业务风险情报

API 文档

产品文档

腾讯云

文档目录

API 文档
更新历史

最近更新时间：2019-06-21 19:56:02

第 1 次发布

发布时间：2019-06-21 19:18:04

本次发布包含了以下内容：

改善已有的文档。

新增接口：

- DescribeBRI

新增数据结构：

- BRIRequest
- BRIResponse

简介

最近更新时间：2019-06-21 19:56:02

业务风险情报 API 升级到 3.0 版本。全新的 API 接口文档更加规范和全面，统一的参数风格和公共错误码，统一的 SDK/CLI 版本与 API 文档严格一致，给您带来简单快捷的使用体验。支持全地域就近接入让您更快连接腾讯云产品。

产品概述

什么是业务风险情报？

业务风险情报（Business Risk Intelligence，BRI）为您提供全面、实时、精准的业务风险情报服务。通过简单的 API 接入，您即可获取业务中 IP、号码、设备、APP、URL 等的画像数据，对其风险进行精确评估，做到对业务风险、黑产攻击实时感知、评估、应对、止损。 您也可利用业务风险情报服务搭建或完善自身的风控体系，补充自身风险情报数据，提升对风险的感知、应对能力。 BRI 支持按需付费，您可根据您的需求，选取不同的套餐，更易优化成本。

产品功能

BRI拥有多个风险情报查询接口，可帮助您判断业务中 IP、号码、设备、APP、URL 等风险等级，提升对风险的感知、应对能力。

- 号码标签

  客户通过相关接口查询号码风险等级，BRI会反馈号码相关风险值(0-100)，分值越大代表相关号码潜在欺诈风险越高，同时，BRI还会反馈高风险号码标签，说明号码欺诈属性，辅助客户更好地进行风险判断；客户可根据风险值结合自身风控系统对相关号码的业务请求做出风险判别，及时感知风险并做出应对。

- 设备标签

  客户通过相关接口查询设备风险等级，BRI会反馈设备相关风险值(0-100)，分值越大代表相关设备潜在欺诈风险越高，同时，BRI还会反馈高风险设备标签，说明设备欺诈属性，辅助客户更好地进行风险判断。

- IP标签

  客户通过相关接口查询IP风险等级，BRI会反馈IP相关风险值(0-100)，分值越大代表相关设备潜在欺诈风险越高。

- APP标签

  客户通过相关接口查询APP风险等级，BRI会反馈APP相关风险值(0-100)，分值越大代表相关设备潜在欺诈风险越高，同时，BRI还会反馈高风险APP标签，说明APP判定详情，辅助客户更好地进行风险判断。

- URL标签

  客户通过相关接口查询URL风险等级，BRI会反馈URL相关风险值(0-100)，分值越大代表相关URL潜在欺诈风险越高。

产品优势

BRI产品优势如下：

- 海量数据

  基于海量的腾讯安全大数据，及丰富的黑产对抗经验，持续、实时对 IP、号码、URL、APK 等进行风险检测与标识，建立高实时性的精准画像，以此构建全面、准确的安全情报，覆盖率高达9%+。

- 精准画像

  结合多维度的安全数据（如应用行为、黑产活动、页面内容等），对 IP、号码、APK 及 URL 等进行精准画像，构建丰富的风险标签，便于客户针对不同的类别制定精细化的防控策略。

- 灵活接入

  根据客户自身业务情况，提供线上 API 调用、本地化部署两种交付形式，客户可灵活选择接入方式，保障客户拥有快速、0负担的接入体验。

应用场景

实时风险感知

场景描述：在企业没有自身风控系统的情况下，运维人员利用腾讯业务风险情报对业务进行安全监控，实时感知业务风险。 使用效果：实时、精准感知业务风险，精确打击黑产，及时应对、解决安全问题。

风控体系情报补充

场景描述：针对拥有自身风控体系的企业，安全团队可接入腾讯业务风险情报，补充情报数据来源，更好掌握业务安全。 使用效果：海量、实时、精准的业务风险情报数据，对已有风控体系进行有效数据补充，加强风控能力。

API 概览

最近更新时间：2019-06-21 19:56:02

风险查询相关接口

接口名称	接口功能
DescribeBRI	获取业务风险情报

调用方式
请求结构

最近更新时间：2019-08-14 19:16:48

1. 服务地址

API 支持就近地域接入，本产品就近地域接入域名为 bri.tencentcloudapi.com ，也支持指定地域域名访问，例如广州地域的域名为 bri.ap-guangzhou.tencentcloudapi.com 。

推荐使用就近地域接入域名。根据调用接口时客户端所在位置，会自动解析到**最近的**某个具体地域的服务器。例如在广州发起请求，会自动解析到广州的服务器，效果和指定 bri.ap-guangzhou.tencentcloudapi.com 是一致的。

注意：对时延敏感的业务，建议指定带地域的域名。

目前支持的域名列表为：

接入地域	域名
就近地域接入（推荐，只支持非金融区）	bri.tencentcloudapi.com
华南地区(广州)	bri.ap-guangzhou.tencentcloudapi.com
华东地区(上海)	bri.ap-shanghai.tencentcloudapi.com
华北地区(北京)	bri.ap-beijing.tencentcloudapi.com
西南地区(成都)	bri.ap-chengdu.tencentcloudapi.com
西南地区(重庆)	bri.ap-chongqing.tencentcloudapi.com
港澳台地区(中国香港)	bri.ap-hongkong.tencentcloudapi.com
亚太东南(新加坡)	bri.ap-singapore.tencentcloudapi.com
亚太东南(曼谷)	bri.ap-bangkok.tencentcloudapi.com
亚太南部(孟买)	bri.ap-mumbai.tencentcloudapi.com
亚太东北(首尔)	bri.ap-seoul.tencentcloudapi.com
亚太东北(东京)	bri.ap-tokyo.tencentcloudapi.com
美国东部(弗吉尼亚)	bri.na-ashburn.tencentcloudapi.com
美国西部(硅谷)	bri.na-siliconvalley.tencentcloudapi.com
北美地区(多伦多)	bri.na-toronto.tencentcloudapi.com
欧洲地区(法兰克福)	bri.eu-frankfurt.tencentcloudapi.com
欧洲地区(莫斯科)	bri.eu-moscow.tencentcloudapi.com

