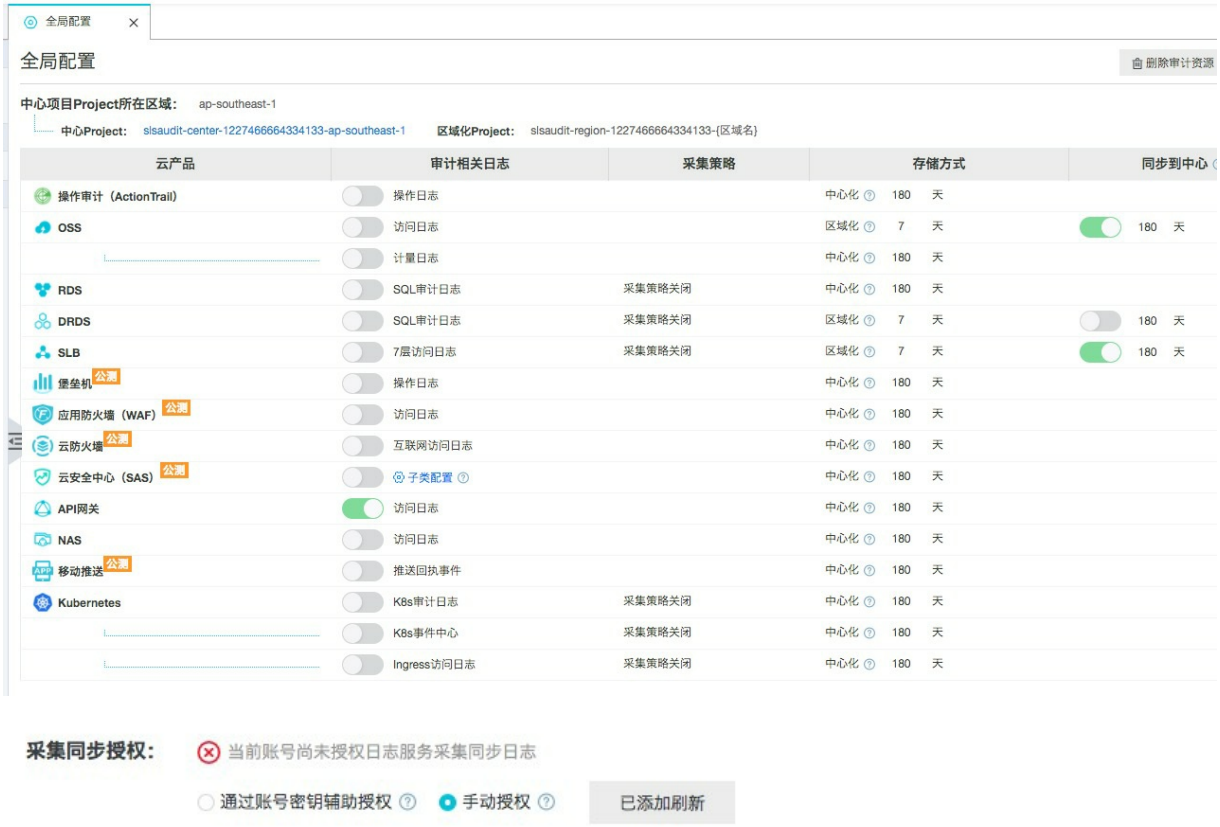
2.1 配置日志服务

目前有2种配置方式：1）通过日志服务页面的“日志审计”进行API网关日志同步。这种方式所有region的日志都会集中到日志审计这个project下。API网关上不需要做额外的配置。2）通过sls页面做API网关数据接入的方式配置，这种方式每个region都需要做一次同步配置。下面将分别介绍这两种配置方法。

