

配置审计

API 文档

产品文档



【版权声明】

©2013–2026 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

 Tencent Cloud

及其他腾讯云服务相关的商标均为腾讯集团下的相关公司主体所有。另外，本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

文档目录

API 文档

更新历史

Introduction

API 概览

调用方式

请求结构

公共参数

接口鉴权 v3

接口鉴权

返回结果

规则相关接口

上报自定义规则评估结果

获取规则列表

账号组获取规则列表

资源相关接口

获取资源列表

资源详情

账号组获取资源列表

数据结构

错误码

API 文档 更新历史

最近更新时间：2026-04-16 17:03:57

第 2 次发布

发布时间：2025-01-15 16:55:45

本次发布包含了以下内容：

改善已有的文档。

新增接口：

- [ListAggregateDiscoveredResources](#)

新增数据结构：

- [AggregateResourceInfo](#)

修改数据结构：

- [ConfigRule](#)
 - **修改成员：** AccountGroupId, AccountGroupName, RuleOwnerId, ManageTriggerType

第 1 次发布

发布时间：2024-12-02 15:05:48

本次发布包含了以下内容：

改善已有的文档。

新增接口：

- [DescribeDiscoveredResource](#)
- [ListAggregateConfigRules](#)
- [ListConfigRules](#)
- [ListDiscoveredResources](#)
- [PutEvaluations](#)

新增数据结构：

- [Annotation](#)
- [ConfigRule](#)
- [Evaluation](#)
- [Filter](#)
- [InputParameter](#)
- [InputParameterForManage](#)
- [ResourceListInfo](#)
- [SourceConditionForManage](#)
- [Tag](#)
- [TriggerType](#)

Introduction

最近更新时间：2026-04-16 16:48:57

CloudConfig (Config) is a cloud resource auditing and governance platform. It continuously records and evaluates the configuration information and change operations of different cloud resources in different regions under multiple customer accounts. CloudConfig (Config) supports Tencent Cloud best practices, providing customers with managed compliance rules and various scenario compliance packages, and also supports custom rules. It helps users continuously evaluate the compliance of resource configurations.

API 概览

最近更新时间：2026-04-16 17:04:52

规则相关接口

接口名称	接口功能	频率限制（次/秒）
ListAggregateConfigRules	账号组获取规则列表	20
ListConfigRules	获取规则列表	20
PutEvaluations	上报自定义规则评估结果	20

资源相关接口

接口名称	接口功能	频率限制（次/秒）
DescribeDiscoveredResource	资源详情	20
ListAggregateDiscoveredResources	账号组获取资源列表	20
ListDiscoveredResources	获取资源列表	20

调用方式

请求结构

最近更新时间：2026-04-16 17:11:34

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 `config.intl.tencentcloudapi.com`，也支持指定地域域名访问，例如广州地域的域名为 `config.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 `config.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。

注意：域名是 API 的接入点，并不代表产品或者接口实际提供服务的地域。产品支持的地域列表请在调用方式/公共参数文档中查阅，接口支持的地域请在接口文档输入参数中查阅。

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）	<code>config.intl.tencentcloudapi.com</code>
华南地区（广州）	<code>config.ap-guangzhou.tencentcloudapi.com</code>
华东地区（上海）	<code>config.ap-shanghai.tencentcloudapi.com</code>
华东地区（南京）	<code>config.ap-nanjing.tencentcloudapi.com</code>
华北地区（北京）	<code>config.ap-beijing.tencentcloudapi.com</code>
西南地区（成都）	<code>config.ap-chengdu.tencentcloudapi.com</code>
西南地区（重庆）	<code>config.ap-chongqing.tencentcloudapi.com</code>
港澳台地区（中国香港）	<code>config.ap-hongkong.tencentcloudapi.com</code>
亚太东南（新加坡）	<code>config.ap-singapore.tencentcloudapi.com</code>
亚太东南（雅加达）	<code>config.ap-jakarta.tencentcloudapi.com</code>
亚太东南（曼谷）	<code>config.ap-bangkok.tencentcloudapi.com</code>
亚太东北（首尔）	<code>config.ap-seoul.tencentcloudapi.com</code>

接入地域	域名
亚太东北（东京）	config.ap-tokyo.tencentcloudapi.com
美国东部（弗吉尼亚）	config.na-ashburn.tencentcloudapi.com
美国西部（硅谷）	config.na-siliconvalley.tencentcloudapi.com
南美地区（圣保罗）	config.sa-saopaulo.tencentcloudapi.com
欧洲地区（法兰克福）	config.eu-frankfurt.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）	config.ap-shanghai-fsi.tencentcloudapi.com
华南地区（深圳金融）	config.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），必须使用签名方法 v3（TC3-HMAC-SHA256）。
- application/x-www-form-urlencoded，必须使用签名方法 v1（HmacSHA1 或 HmacSHA256）。
- multipart/form-data（仅部分接口支持），必须使用签名方法 v3（TC3-HMAC-SHA256）。

GET 请求的请求包大小不得超过32KB。POST 请求使用签名方法 v1（HmacSHA1、HmacSHA256）时不得超过1MB。POST 请求使用签名方法 v3（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：2026-04-16 17:11:53

公共参数是用于标识用户和接口签名的参数，如非必要，在每个接口单独的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。

公共参数的具体内容会因您使用的签名方法版本不同而有所差异。

使用签名方法 v3 的公共参数

签名方法 v3（有时也称作 TC3-HMAC-SHA256）相比签名方法 v1（有些文档可能会简称签名方法），更安全，支持更大的请求包，支持 POST JSON 格式，性能有一定提升，推荐使用该签名方法计算签名。