注意：由于金融区和非金融区是隔离不互通的，因此当访问金融区服务时（公共参数 Region 为金融区地域），需要同时指定带金融区地域的域名，最好和 Region 的地域保持一致。

金融区接入地域	金融区域名
华东地区(上海金融)	bri.ap-shanghai-fsi.tencentcloudapi.com
华南地区(深圳金融)	bri.ap-shenzhen-fsi.tencentcloudapi.com

2. 通信协议

腾讯云 API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过32KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过1MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持10MB。

4. 字符编码

均使用 `UTF-8` 编码。

公共参数

最近更新时间：2019-06-21 19:56:03

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service 为产品名，通常为域名前缀，例如域名 cvm.tencentcloudapi.com 意味着产品名是 cvm。本产品取值为 bri； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

假设用户想要查询广州地域的云服务器实例列表，则其请求结构按照请求 URL、请求头部、请求体示例如下:

HTTP GET 请求结构示例:

```
https://cvm.tencentcloudapi.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
```

```
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: ap-guangzhou
```

HTTP POST （ application/json ）请求结构示例：

```
https://cvm.tencentcloudapi.com/

Authorization: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/2018-05-30/cvm/tc3_request, SignedHeaders=content-type;host, Signature=582c400e06b5924a6f2b5d7d672d79c15b13162d9279b0855cfba6789a8edb4c
Content-Type: application/json
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1527672334
X-TC-Region: ap-guangzhou

{"Offset":0,"Limit":10}
```

HTTP POST （ multipart/form-data ）请求结构示例（仅特定的接口支持）：

```
https://cvm.tencentcloudapi.com/

Authorization: TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/2018-05-30/cvm/tc3_request, SignedHeaders=content-type;host, Signature=582c400e06b5924a6f2b5d7d672d79c15b13162d9279b0855cfba6789a8edb4c
Content-Type: multipart/form-data; boundary=58731222010402
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1527672334
X-TC-Region: ap-guangzhou

--58731222010402
Content-Disposition: form-data; name="Offset"

0
--58731222010402
Content-Disposition: form-data; name="Limit"

10
--58731222010402--
```

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

假设用户想要查询广州地域的云服务器实例列表，其请求结构按照请求 URL、请求头部、请求体示例如下:

HTTP GET 请求结构示例:

```
https://cvm.tencentcloudapi.com/?Action=DescribeInstances&Version=2017-03-12&SignatureMethod=HmacSHA256&Timestamp=1527672334&Signature=37ac2f4fde00b0ac9bd9eadeb459b1bbee224158d66e7ae5fcadb70b2d181d02&Region=ap-guangzhou&Nonce=23823223&SecretId=AKIDEXAMPLE

Host: cvm.tencentcloudapi.com
Content-Type: application/x-www-form-urlencoded
```

HTTP POST 请求结构示例：

```
https://cvm.tencentcloudapi.com/

Host: cvm.tencentcloudapi.com
Content-Type: application/x-www-form-urlencoded

Action=DescribeInstances&Version=2017-03-12&SignatureMethod=HmacSHA256&Timestamp=1527672334&Signature=37ac2f4fde00b0ac9bd9eadeb459b1bbee224158d66e7ae5fcadb70b2d181d02&Region=ap-guangzhou&Nonce=23823223&SecretId=AKIDEXAMPLE
```

地域列表

本产品所有接口 Region 字段的可选值如下表所示。如果接口不支持该表中的所有地域，则会在接口文档中单独说明。

区域	取值
华南地区(广州)	ap-guangzhou

接口鉴权 v3

最近更新时间：2019-08-14 19:16:48

腾讯云 API 会对每个请求进行身份验证，用户需要使用安全凭证，经过特定的步骤对请求进行签名（Signature），每个请求都需要在公共请求参数中指定该签名结果并以指定的方式和格式发送请求。

申请安全凭证

本文使用的安全凭证为密钥，密钥包括 SecretId 和 SecretKey。每个用户最多可以拥有两对密钥。

- SecretId：用于标识 API 调用者身份，可以简单类比为用户名。
- SecretKey：用于验证 API 调用者的身份，可以简单类比为密码。
- **用户必须严格保管安全凭证，避免泄露，否则将危及财产安全。如已泄漏，请立刻禁用该安全凭证。**

申请安全凭证的具体步骤如下：

1. 登录 腾讯云管理中心控制台。
2. 前往 云API密钥 的控制台页面。
3. 在 云API密钥 页面，单击【新建】即可以创建一对密钥。

使用开发者资源

腾讯云 API 配套了 7 种常见的编程语言 SDK，均已开源，包括 Python、Java、PHP、Go、NodeJS、.NET、C++。同时还提供了 API Explorer 供用户在线调用、签名验证、生成 SDK 代码。如果在签名时遇到困难，请善加利用这些资源。

TC3-HMAC-SHA256 签名方法

TC3-HMAC-SHA256 签名方法相比以前的 HmacSHA1 和 HmacSHA256 签名方法，功能上覆盖了以前的签名方法，而且更安全，支持更大的请求，支持 json 格式，性能有一定提升，建议使用该签名方法计算签名。

云 API 支持 GET 和 POST 请求。对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST 方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式绝大多数接口均支持，multipart 格式只有特定接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。推荐使用 POST 请求，因为两者的结果并无差异，但 GET 请求只支持 32 KB 以内的请求包。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们选择该接口是因为：

1. 云服务器默认已开通，该接口很常用；
2. 该接口是只读的，不会改变现有资源的状态；
3. 接口覆盖的参数种类较全，可以演示包含数据结构的数组如何使用。

在示例中，不论公共参数或者接口的参数，我们尽量选择容易犯错的情况。在实际调用接口时，请根据实际情况来，每个接口的参数并不相同，不要照抄这个例子的参数和值。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE。用户想查看广州区云服务器名为"未命名"的主机状态，只返回一条数据。则请求可能为：

```
curl -X POST https://cvm.tencentcloudapi.com \
-H "Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=72e494ea809ad7a8c8f7a4507b9bddcbaa8e581f516e8da2f66e2c5a96525168" \
-H "Content-Type: application/json; charset=utf-8" \
-H "Host: cvm.tencentcloudapi.com" \
-H "X-TC-Action: DescribeInstances" \
-H "X-TC-Timestamp: 1551113065" \
-H "X-TC-Version: 2017-03-12" \
-H "X-TC-Region: ap-guangzhou" \
-d '{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name": "instance-name"}]}'
```