政务云和金融云的SLS日志同步，目前仅支持用第1种方法配置。

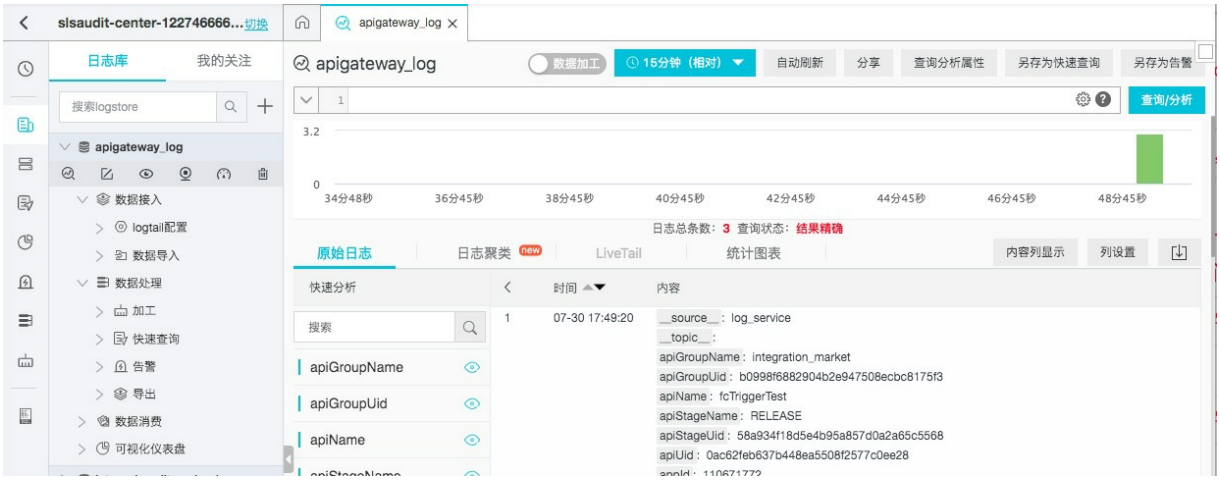
2.1.1 通过日志审计方式配置

1）打开sls日志审计服务配置页面，选择中心region，根据自己需要选择对应的region就行，后续所有的API网关日志都会投递到这个region。



然后选择以上2种方式之一做授权，根据文档提示操作。文示例选择“手动授权”。

授权完成后，根据本页面的中心project下的apigateway_log查看API网关的调用日志。



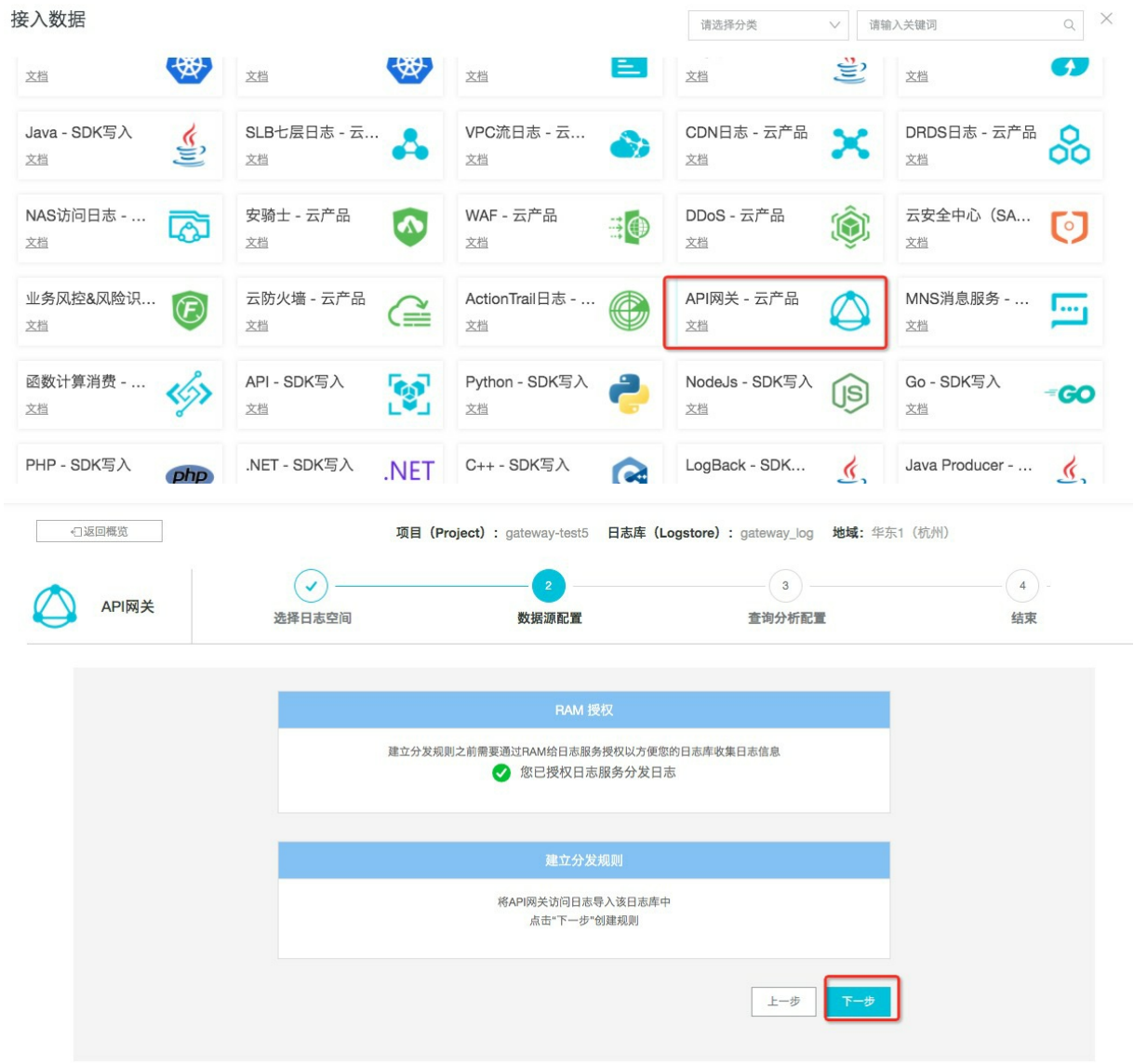
2.1.2 在API网关控制台配置

1）请确保您已经开通了日志服务，然后在SLS控制台选择对应的region，创建Project 和 Logstore。以华东1 region为例。


创建Project
* Project名称:
gateway-test5
注释:
不支持尖括号（<>）、撇号（'）、反斜线（\）、双引号（"）和两个反斜线（\\），最多包含64个字符
* 所属地域:
华东1（杭州）
开通服务日志:
详细日志（完整操作日志，按量收费）
重要日志（计量、消费组延迟和Logtail心跳日志等，免费）
开通服务日志会在您选择的存储位置创建对应的Logstore和仪表盘，存放操作日志的Logstore按照正常Logstore计费，存放其他日志的Logstore不产生费用。
查看帮助


