ALIBABA CLOUD

阿里云

API 网关

历史功能

文档版本：20200826

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.流量控制策略 ---------- 05
2.后端签名说明文档 ---------- 06

1.流量控制策略

流量控制策略和 API 分别是独立管理的，操作两者绑定后，流控策略才会对已绑定的 API 起作用。

在已有的流量控制策略上，可以额外配置特殊用户和特殊应用（APP），这些特例也是针对当前策略已绑定的API生效。

流量控制策略可以配置对 API、用户、应用三个对象的流控值，流控的单位可以是秒、分钟、小时、天。使用流量控制策略您需要了解以下几点：

- 流量控制策略可以涵盖下表中的维度：

API 流量限制	该策略绑定的API在单位时间内被调用的次数不能超过设定值，单位时间可选秒、分钟、小时、天，如5000次/分钟。
APP 流量限制	每个APP对该策略绑定的任何一个API在单位时间内的调用次数不能超过设定值。如50000次/小时。
用户流量限制	每个阿里云账号对该策略绑定的任何一个 API 在单位时间内的调用次数不能超过设定值。一个阿里云账号可能有多个 APP，所以对阿里云账号的流量限制就是对该账号下所有 APP 的流量总和的限制。如 50 万次/天。

  在一个流控策略里面，这三个值可以同时设置。请注意，用户流量限制应不大于 API 流量限制，APP 流量限制应不大于用户流量限制。即 APP 流量限制 <= 用户流量限制 <= API 流量限制。

  此外，您可以在流控策略下添加特殊应用（APP）和特殊用户。对于特例，流控策略基础的 **API 流量限制** 依然有效，您需要额外设定一个阈值作为该 APP 或者该用户的流量限制值，该值不能超过策略的 **API流量限制** 值，同时流控策略基础的 **APP流量限制** 和 **用户流量限制** 对该 APP 或用户失效。

- 与签名密钥相似，当您创建流量控制策略时，需要选择 Region，Region 一旦选定不可更改，且仅能被应用于同一个 Region 下的 API。
- 由于 API 网关限制，当您设置 **API 流量限制** 值时，考虑每个 API 分组的默认流控上限是500QPS（该值可以通过提交工单申请提高）。
- 绑定 API。您可以将策略绑定于多个 API，流控策略的限制值和特例将对该策略绑定的每一个 API 单独生效。当您绑定 API 时，如果该 API 已经与某个策略绑定，您的此次操作将替换之前的策略，实时生效。
- 特殊对象。如果您想要添加特殊应用或者特殊用户，您需要获得应用 ID 即 AppID 或者用户的阿里云邮箱账号。
- 在 API 网关控制台，您可以完成对流量控制策略的创建、修改、删除、查看等基本操作。还有流控策略与 API 的绑定解绑，流量控制策略特殊对象的添加删除等操作。

2.后端签名说明文档

后端签名密钥是由您创建的一对 Key 和 Secret，相当于您给网关颁发了一个账号密码。开启后端签名后，API 网关向您后端服务请求时会使用这一对Key和Secret对请求内容进行加签处理，您后端服务可以对网关发送过来的请求做对称加签计算，对比网关的签名和服务器端计算的签名是否一致就可以对网关做身份验证。

概述

- 创建签名密钥并将签名密钥绑定到 API 即可开启后端签名（请妥善保管此密钥，API 网关会对密钥进行加密存储来保障密钥的安全性）。
- 创建密钥时需要选择 Region，Region 一旦选定不能更改，而且密钥只能被绑定到同一个 Region 下的API上。
- 一个 API 仅能绑定一个密钥，密钥可以被替换和修改。
- 所有您定义的参数都会参与签名，包括您录入的业务参数、您定义的常量系统参数和 API 网关系统参数（如 CaClientIp 等）。
- 后端对 API 网关的签名字符串校验后，如果校验失败，建议返回 errorcode = 403；errormessage = “InvalidSignature”。
- 若您的后端服务为VPC环境，且通过内网对接（专属网络VPC环境开放API），您无需使用后端签名，通道自身是安全的。

读取 API 网关签名方法

网关计算的签名保存在 Request 的 Header 中，Header 名称：X-Ca-Proxy-Signature。

后端 HTTP 服务加签方法

签名计算的详细 demo（JAVA）请参照链接：https://github.com/aliyun/api-gateway-demo-sign-backend-java。