下面详细解释签名计算过程。

1. 拼接规范请求串

按如下伪代码格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
HTTPRequestMethod + '\n' +
CanonicalURI + '\n' +
CanonicalQueryString + '\n' +
CanonicalHeaders + '\n' +
SignedHeaders + '\n' +
HashedRequestPayload
```

字段名称	解释
HTTPRequestMethod	HTTP 请求方法（GET、POST ）。此示例取值为 `POST` 。
CanonicalURI	URI 参数，API 3.0 固定为正斜杠（/）。
CanonicalQueryString	发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串""，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，例如：Limit=10&Offset=0。 注意：CanonicalQueryString 需要经过 URL 编码。
CanonicalHeaders	参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。 拼接规则： 1. 头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接； 2. 多个头部，按照头部 key（小写）的 ASCII 升序进行拼接。 此示例计算结果是 `content-type:application/json; charset=utf-8\nhost:cvm.tencentcloudapi.com\n` 。 注意：content-type 必须和实际发送的相符合，有些编程语言网络库即使未指定也会自动添加 charset 值，如果签名时和发送时不一致，服务器会返回签名校验失败。

字段名称	解释
SignedHeaders	参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。 拼接规则： 1. 头部 key 统一转成小写； 2. 多个头部 key（小写）按照 ASCII 升序进行拼接，并且以分号（;）分隔。 此示例为 content-type;host
HashedRequestPayload	请求正文（payload，即 body，此示例为 `{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name": "instance-name"}]}` ）的哈希值，计算伪代码为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，即对 HTTP 请求正文做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。对于 GET 请求，RequestPayload 固定为空字符串。此示例计算结果是 `35e9c5b0e3ae67532d3c9f17ead6c90222632e5b1ff7f6e89887f1398934f064` 。

根据以上规则，示例中得到的规范请求串如下：

```
POST
/

content-type:application/json; charset=utf-8
host:cvm.tencentcloudapi.com

content-type;host
35e9c5b0e3ae67532d3c9f17ead6c90222632e5b1ff7f6e89887f1398934f064
```

2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
Algorithm + \n +
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

字段名称	解释
Algorithm	签名算法，目前固定为 `TC3-HMAC-SHA256` 。
RequestTimestamp	请求时间戳，即请求头部的公共参数 X-TC-Timestamp 取值，取当前时间 UNIX 时间戳，精确到秒。此示例取值为 `1551113065` 。
CredentialScope	凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。**Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致**；service 为产品名，必须与调用的产品域名一致。此示例计算结果是 2019-02-25/cvm/tc3_request。

字段名称	解释
HashedCanonicalRequest	前述步骤拼接所得规范请求串的哈希值，计算伪代码为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。此示例计算结果是 `5ffe6a04c0664d6b969fab9a13bdab201d63ee709638e2749d62a09ca18d7031` 。

注意：

1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。
2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败，返回签名过期错误。

根据以上规则，示例中得到的待签名字符串如下：

```
TC3-HMAC-SHA256
1551113065
2019-02-25/cvm/tc3_request
5ffe6a04c0664d6b969fab9a13bdab201d63ee709638e2749d62a09ca18d7031
```

3. 计算签名

1）计算派生签名密钥，伪代码如下：

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

字段名称	解释
SecretKey	原始的 SecretKey，即 `Gu5t9xGARNpq86cd98joQYCN3EXAMPLE` 。
Date	即 Credential 中的 Date 字段信息。此示例取值为 `2019-02-25` 。
Service	即 Credential 中的 Service 字段信息。此示例取值为 `cvm` 。

2）计算签名，伪代码如下：

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
Algorithm + ' ' +
```

```
'Credential=' + SecretId + '/' + CredentialScope + ', ' +
'SignedHeaders=' + SignedHeaders + ', ' +
'Signature=' + Signature
```

字段名称	解释
Algorithm	签名方法，固定为 TC3-HMAC-SHA256 。
SecretId	密钥对中的 SecretId，即 AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 。
CredentialScope	见上文，凭证范围。此示例计算结果是 2019-02-25/cvm/tc3_request 。
SignedHeaders	见上文，参与签名的头部信息。此示例取值为 content-type;host 。
Signature	签名值。此示例计算结果是 72e494ea809ad7a8c8f7a4507b9bddcbaa8e581f516e8da2f66e2c5a96525168 。

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=72e494ea809ad7a8c8f7a4507b9bddcbaa8e581f516e8da2f66e2c5a96525168
```

最终完整的调用信息如下：

```
POST https://cvm.tencentcloudapi.com/
Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host, Signature=72e494ea809ad7a8c8f7a4507b9bddcbaa8e581f516e8da2f66e2c5a96525168
Content-Type: application/json; charset=utf-8
Host: cvm.tencentcloudapi.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1551113065
X-TC-Region: ap-guangzhou

{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name": "instance-name"}]}
```

5. 签名演示

Java

```
import java.nio.charset.Charset;
import java.nio.charset.StandardCharsets;
import java.security.MessageDigest;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TencentCloudAPITC3Demo {
```

```
private final static Charset UTF8 = StandardCharsets.UTF_8;
private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
private final static String CT_JSON = "application/json; charset=utf-8";

public static byte[] hmac256(byte[] key, String msg) throws Exception {
Mac mac = Mac.getInstance("HmacSHA256");
SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
mac.init(secretKeySpec);
return mac.doFinal(msg.getBytes(UTF8));
}

public static String sha256Hex(String s) throws Exception {
MessageDigest md = MessageDigest.getInstance("SHA-256");
byte[] d = md.digest(s.getBytes(UTF8));
return DatatypeConverter.printHexBinary(d).toLowerCase();
}

public static void main(String[] args) throws Exception {
String service = "cvm";
String host = "cvm.tencentcloudapi.com";
String region = "ap-guangzhou";
String action = "DescribeInstances";
String version = "2017-03-12";
String algorithm = "TC3-HMAC-SHA256";
String timestamp = "1551113065";
//String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
// 注意时区，否则容易出错
sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