创建成功
Project: gateway-test5
创建成功，是否立即创建logStore用于日志数据存储?
确认
取消

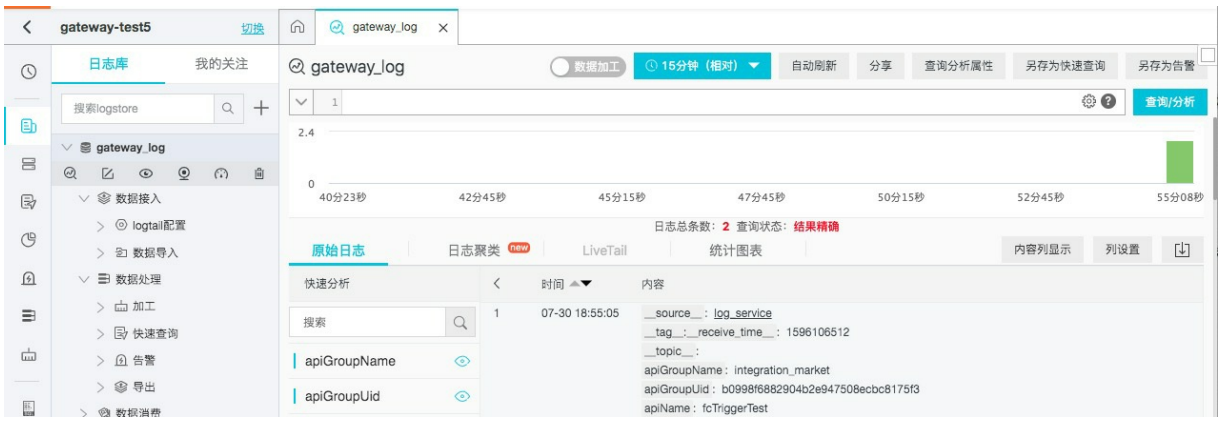
2）配置API网关数据接入，选择API网关产品



然后一直“下一步”，至成功为止。

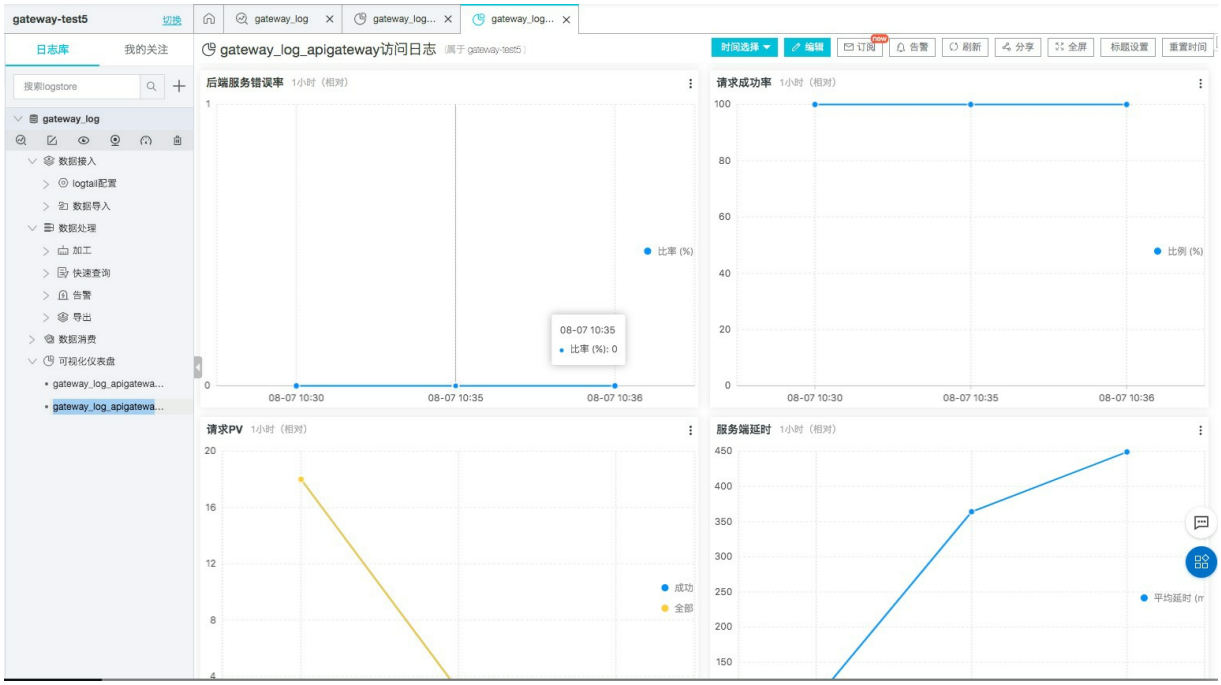
2.2 查看日志

您可以登录日志服务控制台查看日志，根据日志服务的查询语法，在线检索调用日志。



2.3 查看预定义报表

API网关为了方便用户统计查询，在系统中预置了一些报表统计。包括：请求量大小、成功率、错误率、延时情况、调用API的APP数量，错误情况统计、TOP 分组、TOP API、Top 延迟等等。您可以进入配置后的SLS的logstore，点开logstore详情->**可视化仪表盘** 查看预定义报表 **gateway_log_apigateway访问日志**。



2.4 自定义查询报表

您可以根据自身业务需要自定义查询报表，请参照定义方法：创建仪表盘。

6.配置记录HTTP请求应答日志

您可以参考本文来配置记录HTTP请求及应答日志，本功能仅支持专享实例。

如果需要在日志中记录API网关收到的HTTP的请求及API网关返回给客户端的HTTP应答，您可以在分组详情中进行设置。

- 记录请求Headers：逗号分隔需要记录的Header名称（如上图所示），'*'记录全部
- 记录应答Headers：逗号分隔需要记录的Header名称，'*'记录全部
- 记录请求QueryString：逗号分隔需要记录的字段名，'*'记录全部