注意：出于简化的目的，部分接口文档中的示例使用的是签名方法 v1 GET 请求，而不是更安全的签名方法 v3。

使用签名方法 v3 时，公共参数需要统一放到 HTTP Header 请求头部中，如下表所示：

参数名称	类型	必选	描述
Action	String	是	HTTP 请求头：X-TC-Action。操作的接口名称。取值参考接口文档输入参数章节关于公共参数 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	-	HTTP 请求头：X-TC-Region。地域参数，用来标识希望操作哪个地域的数据。取值参考接口文档中输入参数章节关于公共参数 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	HTTP 请求头：X-TC-Timestamp。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。
Version	String	是	HTTP 请求头：X-TC-Version。操作的 API 的版本。取值参考接口文档中输入公共参数 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=AKID***/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，AKID*** 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 为具体产品名，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 config；tc3_request 为固定字符串； - 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。
Token	String	否	HTTP 请求头：X-TC-Token。即 安全凭证服务 所颁发的临时安全凭证中的 Token，使用时需要将 SecretId 和 SecretKey 的值替换为临时安全凭证中的 TmpSecretId 和 TmpSecretKey。使用长期密钥时不能设置此 Token 字段。
Language	String	否	HTTP 请求头：X-TC-Language。指定接口返回的语言，仅部分接口支持此参数。取值：zh-CN，en-US。zh-CN 返回中文，en-US 返回英文。

假设用户想要查询广州地域的云服务器实例列表中的前十个，接口参数设置为偏移量 Offset=0，返回数量 Limit=10，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=AKID****/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=582c400e06b5924a6f2b5d7d672d79c15b13162d9279b0855cfba6789a8edb4c
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=AKID****/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=AKID****/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--

```

使用签名方法 v1 的公共参数

使用签名方法 v1（有时会称作 HmacSHA256 和 HmacSHA1），公共参数需要统一放到请求串中。

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章节关于公共参数 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	-	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。
Version	String	是	操作的 API 的版本。取值参考接口文档中输入公共参数 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	即 安全凭证服务 所颁发的临时安全凭证中的 Token，使用时需要将 SecretId 和 SecretKey 的值替换为临时安全凭证中的 TmpSecretId 和 TmpSecretKey。使用长期密钥时不能设置此 Token 字段。
Language	String	否	指定接口返回的语言，仅部分接口支持此参数。取值：zh-CN，en-US。zh-CN 返回中文，en-US 返回英文。

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

```

```
=AKID*****
```

```
Host: cvm.tencentcloudapi.com
```

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=15.
```

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。

地域	取值
港澳台地区（中国香港）	ap-hongkong
亚太东南（新加坡）	ap-singapore

接口鉴权 v3

最近更新时间：2026-04-16 17:13:47

以下文档说明了签名方法 v3 的签名过程，但仅在您编写自己的代码来调用腾讯云 API 时才有用。我们推荐您使用 [腾讯云 API Explorer](#) 和 [腾讯云命令行工具 \(TCCLI\)](#) 等开发者工具，从而无需学习如何对 API 请求进行签名。

推荐使用 API Explorer

[点击调试](#)

您可以通过 API Explorer 的【签名串生成】模块查看每个接口签名的生成过程。

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参数中指定该签名结果并以指定的方式和格式发送请求。

为什么要进行签名

签名通过以下方式帮助保护请求：

1. 验证请求者的身份

签名确保请求是由持有有效访问密钥的人发送的。请参阅控制台 [云 API 密钥](#) 页面获取密钥相关信息。

2. 保护传输中的数据

为了防止请求在传输过程中被篡改，腾讯云 API 会使用请求参数来计算请求的哈希值，并将生成的哈希值加密后作为请求的一部分，发送到腾讯云 API 服务器。服务器会使用收到的请求参数以同样的过程计算哈希值，并验证请求中的哈希值。如果请求被篡改，将导致哈希值不一致，腾讯云 API 将拒绝本次请求。

签名方法 v3 (TC3-HMAC-SHA256) 功能上覆盖了以前的签名方法 v1，而且更安全，支持更大的请求，支持 JSON 格式，POST 请求支持传空数组和空字符串，性能有一定提升，推荐使用该签名方法计算签名。

首次接触，建议使用 [API Explorer](#) 中的“签名串生成”功能，选择签名版本为“API 3.0 签名 v3”，可以对生成签名过程进行验证，也可直接生成 SDK 代码。推荐使用腾讯云 API 配套的 7 种常见的编程语言 SDK，已经封装了签名和请求过程，均已开源，支持 [Python](#)、[Java](#)、[PHP](#)、[Go](#)、[NodeJS](#)、[.NET](#)、[C++](#)。

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。如已泄露，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【新建密钥】创建一对密钥。

签名版本 v3 签名过程

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齐全，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。此外，这里只展示了部分公共参数和接口输入参数，用户可以根据实际需要添加其他参数，例如 Language 和 Token 公共参数（在 HTTP 头部设置，添加 X-TC- 前缀）。

假设用户的 SecretId 和 SecretKey 分别是：`AKID*****` 和 `*****`。用户想查看广州云服务器名为“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=AKID*****
*/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host;x-tc-action, Signat
ure=10b1a37a7301a02ca19a647ad722d5e43b4b3cff309d421d85b46093f6ab6c4f" \
-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 <code>POST</code> 。
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 中间号 (?) 后面的字符串内容, 例如: <code>Limit=10&Offset=0</code> 。 注意: CanonicalQueryString 需要参考 RFC3986 进行 URLEncode 编码 (特殊字符编码后需大写字母), 字符集 UTF-8。推荐使用编程语言标准库进行编码。
CanonicalHeaders	参与签名的头部信息, 至少包含 <code>host</code> 和 <code>content-type</code> 两个头部, 也可加入其他头部参与签名以提高自身请求的唯一性和安全性, 此示例额外增加了接口名头部。 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 <code>key:value\n</code> 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 <code>content-type:application/json; charset=utf-8\nhost:cvm.tencentcloudapi.com\nx-tc-action:describeinstances\n</code> 。 注意: <code>content-type</code> 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 <code>charset</code> 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。
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。 <code>content-type</code> 和 <code>host</code> 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 <code>content-type;host;x-tc-action</code>
HashedRequestPayload	请求正文 (payload, 即 body, 此示例为 <code>{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name": "instance-name"}]}</code>) 的哈希值, 计算伪代码为 <code>Lowercase(HexEncode(Hash.SHA256(RequestPayload)))</code> , 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 <code>35e9c5b0e3ae67532d3c9f17ead6c90222632e5b1ff7f6e89887f1398934f064</code> 。

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
x-tc-action:describeinstances

content-type;host;x-tc-action
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 <code>TC3-HMAC-SHA256</code> 。
RequestTimestamp	请求时间戳，即请求头部的公共参数 <code>X-TC-Timestamp</code> 取值，取当前时间 UNIX 时间戳，精确到秒。此示例取值为 <code>1551113065</code> 。
CredentialScope	凭证范围，格式为 <code>Date/service/tc3_request</code> ，包含日期、所请求的服务和终止字符串 (<code>tc3_request</code>)。 <code>Date</code> 为 UTC 标准时间的日期，取值需要和公共参数 <code>X-TC-Timestamp</code> 换算的 UTC 标准时间日期一致； <code>service</code> 为产品名，必须与调用的产品域名一致。此示例计算结果是 <code>2019-02-25/cvm/tc3_request</code> 。
HashedCanonicalRequest	前述步骤拼接所得规范请求串的哈希值，计算伪代码为 <code>Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))</code> 。此示例计算结果是 <code>7019a55be8395899b900fb5564e4200d984910f34794a27cb3fb7d10ff6a1e84</code> 。

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，可能运行一段时间后，请求失败，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
7019a55be8395899b900fb5564e4200d984910f34794a27cb3fb7d10ff6a1e84
```