// ************ 步骤 1：拼接规范请求串 ************
String httpRequestMethod = "POST";
String canonicalUri = "/";
String canonicalQueryString = "";
String canonicalHeaders = "content-type:application/json; charset=utf-8\n" + "host:" + host + "\n";
String signedHeaders = "content-type;host";

String payload = "{\"Limit\": 1, \"Filters\": [{\"Values\": [\"\\u672a\\u547d\\u540d\"], \"Name\": \"instance-name\"}]}";
String hashedRequestPayload = sha256Hex(payload);
String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryString + "\n"
+ canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
System.out.println(canonicalRequest);

// ************ 步骤 2：拼接待签名字符串 ************
String credentialScope = date + "/" + service + "/" + "tc3_request";
String hashedCanonicalRequest = sha256Hex(canonicalRequest);
String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCanonicalRequest;
System.out.println(stringToSign);

// ************ 步骤 3：计算签名 ************
byte[] secretDate = hmac256(("TC3" + SECRET_KEY).getBytes(UTF8), date);
byte[] secretService = hmac256(secretDate, service);
```

```
byte[] secretSigning = hmac256(secretService, "tc3_request");
String signature = DatatypeConverter.printHexBinary(hmac256(secretSigning, stringToSign)).toLowerCase();
System.out.println(signature);

// ************* 步骤 4：拼接 Authorization *************
String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
+ "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
System.out.println(authorization);

TreeMap<String, String> headers = new TreeMap<String, String>();
headers.put("Authorization", authorization);
headers.put("Content-Type", CT_JSON);
headers.put("Host", host);
headers.put("X-TC-Action", action);
headers.put("X-TC-Timestamp", timestamp);
headers.put("X-TC-Version", version);
headers.put("X-TC-Region", region);

StringBuilder sb = new StringBuilder();
sb.append("curl -X POST https://").append(host)
.append(" -H \"Authorization: ").append(authorization).append("\"")
.append(" -H \"Content-Type: application/json; charset=utf-8\"")
.append(" -H \"Host: ").append(host).append("\"")
.append(" -H \"X-TC-Action: ").append(action).append("\"")
.append(" -H \"X-TC-Timestamp: ").append(timestamp).append("\"")
.append(" -H \"X-TC-Version: ").append(version).append("\"")
.append(" -H \"X-TC-Region: ").append(region).append("\"")
.append(" -d '").append(payload).append("'");
System.out.println(sb.toString());
}
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.tencentcloudapi.com"
endpoint = "https://" + host
region = "ap-guangzhou"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
#timestamp = int(time.time())
timestamp = 1551113065
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 1, "Filters": [{"Name": "instance-name", "Values": [u"未命名"]}]}
```

```
# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "POST"
canonical_uri = "/"
canonical_querystring = ""
ct = "application/json; charset=utf-8"
payload = json.dumps(params)
canonical_headers = "content-type:%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
canonical_uri + "\n" +
canonical_querystring + "\n" +
canonical_headers + "\n" +
signed_headers + "\n" +
hashed_request_payload)
print(canonical_request)

# ************* 步骤 2：拼接待签名字符串 *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
str(timestamp) + "\n" +
credential_scope + "\n" +
hashed_canonical_request)
print(string_to_sign)

# ************* 步骤 3：计算签名 *************
# 计算签名摘要函数
def sign(key, msg):
return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* 步骤 4：拼接 Authorization *************
authorization = (algorithm + " " +
"Credential=" + secret_id + "/" + credential_scope + ", " +
"SignedHeaders=" + signed_headers + ", " +
"Signature=" + signature)
print(authorization)

print('curl -X POST ' + endpoint
+ ' -H "Authorization: ' + authorization + '"'
+ ' -H "Content-Type: application/json; charset=utf-8"'
+ ' -H "Host: ' + host + '"'
+ ' -H "X-TC-Action: ' + action + '"'
+ ' -H "X-TC-Timestamp: ' + str(timestamp) + '"'
+ ' -H "X-TC-Version: ' + version + '"'
+ ' -H "X-TC-Region: ' + region + '"'
+ " -d '" + payload + "'")
```

签名失败

存在以下签名失败的错误码，请根据实际情况处理。

错误码	错误描述
AuthFailure.SignatureExpire	签名过期。Timestamp 与服务器接收到请求的时间相差不得超过五分钟。
AuthFailure.SecretIdNotFound	密钥不存在。请到控制台查看密钥是否被禁用，是否少复制了字符或者多了字符。
AuthFailure.SignatureFailure	签名错误。可能是签名计算错误，或者签名与实际发送的内容不相符合，也有可能是密钥 SecretKey 错误导致的。
AuthFailure.TokenFailure	临时证书 Token 错误。
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。

接口鉴权

最近更新时间：2019-08-14 19:16:48

腾讯云 API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。 签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往 云API密钥页面 申请，否则无法调用云 API 接口。

1. 申请安全凭证

在第一次使用云 API 之前，请前往 云 API 密钥页面 申请安全凭证。 安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- **用户必须严格保管安全凭证，避免泄露。**

申请安全凭证的具体步骤如下：

1. 登录 腾讯云管理中心控制台。
2. 前往 云 API 密钥 的控制台页面
3. 在 云 API 密钥 页面，单击【新建】即可以创建一对 SecretId/SecretKey。

注意：每个账号最多可以拥有两对 SecretId/SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥 ID	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	ap-guangzhou
InstanceIds.0	待查询的实例 ID	ins-09dx96dg

参数名称	中文	参数值
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 PHP 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
'Timestamp' : 1465185768,
'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。 将把上一步排序好的请求参数格式化成"参数名称=参数值"的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。 **注意：“参数值”为原始值而非 url 编码后的值。**

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。 签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.tencentcloudapi.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为： `请求方法 + 请求主机 +请求路径 + ? + 请求字符串` 。

示例的拼接结果为：

```
GETcvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。 首先使用 HMAC-SHA1 算法对上一步中获得的**签名原文字符串**进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例：

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为：

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt/+WcGeI=，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的网络库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中“X”和“Y”为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理。