设置成功后就可以在日志中看到这些信息，如图

打开用户日志设置后，将在根据设置在用户日志中额外记录以下字段：（requestBody,responseBody,requestHeaders,responseHeaders,queryString），日志字段的记录限制为4096Byte，超长的字段将截断后记录。

7.API报警设置

您可以通过云监控来对发布在API网关上的API配置报警，以便随时了解API服务运行情况，保障服务的稳定性。

1. 关联资源

API网关监控报警功能可以满足您多样化的业务需求，监控报警的指标包括：

- HttpStatusCode
- API响应时间
- API总体请求次数
- 流入流量
- 流出流量

创建报警规则关联资源时，有三种方式，如下：

- 手动关联同一Region下的一个API或者多个API。此方式适合对同Region下某一个或多个API设置相同的报警规则。API配置修改后，报警规则不受影响；
- 关联API分组，也就是对一个API分组下的所有API设置相同的报警规则，监控这些API的调用情况。API分组下若需要对API进行增删改操作，会自动同步报警规则，无需额外修改；
- 关联全部资源，指账号下的API网关产品中的所有API都作为关联资源，适用于需要管理的API很少的场景下。

> **说明**
>
> 除关联全部资源方式，其他方式创建报警规则时可以选择具体环境（RELEASE、PRE、TEST）来配置API的监控报警。

2. 报警级别和方式

云监控报警可设置多级报警，阈值处于不同区间时，对应Critical 、Warning、Info三个不同级别，不同级别通过不同渠道发送报警通知。报警通知等详细配置可以参考概览