签名计算方法步骤如下：

1. 组织参与加签的数据：

```
String stringToSign=
HTTPMethod + "\n" + //Method全大写
Content-MD5 + "\n" + //Content-MD5 需要判断是否为空，如果为空则跳过，但是为空也需要添加换行符 "\n"
Headers + //Headers 如果为空不需要添加"\n"，不为空的Headers中包含了"\n"，详见下面组织Headers的描述
Url
```

2. 计算签名：

```
Mac hmacSha256 = Mac.getInstance("HmacSHA256");
byte[] keyBytes = secret.getBytes("UTF-8"); //secret 为绑定到 API 上的签名密钥
hmacSha256.init(new SecretKeySpec(keyBytes, 0, keyBytes.length, "HmacSHA256"));
String sign = new String(Base64.encodeBase64(Sha256.doFinal(stringToSign.getBytes("UTF-8")),"UTF-8"));
```

补充说明

- **Content-MD5**

  Content-MD5 是指 Body 的 MD5 值，只有 HttpMethod 为 PUT 或者 POST 且 Body 为非 Form 表单时才计算 MD5，计算方式为：

```
String content-MD5 = Base64.encodeBase64(MD5(bodyStream.getbytes("UTF-8")));
```

- **Headers**

  Headers 指所有参与签名计算的 Header的Key、Value。参与签名计算的 Header 的 Key 从 Request Header 中读取，Key为："X-Ca-Proxy-Signature-Headers"，多个 Key 用英文逗号分割。

- **Headers 组织方法：**

  先对所有参与签名计算的 Header 的 Key 按照字典排序，然后将 Header 的 Key 转换成小写后按照如下方式拼接：

```
String headers = HeaderKey1.toLowerCase() + ":" + HeaderValue1 +"\n"+
HeaderKey2.toLowerCase() + ":" + HeaderValue2 +"\n"+
... +
HeaderKeyN.toLowerCase() + ":" + HeaderValueN + "\n"
```

- **Url**

  Url指 Path+Query+Body 中 Form 参数，组织方法： 如果有 Query 或 Form 参数则加 ?，然后对 Query+Form 参数按照字典对 Key 进行排序后按照如下方法拼接，如果没有 Query 或 Form 参数，则 Url = Path。

```
String url =
Path +
"?" +
Key1 + "=" + Value1
+ "&" + Key2 + "=" + Value2 +
...
"&" + KeyN + "=" + ValueN
```

  > 说明 1. 这里 Query 或 Form 参数的 Value 可能有多个，多个的时候只取第一个 Value 参与签名计算；2. 只要传递了的参数，签名过程中的等号 “=” 无论什么情况都需要保留，比如这两个query参数传递时的形式："path?a=&b"，签名时需要写成："path?a=&b="。

- **调试模式**

  为了方便后端签名接入与调试，可以开启 Debug 模式进行调试，具体方法如下：

  i. 请求API网关的 Header 中添加 X-Ca-Request-Mode = debug。

  ii. 后端服务在 Header 中读取 X-Ca-Proxy-Signature-String-To-Sign 即可，因为 HTTP Header 中值不允许有换行符，因此换行符被替换成了 "|"。

注意：X-Ca-Proxy-Signature-String-To-Sign 不参与后端签名计算。

- **时间戳校验**

  如果后端需要对请求进行时间戳校验，可以在 API 定义中选择系统参数 "CaRequestHandleTime"，值为网关收到请求的格林威治时间。

密钥泄露 修改替换

当您遇到如下情况：

- 您的某一个密钥发生了泄露，您可能想要保留该密钥与 API 的绑定关系，但是想要修改密钥的 Key 和 Secret。
- 当您操作将密钥应用于 API 时，可能该 API 已经绑定了某个密钥，需要替换密钥。

以上两种情况都建议按照下面的流程来操作：

1. 先在后端同时支持两个密钥：原来的密钥和即将修改或替换的密钥，确保切换过程中的请求能够通过签名验证，不受修改或替换的影响。
2. 后端配置完备后，完成修改，确定新 Key 和 Secret 生效后再将之前已泄露或废弃的密钥删除。