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在

错误代码	错误描述
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的腾讯云 SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java
- PHP
- Go
- JavaScript
- .NET

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： `https://cvm.tencentcloudapi.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt/+WcGeI=&Timestamp=1465185768&Version=2017-03-12` 。

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class TencentCloudAPIDemo {
private final static String CHARSET = "UTF-8";
```

```
public static String sign(String s, String key, String method) throws Exception {
Mac mac = Mac.getInstance(method);
SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
mac.init(secretKeySpec);
byte[] hash = mac.doFinal(s.getBytes(CHARSET));
return DatatypeConverter.printBase64Binary(hash);
}

public static String getStringToSign(TreeMap<String, Object> params) {
StringBuilder s2s = new StringBuilder("GETcvm.tencentcloudapi.com/?");
// 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
for (String k : params.keySet()) {
s2s.append(k).append("=").append(params.get(k).toString()).append("&");
}
return s2s.toString().substring(0, s2s.length() - 1);
}

public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException {
StringBuilder url = new StringBuilder("https://cvm.tencentcloudapi.com/?");
// 实际请求的url中对参数顺序没有要求
for (String k : params.keySet()) {
// 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append("&");
}
return url.toString().substring(0, url.length() - 1);
}

public static void main(String[] args) throws Exception {
TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
// 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Integer.MAX_VALUE));
params.put("Nonce", 11886); // 公共参数
// 实际调用时应当使用系统当前时间，例如： params.put("Timestamp", System.currentTimeMillis() / 1000);
params.put("Timestamp", 1465185768); // 公共参数
params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
params.put("Action", "DescribeInstances"); // 公共参数
params.put("Version", "2017-03-12"); // 公共参数
params.put("Region", "ap-guangzhou"); // 公共参数
params.put("Limit", 20); // 业务参数
params.put("Offset", 0); // 业务参数
params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE", "HmacSHA1")); // 公共参数
System.out.println(getUrl(params));
}
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： `pip install requests` 。

```
# -*- coding: utf8 -*-
import base64
```

```
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
s = method + endpoint + "/?"
query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
return s + query_str

def sign_str(key, s, method):
hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
return base64.b64encode(hmac_str)

if __name__ == '__main__':
endpoint = "cvm.tencentcloudapi.com"
data = {
'Action' : 'DescribeInstances',
'InstanceIds.0' : 'ins-09dx96dg',
'Limit' : 20,
'Nonce' : 11886,
'Offset' : 0,
'Region' : 'ap-guangzhou',
'SecretId' : secret_id,
'Timestamp' : 1465185768, # int(time.time())
'Version': '2017-03-12'
}
s = get_string_to_sign("GET", endpoint, data)
data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
print(data["Signature"])
# 此处会实际调用，成功后可能产生计费
# resp = requests.get("https://" + endpoint, params=data)
# print(resp.url)
```

返回结果

最近更新时间：2019-08-14 19:16:49

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
"Response": {
"TotalCount": 0,
"InstanceStatusSet": [],
"RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
}
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0， InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。
- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	HTTPS 请求方法错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

风险查询相关接口
获取业务风险情报

最近更新时间：2019-07-24 15:05:36

1. 接口描述

接口请求域名： bri.tencentcloudapi.com 。

输入业务名 (bri_num, bri_dev, bri_ip, bri_apk, bri_url 五种之一) 及其 相应字段, 获取业务风险分数和标签。

当业务名为bri_num时，必须填PhoneNumber字段.

当业务名为bri_dev时, 必须填Imei字段.

当业务名为bri_ip时，必须填Ip字段.

当业务名为bri_apk时，必须填 (PackageName,CertMd5,FileSize) 三个字段 或者 FileMd5一个字段.

当业务名为bri_url时，必须填Url字段.

默认接口请求频率限制：20次/秒。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见 公共请求参数。

参数名称	必选	类型	描述
Action	是	String	公共参数，本接口取值：DescribeBRI
Version	是	String	公共参数，本接口取值：2019-03-28
Region	是	String	公共参数，详见产品支持的 地域列表。
RequestData	否	BRIRequest	业务风险情报请求体
ResourceId	否	String	客户用于计费的资源Id

3. 输出参数

参数名称	类型	描述
ResponseData	BRIResponse	业务风险情报响应体
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 bri_num

输入示例

```
https://bri.tencentcloudapi.com/?Action=DescribeBRI
&ResourceId= test_resource_id_for_bri_num
&RequestData.Service=bri_num
&RequestData.PhoneNumber= 18122223554
&<公共请求参数>
```

输出示例

```
{
"Response": {
"RequestId": "891f2f2e-4851-4cd8-9555-8d92d6e77902",
"ResponseData": {
"Score": 71.0,
"Tags": [
"疑似新客户"
]
}
}
}
```

5. 开发者资源

API Explorer

该工具提供了在线调用、签名验证、SDK 代码生成和快速检索接口等能力，能显著降低使用云 API 的难度，推荐使用。

- API 3.0 Explorer

SDK

云 API 3.0 提供了配套的开发工具集（SDK），支持多种编程语言，能更方便的调用 API。

- Tencent Cloud SDK 3.0 for Python
- Tencent Cloud SDK 3.0 for Java
- Tencent Cloud SDK 3.0 for PHP
- Tencent Cloud SDK 3.0 for Go
- Tencent Cloud SDK 3.0 for NodeJS
- Tencent Cloud SDK 3.0 for .NET

命令行工具

- Tencent Cloud CLI 3.0

6. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见 公共错误码。

错误码	描述
InternalError	内部错误
InternalError.Timeout	查询超时
InvalidParameter	参数错误
InvalidParameter.CertMd5	CertMd5参数错误
InvalidParameter.FileMd5	FileMd5参数错误
InvalidParameter.FileSize	FileSize参数错误
InvalidParameter.Imei	Imei参数错误
InvalidParameter.InvalidAction	接口不存在
InvalidParameter.Ip	Ip参数错误
InvalidParameter.PackageName	包名填写错误
InvalidParameter.PhoneNumber	PhoneNumber参数错误
InvalidParameter.Service	Service参数错误
InvalidParameter.Url	Url参数错误
InvalidParameterValue	参数取值错误
LimitExceeded	请求的次数超过了频率限制
MissingParameter	缺少参数错误
ResourceInsufficient	资源不足
ResourceNotFound	资源不存在
ResourceUnavailable	资源不可用
UnknownParameter	未知参数错误，用户多传未定义的参数会导致错误