- Critical：电话语音+手机短信+邮件+钉钉机器人(需付费使用)
- Warning：手机短信+邮件+钉钉机器人
- Info：邮件+钉钉机器人

> **说明**
>
> 阈值举例说明：如上图，含义是连续5分钟，其中每分钟的返回码2XX都超过200个，那么就会发送报警通知。

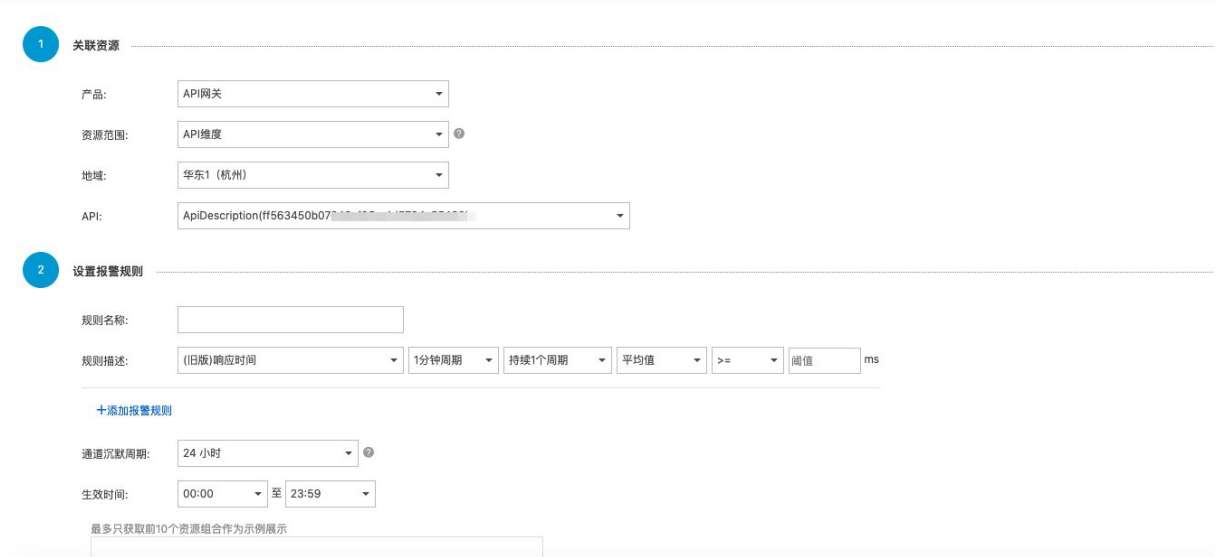
3. 设置一个或多个API的报警规则

配置过程中涉及的报警模板，报警规则，通知联系人，报警通知等详细配置可以参考概览

1、登录API网关控制台，选择地域，在API列表中找到想设置报警规则的API。

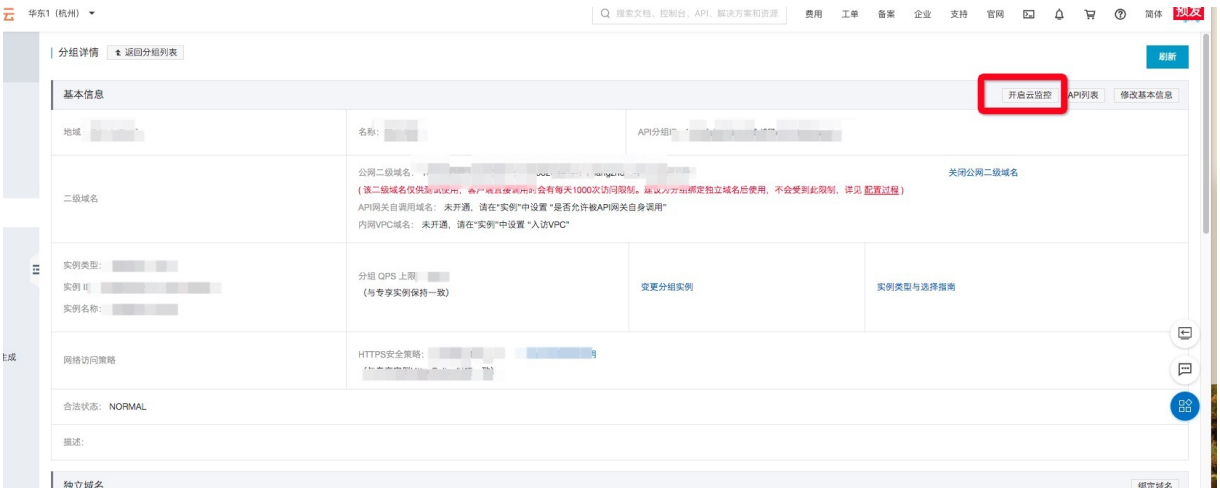
2、进入API管理页面，点击左侧菜单**监控信息**，之后点击页面右上角中的“报警设置”按钮，即进入到云监控配置控制台。