3. 计算签名

1) 计算派生签名密钥，伪代码如下：

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

派生出的密钥 `SecretDate`、`SecretService` 和 `SecretSigning` 是二进制的数，可能包含不可打印字符，将其转为十六进制字符串打印的输出分别为：

```
da98fb70dcf6b112dc21038d1eeeb3a95c74b4dcb12c1131f864f6066bd02be0,
8d70cbefb03939f929db64d32dc2ba89b1095620119fe3e050e2b18c5bd2752f,
b596b923aad85185e2d1f6659d2a062e0a86731226e021e61bfe06f7ed05f5af.
```

请注意，不同的编程语言，HMAC 库函数中参数顺序可能不一样，请以实际情况为准。此处的伪代码密钥参数 `key` 在前，消息参数 `data` 在后。通常标准库函数会提供二进制格式的返回值，也可能会提供打印友好的十六进制格式的返回值，此处使用的是二进制格式。

字段名称	解释
SecretKey	原始的 SecretKey，即 *****。
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))
```

此示例计算结果是 10b1a37a7301a02ca19a647ad722d5e43b4b3cff309d421d85b46093f6ab6c4f。

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 <code>TC3-HMAC-SHA256</code> 。
SecretId	密钥对中的 SecretId, 即 <code>AKID*****</code> 。
CredentialScope	见上文, 凭证范围。此示例计算结果是 <code>2019-02-25/cvm/tc3_request</code> 。
SignedHeaders	见上文, 参与签名的头部信息。此示例取值为 <code>content-type;host;x-tc-action</code> 。
Signature	签名值。此示例计算结果是 <code>10b1a37a7301a02ca19a647ad722d5e43b4b3cff309d421d85b46093f6ab6c4f</code> 。

根据以上规则, 示例中得到的值为:

```
TC3-HMAC-SHA256 Credential=AKID*****/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host;x-tc-action, Signature=10b1a37a7301a02ca19a647ad722d5e43b4b3cff309d421d85b46093f6ab6c4f
```

最终完整的调用信息如下:

```
POST https://cvm.tencentcloudapi.com/
Authorization: TC3-HMAC-SHA256 Credential=AKID*****/2019-02-25/cvm/tc3_request, SignedHeaders=content-type;host;x-tc-action, Signature=10b1a37a7301a02ca19a647ad722d5e43b4b3cff309d421d85b46093f6ab6c4f
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"}
```