数据结构

最近更新时间：2019-06-21 19:56:02

BRIRequest

BRI请求

被如下接口引用：DescribeBRI。

名称	类型	必选	描述
Service	String	是	业务名, 必须是以下五个业务名之一(bri_num,bri_dev,bri_ip_bri_apk,bri_url)
CertMd5	String	否	Apk证书Md5 (业务名为bri_apk时必填，除非已填FileMd5)
FileMd5	String	否	Apk文件Md5 (业务名为bri_apk时必填，除非已填PackageName,CertMd5,FileSize)
FileSize	Integer	否	Apk文件大小 (业务名为bri_apk时必填，除非已填FileMd5)
Imei	String	否	安卓设备的Imei (业务名为bri_dev时必填)
Ip	String	否	点分格式的IP (业务名为bri_ip时必填)
PackageName	String	否	Apk安装包名 (业务名为bri_apk时必填，除非已填FileMd5)
PhoneNumber	String	否	电话号码 (业务名为bri_num时必填)
Url	String	否	网址 (业务名为bri_url时必填)

BRIResponse

响应

被如下接口引用：DescribeBRI。

名称	类型	必选	描述
Score	Float	否	风险分值，取值[0,100], 分值越高风险越高

名称	类型	必选	描述
Tags	Array of String	否	当Service为bri_num时,返回的风险标签有: 1) 疑似垃圾流量 说明: 结合号码的历史数据表现，判断该号码历史用互联网业务作恶行为，其产生的互联网行为对于其他业务来说属于作弊或垃圾流量。 2) 疑似新客户 说明: 通过号码互联网行为（社交，浏览等）是否异常判断为小号或接码平台帐号。 当Service为bri_dev时,返回的风险标签有: 1) 疑似真机假用户 说明: 根据设备的一些数据表现，我们判定为群控设备 2) 疑似假机 说明: 根据设备的一些数据表现，我们判定为模拟器或虚假设备ID 3) 疑似真用户假行为 说明: 根据设备的用户使用情况，我们判定该用户存在使用脚本、外挂、病毒等作弊行为 当Service为bri_ip时,返回的风险标签有: 1) 疑似垃圾流量 说明:结合IP的历史数据表现，判断该IP历史用互联网业务作恶行为，其产生的互联网行为对于其他业务来说属于作弊或垃圾流量。 当Service为bri_url时,返回的风险标签有: 1) 社工欺诈 说明: URL为社工欺诈 2) 信息诈骗 说明: URL为信息诈骗 3) 虚假销售 说明: URL为虚假销售 4) 恶意文件 说明: URL为恶意文件 5) 博彩网站 说明: URL为博彩网站 6) 色情网站 说明: URL为色情网站 当Service为bri_apk时,返回的风险标签有: 1) 安全 说明: APK为正规应用 2) 一般 说明: APK为未发现问题的正常应用 3) 风险 说明: APK为外挂或色情等风险应用 4) 病毒 说明: APK为包含恶意代码的恶意软件吗,可能破坏系统或者其他app正常使用

错误码

最近更新时间：2019-07-24 15:05:37

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
"Response": {
"Error": {
"Code": "AuthFailure.SignatureFailure",
"Message": "The provided credentials could not be validated. Please check your signature is correct."
},
"RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
}
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未授权。请参考 CAM 文档对鉴权的说明。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。

错误码	说明
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	HTTP(S)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
InternalError	内部错误
InternalError.Timeout	查询超时
InvalidParameter	参数错误
InvalidParameter.CertMd5	CertMd5参数错误
InvalidParameter.FileMd5	FileMd5参数错误
InvalidParameter.FileSize	FileSize参数错误
InvalidParameter.Imei	Imei参数错误
InvalidParameter.InvalidAction	接口不存在
InvalidParameter.Ip	Ip参数错误
InvalidParameter.PackageName	包名填写错误
InvalidParameter.PhoneNumber	PhoneNumber参数错误
InvalidParameter.Service	Service参数错误

错误码	说明
InvalidParameter.Url	Url参数错误
InvalidParameterValue	参数取值错误
LimitExceeded	请求的次数超过了频率限制
MissingParameter	缺少参数错误
ResourceInsufficient	资源不足
ResourceNotFound	资源不存在
ResourceUnavailable	资源不可用
UnknownParameter	未知参数错误，用户多传未定义的参数会导致错误

业务风险情报 API 2017
号码标签接口

最近更新时间：2019-04-01 10:06:08

总体描述

本文说明腾讯广告反欺诈在线查询接口的使用方法和协议规范。通过本查询接口，可以实时查询广告流量的虚假欺诈嫌疑。

接口定义

接口总述

- 接口采用 JSON + HTTP 协议，请求和响应数据均为 UTF-8 编码。
- 使用 post 方法提交完整报文，HTTP 头部无特殊校验逻辑，报文内容均在 HTTP 消息体中。
- 接口请求域名： `api.telesafe.qq.com` 。
- 接口名：BlackLibQuery。
- 查询请求报文内容包含：请求消息头 + 请求消息体。
- 查询响应报文内容包含：响应消息头 + 响应消息体。

请求报文

- **请求消息头部 req_header 参数说明：**

参数	是否必选	类型	说明
appid	是	String	请求方唯一 ID，16个字符，每次请求时传递，用于身份识别。
timestamp	是	Int	从格林威治时间1970年01月01日00:00:00起至现在的总秒数，精确到秒，与标准时间偏差5分钟之内。
v	是	String	接口版本，此处填1.1。
nonce	是	String	单次值，随机字符串，每次请求都必须不同，防止重放攻击。
echostr	是	String	随机字符串，服务器原样带回，客户端校验，长度16个字节。
sign	是	String	请求参数签名，以下两种字符串拼接后，经 MD5 计算出的32个字符的后16个字符： • 1. header 按必选字段 key 以字典序排序后，value 拼接（不包括 sign 字段） • 2. secret（固定密钥，16位），服务端分配