3、在云监控配置控制台创建报警规则，资源范围选择**API维度**，API处您可以选择您需要关联的一个API或者多个API。



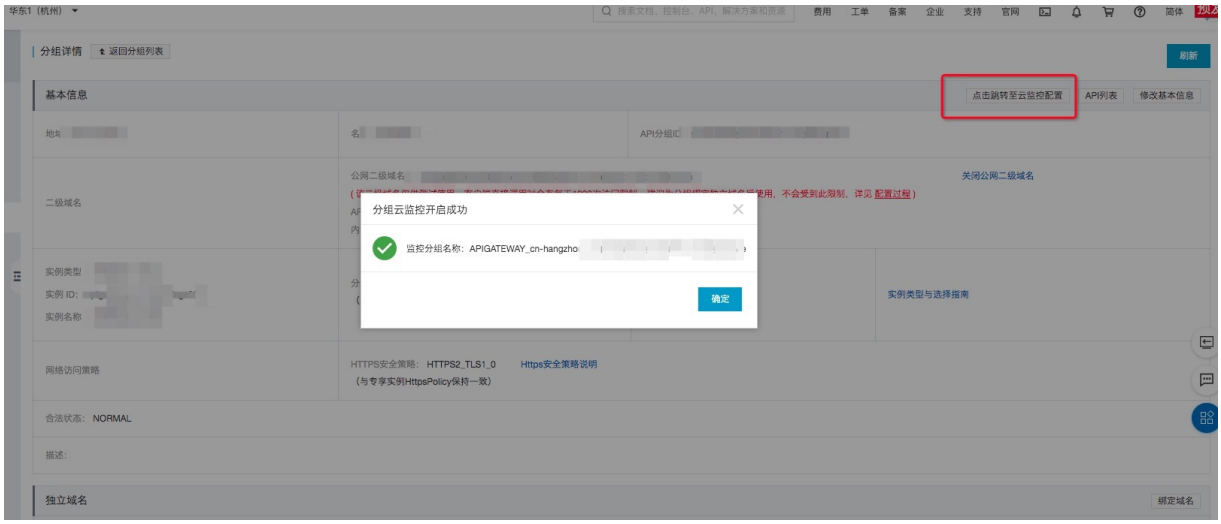
4.设置API分组的报警规则

1、如果需要对该API分组下的所有API应用相同的报警规则，进入API分组详情页，点击详情页右上角的 开启云监控



2、在第一次配置API分组云监控时，会有下面的弹出框提示用户创建API网关 - 监控服务关联角色。

3、点击确定后，提示云监控开启成功，提示信息中会附有云监控的应用分组名称。云监控的这个应用分组是由API网关经用户授权后创建的，和当前的API分组对应，命名格式固定为：`APIGATEWAY_${region}_${groupId}`，region的值是API分组所在的region，groupId是API分组的分组ID。



4、成功开通云监控后，通过API分组详情页右上角的按钮 **点击跳转至云监控配置** ，即可直接配置应用到当前应用分组的报警规则。

5. 设置全部资源的报警规则

步骤与第3章相同，资源范围选择“全部资源”即可。设置完成后账号下API网关上的所有Region所有API都将使用同一报警规则，不能选择API，适用于需要管理的API很少的场景。

6. API网关支持的报警规则

API网关提供了HttpStatusCode，API响应时间，API总体请求次数，流入流量，流出流量 五个指标的规则；您可以就这几个方面，配置您的报警。

- API响应时间：API网关的后端响应时间。
- API总体请求次数：某一周期内API网关收到客户端的请求总次数。
- 流入流量：某一周期内API网关收到的客户端请求产生的流量。
- 流出流量：某一周期内API网关向后端服务发出请求产生的流量。
- HttpStatusCode：API网关返回状态码，有Code2XX，Code4XX，Code5XX可选。

-Code2XX：表示API请求成功。（注意：此处并非一定是业务成功）

-Code4XX：表示客户端错误，可能是参数错误等。

-Code5XX：表示服务端错误，这个对于API开放者来说，一般需要重点监控。

6. 注意事项

- 建议API分组在经典网络的用户使用标有 `旧版` 的报警规则，API分组在VPC网络的用户使用没有标记 `旧版` 的报警规则。
- 可以根据API发布环境进行报警，如果VPC网络的用户根据环境配置报警无效，建议先打开API网关控制台，进入API详情页，在监控页面查看该API是否支持根据环境查询监控数据，如果不支持，请工单联系我们，我们将升级您的API网关版本。