```
<blockquote class="d-mod-notice">
<div class="d-mod-title d-notice-title">
<i class="d-icon-notice"></i>注意:
```

</div>

<p>
请求发送时的 HTTP 头部 (Header) 和请求体 (Payload) 必须和签名计算过程中的内容完全一致, 否则会返回签名不一致错误。可以通过打印实际请求内容, 网络抓包等方式对比排查。</p>

</blockquote>

<h2 id=".E7.AD.BE.E5.90.8D.E6.BC.94.E7.A4.BA">签名演示</h2><p>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。当前支持的编程语言有: </p>

- [Python](#)
- [Java](#)
- [PHP](#)
- [Go](#)
- [NodeJS](#)
- [.NET](#)
- [C++](#)

下面提供了不同产品的生成签名 demo, 您可以找到对应的产品参考签名的生成:

- [Signature Demo](#)

为了更清楚地解释签名过程, 下面以实际编程语言为例, 将上述的签名过程完整实现。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。

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;
    // 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
    private final static String SECRET_ID = System.getenv("TENCENTCLOUD_SECRET_ID");
    // 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
    private final static String SECRET_KEY = System.getenv("TENCENTCLOUD_SECRET_KEY");
}
```

```
Y");
private final static String CT_JSON = "application/json; charset=utf-8";

<span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span>
<span class="hljs-keyword">byte</span>[] hmac256(<span class="hljs-keyword">byte</span>[] key, <span class="hljs-keyword">String</span> msg) <span class="hljs-keyword">throws</span> E
xception {
    Mac mac = Mac.getInstance(<span class="hljs-string">"HmacSHA256"</span>);
    SecretKeySpec secretKeySpec = <span class="hljs-keyword">new</span> SecretKeySpec(key, mac.getAlgorithm());
    mac.init(secretKeySpec);
    <span class="hljs-keyword">return</span> mac.doFinal(msg.getBytes(UTF8));
}

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> <span class="hljs-keyword">String</span> <span class="hljs-title">sha256Hex</span>
<span class="hljs-params">(String s)</span> <span class="hljs-keyword">throws</span> Exception {
    MessageDigest md = MessageDigest.getInstance(<span class="hljs-string">"SHA-256"</span>);
    <span class="hljs-keyword">byte</span>[] d = md.digest(s.getBytes(UTF8));
    <span class="hljs-keyword">return</span> DatatypeConverter.printHexBinary(d).
toLowerCase();
}

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> <span class="hljs-keyword">void</span> <span class="hljs-title">main</span>
<span class="hljs-params">(String[] args)</span> <span class="hljs-keyword">throws</span> Exception {
    <span class="hljs-string">"</span>cvm<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>cvm.tencentcloudapi.com<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>ap-guangzhou<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>DescribeInstances<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>2017-03-12<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>TC3-HMAC-SHA256<span class="hljs-string">"</span>;
    <span class="hljs-string">"</span>1551113065<span class="hljs-string">"</span>;
    <span class="hljs-comment">//String timestamp = String.valueOf(System.current
TimeMillis() / 1000);</span>
    SimpleDateFormat sdf = <span class="hljs-keyword">new</span> SimpleDateFormat
(<span class="hljs-string">"</span>yyyy-MM-dd<span class="hljs-string">"</span>);
    <span class="hljs-comment">// 注意时区，否则容易出错</span>
    sdf.setTimeZone(TimeZone.getTimeZone(<span class="hljs-string">"</span>UTC<span class="hljs-string">"</span>);
```

```

t;</span>));
String date = sdf.format(<span class="hljs-keyword">new</span> Date(Long.valu
eof(timestamp + <span class="hljs-string">&quot;000&quot;</span>));

<span class="hljs-comment">// ***** 步骤 1: 拼接规范请求串 *****
</span>
String httpRequestMethod = <span class="hljs-string">&quot;POST&quot;</span>;
String canonicalUri = <span class="hljs-string">&quot;/&quot;</span>;
String canonicalQueryString = <span class="hljs-string">&quot;&quot;</span>;
String canonicalHeaders = <span class="hljs-string">&quot;content-type:applic
ation/json; charset=utf-8\n&quot;</span>
+ <span class="hljs-string">&quot;host:&quot;</span> + host + <span class="hljs-
string">&quot;\n&quot;</span> + <span class="hljs-string">&quot;x-tc-actio
n:&quot;</span> + action.toLowerCase() + <span class="hljs-string">&quot;\n&q
uot;</span>;
String signedHeaders = <span class="hljs-string">&quot;content-type;host;x-tc
-action&quot;</span>;

String payload = <span class="hljs-string">&quot;{\&quot;Limit\&quot;: 1, \&
quot;Filters\&quot;: [{\&quot;Values\&quot;: [\&quot;\u672a\u547d\u540d\&
quot;], \&quot;Name\&quot;: \&quot;instance-name\&quot;}}]&quot;</span>;
String hashedRequestPayload = sha256Hex(payload);
String canonicalRequest = httpRequestMethod + <span class="hljs-string">&quo
t;\n&quot;</span> + canonicalUri + <span class="hljs-string">&quot;\n&quot;</
span> + canonicalQueryString + <span class="hljs-string">&quot;\n&quot;</span
>
+ canonicalHeaders + <span class="hljs-string">&quot;\n&quot;</span> + signed
Headers + <span class="hljs-string">&quot;\n&quot;</span> + hashedRequestPayl
oad;
System.out.println(canonicalRequest);

<span class="hljs-comment">// ***** 步骤 2: 拼接待签名字符串 *****
* </span>
String credentialScope = date + <span class="hljs-string">&quot;/&quot;</span>
+ service + <span class="hljs-string">&quot;/&quot;</span> + <span class="h
ljs-string">&quot;tc3_request&quot;</span>;
String hashedCanonicalRequest = sha256Hex(canonicalRequest);
String stringToSign = algorithm + <span class="hljs-string">&quot;\n&quot;</s
pan> + timestamp + <span class="hljs-string">&quot;\n&quot;</span> + credenti
alScope + <span class="hljs-string">&quot;\n&quot;</span> + hashedCanonicalRe
quest;
System.out.println(stringToSign);

<span class="hljs-comment">// ***** 步骤 3: 计算签名 *****</spa
n>
<span class="hljs-keyword">byte</span>[] secretDate = hmac256((<span class="h
ljs-string">&quot;TC3&quot;</span> + SECRET_KEY).getBytes(UTF8), date);

```

```

<span class="hljs-keyword">byte</span>[] secretService = hmac256(secretDate,
service);
<span class="hljs-keyword">byte</span>[] secretSigning = hmac256(secretService,
<span class="hljs-string">“tc3_request”</span>);
String signature = DatatypeConverter.printHexBinary(hmac256(secretSigning, st
ringToSign)).toLowerCase();
System.out.println(signature);

<span class="hljs-comment">// ***** 步骤 4: 拼接 Authorization *****
*****</span>
String authorization = algorithm + <span class="hljs-string">“ ”</s
pan> + <span class="hljs-string">“Credential=“</span> + SECRET_ID +
<span class="hljs-string">“/“</span> + credentialScope + <span clas
s="hljs-string">“ , “</span>
+ <span class="hljs-string">“SignedHeaders=“</span> + signedHeaders
+ <span class="hljs-string">“ , , “</span> + <span class="hljs-strin
g">“Signature=“</span> + signature;
System.out.println(authorization);

TreeMap<String, String> headers = <span class="hljs-keyword">new</span> Tr
eeMap<String, String>();
headers.put(<span class="hljs-string">“Authorization“</span>, autho
rization);
headers.put(<span class="hljs-string">“Content-Type“</span>, CT_JSO
N);
headers.put(<span class="hljs-string">“Host“</span>, host);
headers.put(<span class="hljs-string">“X-TC-Action“</span>, actio
n);
headers.put(<span class="hljs-string">“X-TC-Timestamp“</span>, time
stamp);
headers.put(<span class="hljs-string">“X-TC-Version“</span>, versio
n);
headers.put(<span class="hljs-string">“X-TC-Region“</span>, regio
n);

StringBuilder sb = <span class="hljs-keyword">new</span> StringBuilder();
sb.append(<span class="hljs-string">“curl -X POST https://“</span>
).append(host)
.append(<span class="hljs-string">“ -H “</span>Authorization: “</spa
n>).append(authorization).append(<span class="hljs-string">“ “</span>
);
.append(<span class="hljs-string">“ -H “</span>Content-Type: application/
json; charset=utf-8“</span>
).append(<span class="hljs-string">“ -H “</span>Host: “</span>).append
(host).append(<span class="hljs-string">“ “</span>
).append(<span class="hljs-string">“ -H “</span>X-TC-Action: “</span
>).append(action).append(<span class="hljs-string">“ “</span>