- **请求消息体 req_body 参数说明：**
  req_body 是对请求内容 json 结构的加密字符串，其中请求内容定义如下：

参数名	是否必选	类型	说明
sub_appid	是	int	子业务 ID。

参数名	是否必选	类型	说明
scene	是	int	业务场景ID，详情请参见下文**业务场景 ID 说明。**
query_info	是	string	查询信息，详情请参见下文 **query_info 参数说明。**

- **业务场景 ID 说明：**

场景 ID	场景描述
1007	• 查询时机：登录/注册/营销活动等。 • 查询目的：识别垃圾流量，真机假用户，小号等。
1010	查询时机：微信 OpenID（仅针对微信场景）。 • 查询目的：识别垃圾流量，小号等。

- **query_info 参数说明：**
  query_info 是一个 json 结构，定义如下：

参数名	必选	类型	说明
phone_num	是	String	手机号。
id_num	否	String	身份证号，建议提供。
ip	是	String	IP。
os_type	是	Int	操作系统类型： • 0：未知。 • 1：Android。 • 2：iOS。 • 3：Windows。
os_ver	否	String	操作系统版本号，建议提供。
imei	是	String	Andriod 设备的 IMEI。
imsi	否	String	imsi。
mac	否	String	设备的 MAC 地址。
access_mode	否	String	入网方式，可取值有：wifi、4g、3g、2g。
name	否	String	姓名。
card_no	否	String	银行卡号。
qq	否	String	QQ 号。
wechat	否	String	微信号。
email	否	String	邮箱。
tel	否	String	固定电话。

参数名	必选	类型	说明
address	否	String	所在地址。
contact	否	String	联系人电话号码。
url	否	String	需要检测的页面链接。
context	否	String	上下文信息。
sub_scene	否	Int	子场景（由客户自定义。
idfa	否	string	iOS 的 idfa。
idfa_md5_encrypted	否	Int	idfa 是否 MD5 加密。
imei_md5_encrypted	否	Int	IMEI 是否 MD5 加密。
mac_md5_encrypted	否	Int	MAC 是否 MD5 加密。

- **加密过程：**
  i. 对请求内容用 AES 加密，加密模式 ECB ，填充方式全0，密钥为分配的 secret。
  ii. 对加密后的数据经 Base64 编码后，得到的字符串作为 req_body 的最终值。

响应报文

- **响应消息头 rsp_header 参数说明：**

参数	是否必选	说明
status	是	返回结果码： • 0：请求处理成功。 • 100：错误的 post 数据格式。 • 101：错误的请求消息头。 • 102：错误的请求参数 - appid。 • 103：错误的请求参数 - timestamp。 • 104：错误的请求参数 - body。 • 105：错误的请求参数 - v。 • 106：错误的请求参数 - nonce。 • 107：错误的请求参数 - sign。 • 108：错误的请求类型 - echostr。 • 109：错误的请求消息体。 • 110：错误的加解密方式。 • 201：访问量超过限制。 • 500：未知处理状态。 • 501：服务处理错误。
msg	是	结果/原因描述。
echostr	是	随机字符串，服务器原样带回，客户端校验，长度16个字节。

- **响应消息体 rsp_body 参数说明：**
  rsp_body 是对响应内容 json 结构加密后的字符串，加密方式参照请求体 req_body 加密过程，解密过程与加密过程逆向即可。解密

后的 json 结构如下：

参数	是否必选	类型	说明
tag	否	String	标签，表示识别为欺诈的主要原因。详情请参见下文**标签字段说明。**
evil_level	是	String	欺诈分，取值0 - 100，值越大表示欺诈概率越高。

- **标签字段说明：**

标签名	说明
疑似垃圾流量	结合设备与帐号的历史数据表现，判断该帐号/设备历史用互联网业务作恶行为，其产生的互联网行为对于其他业务来说属于作弊或垃圾流量。
疑似新客户	通过帐号互联网行为（社交，浏览等）是否异常判断为小号或接码平台帐号。
疑似假机	根据设备的一些数据表现，系统判定为模拟器或虚假设备 ID。
疑似真用户假行为	根据设备的用户使用情况，系统判定该用户存在使用脚本、外挂、病毒等作弊行为。
疑似真机假用户	根据设备的一些数据表现，系统判定为群控设备。

示例代码

- **Request 示例：**

```
{
"Header": {
"Service": "PhoneNumber",
"AppId": "XXXX"
},
"Data": {
"PhoneNumber": "13072402195",
"Ip": "103.227.172.251",
"Imei": "xxxxxx"
}
}
```

- **Response 示例：**

```
{
"Header": {
"Message": "OK",
"Service": "PhoneNumber"
},
"Data": {
"Score": 80.0,
"Tags": "疑似垃圾流量"
```

```
}
}
```

接口使用

1. 申请接口使用权限。
2. 调用对应的接口即可查询。

设备标签接口

最近更新时间：2019-04-01 10:06:13

总体描述

本文说明腾讯广告反欺诈在线查询接口的使用方法和协议规范。通过本查询接口，可以实时查询广告流量的虚假欺诈嫌疑。

接口定义

接口总述

- 接口采用 Protobuf + UDP 协议，请求和响应数据均为 UTF-8 编码。
- 接口请求域名： `api.telesafe.qq.com` 。
- 接口名：BlackLibQuery。
- 查询请求报文内容包含：4字节包体长度（不含长度数据的4字节）+请求消息。
- 查询响应报文内容包含：4字节包体长度（不含长度数据的4字节）+ 响应消息。

请求报文

- **请求消息头部 req_header 参数说明：**

参数	是否必选	类型	说明
appid	是	String	请求方唯一 ID，16个字符，每次请求时传递，用于身份识别。
timestamp	是	Int	从格林威治时间1970年01月01日00:00:00起至现在的总秒数，精确到秒，与标准时间偏差5分钟之内。
v	是	String	请求接口版本，此处填1.1。
nonce	是	String	单次值，随机字符串，每次请求都必须不同，防止重放攻击。
echostr	是	String	随机字符串，服务器原样带回，客户端校验，长度16个字节。
sign	是	String	请求参数签名，以下两种字符串拼接后，经 MD5 计算出的32个字符的后16个字符： • 1. header 按必选字段 key 以字典序排序后，value 拼接（不包括 sign 字段） • 2. secret（固定密钥，16位），服务端分配