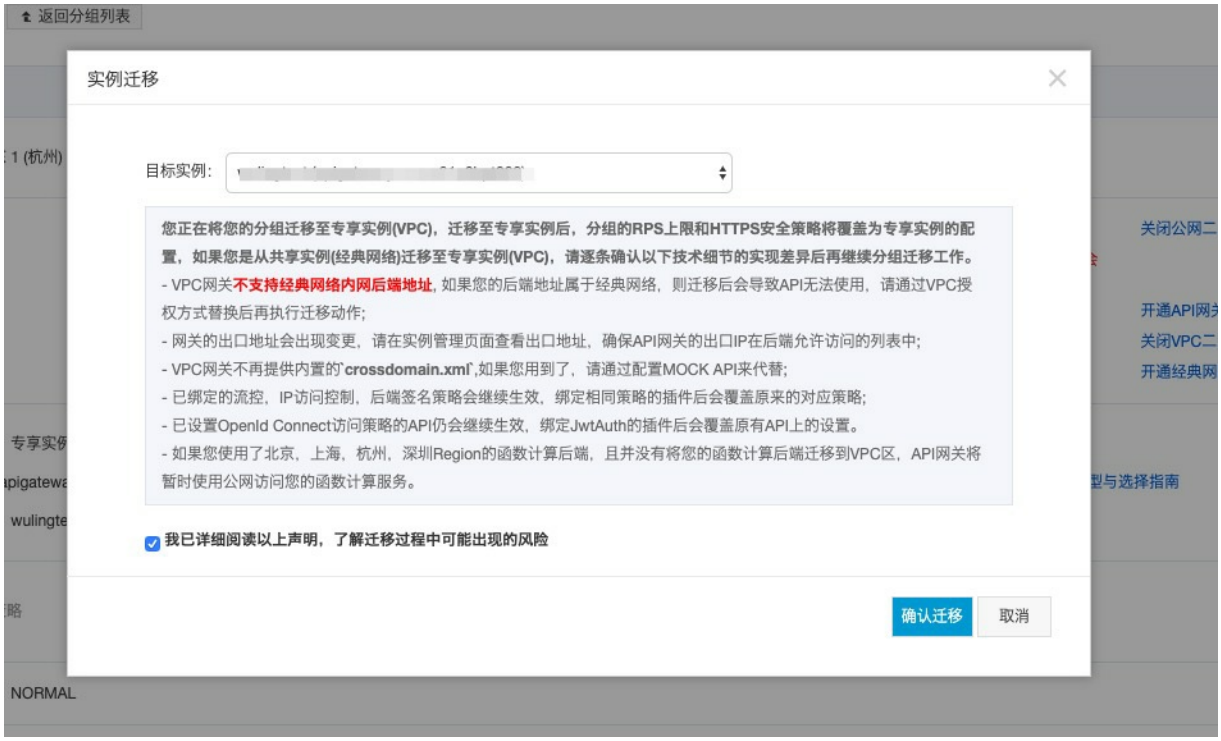
8.API分组的归属实例迁移

1 不同实例的适用场景

- 共享实例（经典网络）：API网关早期实例类型，功能有限制，目前共享实例（经典网络）已停止维护，所有新功能都无法使用，建议用户尽快迁移至共享实例（VPC）或专享实例（VPC）。
- 共享实例（VPC）：多租户共享出口IP与带宽，易受其他租户影响，更适合开发测试、评估和小规模的生产环境使用。
- 专享实例（VPC）：用户可以通过支付规格配置费用自助购买更高的RPS，获取独享的资源，包含公网入口IP地址、仅允许自己VPC访问的内网IP地址、公网出口带宽、独立隔离的服务器集群等，提供更高等级的SLA保障。

2 迁移步骤

您可以在控制台的 `分组` -> `分组详情页` 中找到变更分组实例链接，点击变更分组实例，选择 `目标实例` ，**务必仔细阅读注意事项**，之后点击 `确认迁移` 完成分组迁移，分组迁移会实时生效在API网关二级域名的DNS上，根据DNS的缓存，大约1~10分钟内完整生效至您的分组。



> **说明**
>
> 若您是专享实例，当目前的配置无法满足您的业务需求时，您需要将实例内分组迁移至更高的专享实例规格，操作步骤：
>
> 1. 先购买所需规格的专享实例。
> 2. 按照上面的操作步骤将分组迁移至新的实例。
>
> **注意：由于DNS的缓存原因，迁移后将有一部分请求依旧会访问老实例，请确认请求已全部指向新实例后再释放旧实例。**

3 迁移注意事项

如果您的分组调整过RPS，又希望进行迁移的，请通过工单联系工作人员代为处理。同时，务必逐条确认以下技术细节的实现差异后再继续分组迁移工作。

3.1 共享实例（经典网络）迁移至共享实例(VPC)

- VPC网关 **不支持经典网络内网后端地址** ；
- 网关的出口地址会出现变更，请在实例管理页面查看出口地址，确保API网关的出口IP在后端允许访问的列表中;
- VPC网关不再提供内置的`crossdomain.xml`,如果您用到了，请通过配置MOCK API来代替;
- 已绑定的流控，IP访问控制，后端签名策略会继续生效，绑定相同策略的插件后会覆盖原来的对应策略;
- 已设置OpenId Connect访问策略的API仍会继续生效，绑定JwtAuth的插件后会覆盖原有API上的设置。

3.2 共享实例（经典网络）迁移至专享实例（VPC）

- 迁移至专享实例后，分组的RPS上限和HTTPS安全策略将覆盖为专享实例的配置。

- VPC网关不支持**经典网络内网后端地址**,如果您的后端地址属于经典网络，则迁移后会导致API无法使用，请通过VPC授权方式替换后再执行迁移动作;
- 网关的出口地址会出现变更，请在实例管理页面查看出口地址，确保API网关的出口IP在后端允许访问的列表中;
- VPC网关不再提供内置的`crossdomain.xml`,如果您用到了，请通过配置MOCK API来代替;
- 已绑定的流控，IP访问控制，后端签名策略会继续生效，绑定相同策略的插件后会覆盖原来的对应策略;
- 已设置OpenId Connect访问策略的API仍会继续生效，绑定JwtAuth的插件后会覆盖原有API上的设置。
- 如果您使用了北京，上海，杭州，深圳Region的函数计算后端，且并没有将您的函数计算后端迁移到VPC区，API网关将暂时使用公网访问您的函数计算服务。
- 若分组已开通内网VPC域名，请确保目标实例已开通入访VPC后再执行迁移动作。