```

```

>)
.append(<span class="hljs-string">&quot;; -H \&quot;;X-TC-Timestamp: &quot;;</span
an>).append(timestamp).append(<span class="hljs-string">&quot;;\&quot;;&quot;;</
span>)
.append(<span class="hljs-string">&quot;; -H \&quot;;X-TC-Version: &quot;;</span
>).append(version).append(<span class="hljs-string">&quot;;\&quot;;&quot;;</span
>)
.append(<span class="hljs-string">&quot;; -H \&quot;;X-TC-Region: &quot;;</span
>).append(region).append(<span class="hljs-string">&quot;;\&quot;;&quot;;</span
>)
.append(<span class="hljs-string">&quot;; -d &#x27;&quot;;</span>).append(payload)
.append(<span class="hljs-string">&quot;;&#x27;&quot;;</span>);
System.out.println(sb.toString());
}
}

```

Python

```

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

# 密钥参数
# 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
secret_id = os.environ.get("TENCENTCLOUD_SECRET_ID")
# 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
secret_key = os.environ.get("TENCENTCLOUD_SECRET_KEY")

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": [{"Values": [u"未命名"], "Name": "instance-name"}]}

# * 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\nx-tc-action:%s\n" % (ct, host, action.lower())
signed_headers = "content-type;host;x-tc-action"
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
```

```

+ <span class="hljs-string">#x27; -H &quot;Authorization: &#x27;</span> + au
thorization + <span class="hljs-string">#x27;&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;Content-Type: application/json; c
harset=utf-8&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;Host: &#x27;</span> + host + <spa
n class="hljs-string">#x27;&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;X-TC-Action: &#x27;</span> + acti
on + <span class="hljs-string">#x27;&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;X-TC-Timestamp: &#x27;</span> + <
span class="hljs-built_in">str</span>(timestamp) + <span class="hljs-string">
&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;X-TC-Version: &#x27;</span> + ver
sion + <span class="hljs-string">#x27;&quot;&#x27;</span>
+ <span class="hljs-string">#x27; -H &quot;X-TC-Region: &#x27;</span> + regi
on + <span class="hljs-string">#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&quot; -d &#x27;&quot;</span> + payload + <span c
lass="hljs-string">&quot;&#x27;&quot;</span>

```

Golang

```

package main

import (
    "crypto/hmac"
    "crypto/sha256"
    "encoding/hex"
    "fmt"
    "os"
    "strings"
    "time"
)

func sha256hex(s string) string {
    b := sha256.Sum256([]byte(s))
    return hex.EncodeToString(b[:])
}

func hmacsha256(s, key string) string {
    hashed := hmac.New(sha256.New, []byte(key))
    hashed.Write([]byte(s))
    return string(hashed.Sum(nil))
}

```

```

func main() {
// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
secretId := os.Getenv("TENCENTCLOUD_SECRET_ID")
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
secretKey := os.Getenv("TENCENTCLOUD_SECRET_KEY")
host := "cvm.tencentcloudapi.com"
algorithm := "TC3-HMAC-SHA256"
service := "cvm"
version := "2017-03-12"
action := "DescribeInstances"
region := "ap-guangzhou"
//var timestamp int64 = time.Now().Unix()
var timestamp int64 = 1551113065

// step 1: build canonical request string
httpRequestMethod := "POST"
canonicalURI := "/"
canonicalQueryString := ""
canonicalHeaders := fmt.Sprintf("content-type:%s\nhost:%s\nx-tc-action:%s\n",
"application/json; charset=utf-8",
host, strings.ToLower(action))
signedHeaders := "content-type;host;x-tc-action"
payload := `{"Limit": 1, "Filters": [{"Values": [{"\u672a\u547d\u540d}], "Name": "instance-name"}]`
hashedRequestPayload := sha256hex(payload)
canonicalRequest := fmt.Sprintf("%s\n%s\n%s\n%s\n%s\n%s\n%s",
httpRequestMethod,
canonicalURI,
canonicalQueryString,
canonicalHeaders,
signedHeaders,
hashedRequestPayload)
fmt.Println(canonicalRequest)

// step 2: build string to sign
date := time.Unix(timestamp, 0).UTC().Format("2006-01-02")
credentialScope := fmt.Sprintf("%s/%s/tc3_request", date, service)
hashedCanonicalRequest := sha256hex(canonicalRequest)
string2sign := fmt.Sprintf("%s\n%d\n%s\n%s"