- **请求消息体 req_body 参数说明：**
  req_body 是对请求内容 json 结构的加密字符串，其中请求内容定义如下：

参数名	是否必选	类型	说明
sub_appid	是	int	子业务 ID。
scene	是	int	业务场景ID，详情请参见下文**业务场景 ID 说明。**
query_info	是	string	查询信息，详情请参见下文 **query_info 参数说明。**

- **业务场景 ID 说明：**

场景 ID	场景描述
5001	• 查询时机：用户通知广告位时。欺诈者可能使用非正常用户的设备和虚假的广告位，用来骗取利益。

- **query_info 参数说明：**
  query_info 是一个 json 结构，定义如下：

参数	是否必选	类型	说明
ip	是	String	IP。
os_type	是	Int	操作系统类型： • 0：未知。 • 1：Android。 • 2：iOS。 • 3：Windows。
os_ver	否	String	操作系统版本号，建议提供。
imei	否	String	Andriod 设备的 IMEI。
mac	否	String	MAC 地址，建议提供。
phone_num	否	String	电话号码。
user_agent	否	String	用户端类型。
app	否	String	用户端应用。
package	否	String	应用包名。
device_maker	否	String	设备制造商。
device_module	否	String	设备型号。
access_mode	否	String	入网方式，可取值有：wifi、4g、3g、2g。
sp	否	String	运营商（移动、联通、电信等）。
device_w	否	String	设备屏幕分辨率宽度像素数。
device_h	否	String	设备屏幕分辨率高度像素数。
imp_instl	否	String	是否全屏插广告： • 0：否。 • 1：是。
imp_banner_w	否	String	广告位宽度。
imp_banner_h	否	String	广告位高度。
url	否	String	网址。

参数	是否必选	类型	说明
location	否	String	用户地址。
lat	否	Float	纬度。
lng	否	Float	经度。
context	否	String	上下文信息。
idfa	否	String	iOS 的 idfa。
idfa_md5_encrypted	否	Int	idfa 是否 MD5 加密。
imei_md5_encrypted	否	Int	IMEI 是否 MD5 加密。
mac_md5_encrypted	否	Int	MAC 是否 MD5 加密。
promote_package_name	否	String	推广 App 的 packagename。
promote_app_downloaded	否	Int	推广 App 是否下载： • 0：否。 • 1：是。 • 2：未知。
promote_app_installed	否	Int	推广 App 是否安装 • 0：否。 • 1：是。 • 2：未知。

- **加密过程：**
  i. 对请求内容用 AES 加密，加密模式 ECB ，填充方式全0，密钥为分配的 secret。
  ii. 对加密后的数据经 Base64 编码后，得到的字符串作为 req_body 的最终值。

响应报文

- **响应消息头 rsp_header 参数说明：**

参数	是否必选	说明

参数	是否必选	说明
status	是	返回结果码： • 0：请求处理成功。 • 100：错误的 post 数据格式。 • 101：错误的请求消息头。 • 102：错误的请求参数 - appid。 • 103：错误的请求参数 - timestamp。 • 104：错误的请求参数 - body。 • 105：错误的请求参数 - v。 • 106：错误的请求参数 - nonce。 • 107：错误的请求参数 - sign。 • 108：错误的请求类型 - echostr。 • 109：错误的请求消息体。 • 110：错误的加解密方式。 • 201：访问量超过限制。 • 500：未知处理状态。 • 501：服务处理错误。
msg	是	结果/原因描述。
echostr	是	随机字符串，服务器原样带回，客户端校验，长度16个字节。

- **响应消息体 rsp_body 参数说明：**
  rsp_body 是对响应内容 json 结构加密后的字符串，加密方式参照请求体 req_body 加密过程，解密过程与加密过程逆向即可。解密后的 json 结构如下：

参数	是否必选	类型	说明
evil_level	是	String	恶意等级，取值0 - 100，值越大表示恶意等级越高。
tag	否	String	标签。

示例代码

- **Request 示例：**

```
{
"req_header": {
"appid": "xxxx",
"nonce": "59f5c4a40e8634f1",
"timestamp": 1408103878,
"v": "1.1",
"echostr": "1234567890123456",
"sign": "7eba379599053ee5"
},
"req_body": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
```

其中 req_body 的原始数据为：

```
{
"scene":5001,
"query_info":
{
"ip":"2.2.2.2",
"imei":"46874874874",
"phone_num":"18989898989",
"user_agent":"ios 10.1.1",
"app":"微博",
"package":"weibo-v3.1.20d",
"device_maker":"apple",
"device_module":"iphone6s-A1700",
"mac":"34-64-A9-E6-90-A2",
"access_mode":"wifi",
"sp":"电信",
"device_w":"1980",
"device_h":"1270",
"imp_instl":"0",
"imp_banner_w":"300",
"imp_banner_h":"800",
"url":"http://xxxx.com/xxx/",
"location":"广东省深圳市南山区深南大道",
"lat":132.908002,
"lng":23.00983,
"context":"其他扩展信息..."
}
}
```

- **Response 示例：**

```
{
"rsp_header": {
"status": "0",
"msg": "请求成功",
"echostr": "1234567890123456"
},
"rsp_body": "xxxxxxxxxxxx"
}
```

其中 rsp_body 解密后如下：

```
{
"evil_level":77
}
// json obj,返回对应的结果
```

接口使用

1. 申请接口使用权限。

2. 调用对应的接口即可查询。

错误码

最近更新时间：2019-04-01 10:06:16

BRI 错误码及其说明如下表所示：

公共错误码	错误描述
InvalidParameter	参数错误（包括参数格式、类型等错误）
InvalidParameterValue	参数取值错误
MissingParameter	缺少参数错误，必传参数没填
UnknownParameter	未知参数错误，用户多传未定义的参数会导致错误
InternalError	内部错误
InvalidAction	接口不存在
RequestLimitExceeded	请求的次数超过了频率限制
NoSuchVersion	接口版本不存在
ResourceNotFound	资源不存在
ResourceUnavailable	资源不可用
ResourceInsufficient	资源不足