3.3 共享实例（VPC）至共享实例（经典网络）

- VPC实例支持后端TLS1.2，经典网络实例仅支持TLS1.0;
- 所有的插件配置均会失效，经典网络实例的流控，IP访问控制，后端签名需要在对应的策略中重新配置;
- 网关的出口地址可能出现变更，请在实例管理页面查看出口地址，确保API网关在允许访问的白名单中;
- 一些新的Feature可能不被支持，请关注控制台上的提示。

3.4 共享实例（VPC）迁移至专享实例（VPC）

- 迁移至专享实例后，分组的RPS上限和HTTPS安全策略将覆盖为专享实例的配置。
- 网关的出口地址可能出现变更，请在实例管理页面查看出口地址，确保API网关在允许访问的白名单中。
- 若分组已开通内网VPC域名、自调用域名、IPv6入访或IPv6出访能力，请确保目标实例已开通相关能力后再执行迁移动作。

3.5 专享实例（VPC）迁移至专享实例(VPC)

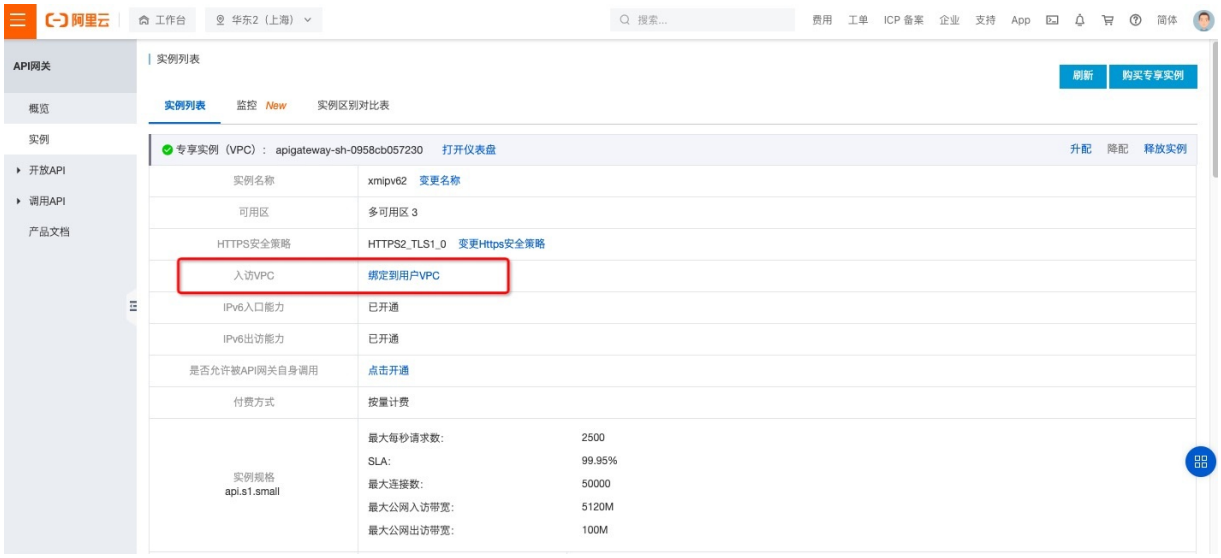
- 迁移至专享实例后，分组的RPS上限和HTTPS安全策略将覆盖为专享实例的配置。
- 网关的出口地址可能出现变更，请在实例管理页面查看出口地址，确保API网关在允许访问的白名单中。
- 若分组已开通内网VPC域名、自调用域名、IPv6入访或IPv6出访能力，请确保目标实例已开通相关能力后再执行迁移动作。

4 常见问题

4.1 迁移分组出现报
You have not opened the intranet access for the instance.

问题原因：源分组开通了内网vpc域名，而目标专享实例未开通。

处理建议：找到目标专享实例，配置入访vpc。可参考文档VPC内网访问API网关。


阿里云
工作台
华东2（上海）
搜索...
费用
工单
ICP 备案
企业
支持
App
简体
API网关
概览
实例
开放API
调用API
产品文档
实例列表
刷新
购买专享实例
实例列表
监控 New
实例区别对比表
专享实例（VPC）： apigateway-sh-0958cb057230
打开仪表盘
升配
降配
释放实例
实例名称
xmipv62 变更名称
可用区
多可用区 3
HTTPS安全策略
HTTPS2_TLS1_0 变更Https安全策略
入访VPC
绑定到用户VPC
IPv6入口能力
已开通
IPv6出访能力
已开通
是否允许被API网关自身调用
点击开通
付费方式
按量计费
实例规格
api.s1.small
最大每秒请求数: 2500
SLA: 99.95%
最大连接数: 50000
最大公网入访带宽: 5120M
最大公网出访带宽: 100M