```

```

t;</span>,
algorithm,
timestamp,
credentialScope,
hashedCanonicalRequest)
fmt.Println(string2sign)

<span class="hljs-comment">// step 3: sign string</span>
secretDate := hmacsha256(date, <span class="hljs-string">&quot;TC3&quot;</span>+secretKey)
secretService := hmacsha256(service, secretDate)
secretSigning := hmacsha256(<span class="hljs-string">&quot;tc3_request&quot;</span>, secretService)
signature := hex.EncodeToString([]<span class="hljs-keyword">byte</span>(hmacsha256(string2sign, secretSigning)))
fmt.Println(signature)

<span class="hljs-comment">// step 4: build authorization</span>
authorization := fmt.Sprintf(<span class="hljs-string">&quot;%s Credential=%s/%s, SignedHeaders=%s, Signature=%s&quot;</span>,
algorithm,
secretId,
credentialScope,
signedHeaders,
signature)
fmt.Println(authorization)

curl := fmt.Sprintf(<span class="hljs-string">&#39;curl -X POST https://%s\
-H "Authorization: %s"
-H "Content-Type: application/json; charset=utf-8"
-H "Host: %s" -H "X-TC-Action: %s"
-H "X-TC-Timestamp: %d"
-H "X-TC-Version: %s"
-H "X-TC-Region: %s"
-d '%s'` , host, authorization, host, action, timestamp, version, region, payload)
fmt.Println(curl)
}

```

PHP

```

<?php
// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID*****
*****
$secretId = getenv("TENCENTCLOUD_SECRET_ID");
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 *****

```

```
***
$secretKey = getenv("TENCENTCLOUD_SECRET_KEY");
$host = "cvm.tencentcloudapi.com";
$service = "cvm";
$version = "2017-03-12";
$action = "DescribeInstances";
$region = "ap-guangzhou";
// $timestamp = time();
$timestamp = 1551113065;
$algorithm = "TC3-HMAC-SHA256";

// step 1: build canonical request string
$httpRequestMethod = "POST";
$canonicalUri = "/";
$canonicalQueryString = "";
$canonicalHeaders = implode("\n", [
    "content-type:application/json; charset=utf-8",
    "host:".$host,
    "x-tc-action:".strtolower($action),
    ""
]);
$signedHeaders = implode(";", [
    "content-type",
    "host",
    "x-tc-action",
]);
$payload = '{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name":
"instance-name"}]'};
$hashedRequestPayload = hash("SHA256", $payload);
$canonicalRequest = $httpRequestMethod."\n"
.$canonicalUri."\n"
.$canonicalQueryString."\n"
.$canonicalHeaders."\n"
.$signedHeaders."\n"
.$hashedRequestPayload;
echo $canonicalRequest.PHP_EOL;

// step 2: build string to sign
$date = gmdate("Y-m-d", $timestamp);
$credentialScope = $date."/".$service."/tc3_request";
$hashedCanonicalRequest = hash("SHA256", $canonicalRequest);
$stringToSign = $algorithm."\n"
.$timestamp."\n"
.$credentialScope."\n"
.$hashedCanonicalRequest;
echo $stringToSign.PHP_EOL;
```

```
// step 3: sign string
$secretDate = hash_hmac("SHA256", $date, "TC3".$secretKey, true);
$secretService = hash_hmac("SHA256", $service, $secretDate, true);
$secretSigning = hash_hmac("SHA256", "tc3_request", $secretService, true);
$signature = hash_hmac("SHA256", $stringToSign, $secretSigning);
echo $signature.PHP_EOL;

// step 4: build authorization
$authorization = $algorithm
." Credential=".$secretId."/".$credentialScope
.", SignedHeaders=".$signedHeaders.", Signature=".$signature;
echo $authorization.PHP_EOL;

$curl = "curl -X POST https://".$host
." -H "Authorization: ".$authorization.""
." -H "Content-Type: application/json; charset=utf-8""
." -H "Host: ".$host.""
." -H "X-TC-Action: ".$action.""
." -H "X-TC-Timestamp: ".$timestamp.""
." -H "X-TC-Version: ".$version.""
." -H "X-TC-Region: ".$region.""
." -d ".$payload.""";
echo $curl.PHP_EOL;
```

Ruby

```
# -*- coding: UTF-8 -*-
# require ruby>=2.3.0
require 'digest'
require 'json'
require 'time'
require 'openssl'

# 密钥参数
# 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
secret_id = ENV["TENCENTCLOUD_SECRET_ID"]
# 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
secret_key = ENV["TENCENTCLOUD_SECRET_KEY"]

service = 'cvm'
host = 'cvm.tencentcloudapi.com'
endpoint = 'https://' + host
region = 'ap-guangzhou'
```

```
action = 'DescribeInstances'
version = '2017-03-12'
algorithm = 'TC3-HMAC-SHA256'
# timestamp = Time.now.to_i
timestamp = 1551113065
date = Time.at(timestamp).utc.strftime('%Y-%m-%d')

# * 步骤 1: 拼接规范请求串 *
http_request_method = 'POST'
canonical_uri = '/'
canonical_querystring = ''
canonical_headers = "content-type:application/json; charset=utf-8\nhost:#{host}\n
x-tc-action:#{action.downcase}\n"
signed_headers = 'content-type;host;x-tc-action'
# params = { 'Limit' => 1, 'Filters' => [{ 'Name' => 'instance-name', 'Values' =>
['未命名'] }] }
# payload = JSON.generate(params, { 'ascii_only' => true, 'space' => ' ' })
# json will generate in random order, to get specified result in example, we hard
-code it here.
payload = '{"Limit": 1, "Filters": [{"Values": ["\u672a\u547d\u540d"], "Name": "i
nstance-name"}]}'
hashed_request_payload = Digest::SHA256.hexdigest(payload)
canonical_request = [
http_request_method,
canonical_uri,
canonical_querystring,
canonical_headers,
signed_headers,
hashed_request_payload,
].join("\n")

puts canonical_request

# * 步骤 2: 拼接待签名字符串 *
credential_scope = date + '/' + service + '/' + 'tc3_request'
hashed_request_payload = Digest::SHA256.hexdigest(canonical_request)
string_to_sign = [
algorithm,
timestamp.to_s,
credential_scope,
hashed_request_payload,
].join("\n")
puts string_to_sign

# * 步骤 3: 计算签名 *
digest = OpenSSL::Digest.new('sha256')
```

```

secret_date = OpenSSL::HMAC.digest(digest, 'TC3' + secret_key, date)
secret_service = OpenSSL::HMAC.digest(digest, secret_date, service)
secret_signing = OpenSSL::HMAC.digest(digest, secret_service, 'tc3_request')
signature = OpenSSL::HMAC.hexdigest(digest, secret_signing, string_to_sign)
puts signature

# * 步骤 4: 拼接 Authorization *
authorization = "#{algorithm} Credential=#{secret_id}/#{credential_scope}, Signed
Headers=#{signed_headers}, Signature=#{signature}"
puts authorization

puts 'curl -X POST ' + endpoint \

+ <span class="hljs-string">#x27; -H &quot;Authorization: &#x27;</span> + au
thorization + <span class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;Content-Type: application/json; c
harset=utf-8&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;Host: &#x27;</span> + host + <spa
n class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;X-TC-Action: &#x27;</span> + acti
on + <span class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;X-TC-Timestamp: &#x27;</span> + t
imestamp.to_s + <span class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;X-TC-Version: &#x27;</span> + ver
sion + <span class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27; -H &quot;X-TC-Region: &#x27;</span> + regi
on + <span class="hljs-string">#x27;&quot;&#x27;</span> \
+ <span class="hljs-string">#x27;&quot; -d &#x27;&quot;&#x27;</span> + payload + <span c
lass="hljs-string">#x27;&quot;&#x27;&quot;&#x27;</span>

```

DotNet

```

using System;
using System.Collections.Generic;
using System.Security.Cryptography;
using System.Text;

public class Application
{
    public static string SHA256Hex(string s)
    {
        using (SHA256 algo = SHA256.Create())
        {

```

```

byte[] hashbytes = algo.ComputeHash(Encoding.UTF8.GetBytes(s));
StringBuilder builder = new StringBuilder();
for (int i = 0; i < hashbytes.Length; ++i)
{
builder.Append(hashbytes[i].ToString("x2"));
}
return builder.ToString();
}
}

```

```

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> <span class="hljs-built_in">byte</span>[] <span class="hljs-title">HmacSHA256</span>(<span class="hljs-params"><span class="hljs-built_in">byte</span>[] key, <span class="hljs-built_in">byte</span>[] msg</span>)</span>
{
<span class="hljs-keyword">using</span> (HMACSHA256 mac = <span class="hljs-keyword">new</span> HMACSHA256(key))
{
<span class="hljs-keyword">return</span> mac.ComputeHash(msg);
}
}

```

```

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> Dictionary<String, String> <span class="hljs-title">BuildHeaders</span>(<span class="hljs-params"><span class="hljs-built_in">string</span> secretid,
<span class="hljs-built_in">string</span> secretkey, <span class="hljs-built_in">string</span> service, <span class="hljs-built_in">string</span> endpoint, <span class="hljs-built_in">string</span> region,
<span class="hljs-built_in">string</span> action, <span class="hljs-built_in">string</span> version, DateTime date, <span class="hljs-built_in">string</span> requestPayload</span>)</span>
{
<span class="hljs-built_in">string</span> datestr = date.ToString(<span class="hljs-string">&quot;yyyy-MM-dd&quot;</span>);
DateTime startTime = <span class="hljs-keyword">new</span> DateTime(<span class="hljs-number">1970</span>, <span class="hljs-number">1</span>, <span class="hljs-number">1</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>,
DateTimeKind.Utc);
<span class="hljs-built_in">long</span> requestTimestamp = (<span class="hljs-built_in">long</span>Math.Round((date - startTime).TotalMilliseconds, MidpointRounding.AwayFromZero) / <span class="hljs-number">1000</span>);
<span class="hljs-comment">// ***** 步骤 1: 拼接规范请求串 *****</span>
</span>

```

```
<span class="hljs-built_in">string</span> algorithm = <span class="hljs-string">&quot;TC3-HMAC-SHA256&quot;</span>;
<span class="hljs-built_in">string</span> httpRequestMethod = <span class="hljs-string">&quot;POST&quot;</span>;
<span class="hljs-built_in">string</span> canonicalUri = <span class="hljs-string">&quot;/&quot;</span>;
<span class="hljs-built_in">string</span> canonicalQueryString = <span class="hljs-string">&quot;&quot;</span>;
<span class="hljs-built_in">string</span> contentType = <span class="hljs-string">&quot;application/json&quot;</span>;
<span class="hljs-built_in">string</span> canonicalHeaders = <span class="hljs-string">&quot;content-type:&quot;</span> + contentType + <span class="hljs-string">&quot;; charset=utf-8\n&quot;</span>
+ <span class="hljs-string">&quot;host:&quot;</span> + endpoint + <span class="hljs-string">&quot;\n&quot;</span>
+ <span class="hljs-string">&quot;x-tc-action:&quot;</span> + action.ToLower
() + <span class="hljs-string">&quot;\n&quot;</span>;
<span class="hljs-built_in">string</span> signedHeaders = <span class="hljs-string">&quot;content-type;host;x-tc-action&quot;</span>;
<span class="hljs-built_in">string</span> hashedRequestPayload = SHA256Hex(requestPayload);
<span class="hljs-built_in">string</span> canonicalRequest = httpRequestMethod + <span class="hljs-string">&quot;\n&quot;</span>
+ canonicalUri + <span class="hljs-string">&quot;\n&quot;</span>
+ canonicalQueryString + <span class="hljs-string">&quot;\n&quot;</span>
+ canonicalHeaders + <span class="hljs-string">&quot;\n&quot;</span>
+ signedHeaders + <span class="hljs-string">&quot;\n&quot;</span>
+ hashedRequestPayload;
Console.WriteLine(canonicalRequest);

<span class="hljs-comment">// ***** 步骤 2: 拼接待签名字符串 *****
*</span>
<span class="hljs-built_in">string</span> credentialScope = datestr + <span class="hljs-string">&quot;/&quot;</span> + service + <span class="hljs-string">&quot;/&quot;</span> + <span class="hljs-string">&quot;tc3_request&quot;</span>;
<span class="hljs-built_in">string</span> hashedCanonicalRequest = SHA256Hex
(canonicalRequest);
<span class="hljs-built_in">string</span> stringToSign = algorithm + <span class="hljs-string">&quot;\n&quot;</span>
+ requestTimestamp.ToString() + <span class="hljs-string">&quot;\n&quot;</span>
+ credentialScope + <span class="hljs-string">&quot;\n&quot;</span>
+ hashedCanonicalRequest;
Console.WriteLine(stringToSign);

<span class="hljs-comment">// ***** 步骤 3: 计算签名 *****</span>
```

```

n>
<span class="hljs-built_in">byte</span>[] tc3SecretKey = Encoding.UTF8.GetBytes(
<span class="hljs-string">&quot;TC3&quot;</span> + secretkey);
<span class="hljs-built_in">byte</span>[] secretDate = HmacSHA256(tc3SecretKey,
Encoding.UTF8.GetBytes(datestr));
<span class="hljs-built_in">byte</span>[] secretService = HmacSHA256(secretDate,
Encoding.UTF8.GetBytes(service));
<span class="hljs-built_in">byte</span>[] secretSigning = HmacSHA256(secretService,
Encoding.UTF8.GetBytes(<span class="hljs-string">&quot;tc3_request&quot;</span>));
<span class="hljs-built_in">byte</span>[] signatureBytes = HmacSHA256(secretSigning,
Encoding.UTF8.GetBytes(stringToSign));
<span class="hljs-built_in">string</span> signature = BitConverter.ToString(signatureBytes).Replace(
<span class="hljs-string">&quot;-&quot;</span>, <span class="hljs-string">&quot;&quot;</span>).ToLower();
Console.WriteLine(signature);

<span class="hljs-comment">// ***** 步骤 4: 拼接 Authorization *****</span>
<span class="hljs-built_in">string</span> authorization = algorithm + <span class="hljs-string">&quot;&quot;</span>
+ <span class="hljs-string">&quot;Credential=&quot;</span> + secretid + <span class="hljs-string">&quot;/&quot;</span> + credentialScope + <span class="hljs-string">&quot;,&quot;</span>
+ <span class="hljs-string">&quot;SignedHeaders=&quot;</span> + signedHeaders
+ <span class="hljs-string">&quot;,&quot;</span>
+ <span class="hljs-string">&quot;Signature=&quot;</span> + signature;
Console.WriteLine(authorization);

Dictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>> headers = <span class="hljs-keyword">new</span> Dictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>>();
headers.Add(<span class="hljs-string">&quot;Authorization&quot;</span>, authorization);
headers.Add(<span class="hljs-string">&quot;Host&quot;</span>, endpoint);
headers.Add(<span class="hljs-string">&quot;Content-Type&quot;</span>, contentType + <span class="hljs-string">&quot;; charset=utf-8&quot;</span>);
headers.Add(<span class="hljs-string">&quot;X-TC-Timestamp&quot;</span>, requestTimestamp.ToString());
headers.Add(<span class="hljs-string">&quot;X-TC-Version&quot;</span>, version);
headers.Add(<span class="hljs-string">&quot;X-TC-Action&quot;</span>, action);
headers.Add(<span class="hljs-string">&quot;X-TC-Region&quot;</span>, region);
<span class="hljs-keyword">return</span> headers;

```

```

}
<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> <span class="hljs-keyword">void</span> <span class="hljs-title">Main</span>(<span class="hljs-params"><span class="hljs-built_in">string</span>[] args</span></span>
{
<span class="hljs-comment">// 密钥参数</span>
<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID*****</span>
<span class="hljs-built_in">string</span> SECRET_ID = Environment.GetEnvironmentVariable(<span class="hljs-string">&quot;TENCENTCLOUD_SECRET_ID&quot;</span>);
<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 *****</span>
<span class="hljs-built_in">string</span> SECRET_KEY = Environment.GetEnvironmentVariable(<span class="hljs-string">&quot;TENCENTCLOUD_SECRET_KEY&quot;</span>);

<span class="hljs-built_in">string</span> service = <span class="hljs-string">&quot;cvm&quot;</span>;
<span class="hljs-built_in">string</span> endpoint = <span class="hljs-string">&quot;cvm.tencentcloudapi.com&quot;</span>;
<span class="hljs-built_in">string</span> region = <span class="hljs-string">&quot;ap-guangzhou&quot;</span>;
<span class="hljs-built_in">string</span> action = <span class="hljs-string">&quot;DescribeInstances&quot;</span>;
<span class="hljs-built_in">string</span> version = <span class="hljs-string">&quot;2017-03-12&quot;</span>;

<span class="hljs-comment">// 此处由于示例规范的原因, 采用时间戳2019-02-26 00:44:25, 此参数作为示例, 如果在项目中, 您应当使用: </span>
<span class="hljs-comment">// DateTime date = DateTime.UtcNow;</span>
<span class="hljs-comment">// 注意时区, 建议此时间统一采用UTC时间戳, 否则容易出错</span>
DateTime date = <span class="hljs-keyword">new</span> DateTime(<span class="hljs-number">1970</span>, <span class="hljs-number">1</span>, <span class="hljs-number">1</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">0</span>, <span class="hljs-number">1551113065</span>);
<span class="hljs-built_in">string</span> requestPayload = <span class="hljs-string">&quot;{\&quot;Limit\&quot;: 1, \&quot;Filters\&quot;: [{\&quot;Values\&quot;: [\&quot;\u672a\u547d\u540d\&quot;], \&quot;Name\&quot;: \&quot;instance-name\&quot;}]}&quot;</span>;

Dictionary<&lt;span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>&gt;> headers = BuildHeaders(SECRET_ID, SECRET_KEY, service

```

```

, endpoint, region, action, version, date, requestPayload);

Console.WriteLine("<span class="hljs-string">&quot;POST https://cvm.tencentclo
udapi.com&quot;</span>");
<span class="hljs-keyword">foreach</span> (KeyValuePair<<span class="hljs-
built_in">string</span>, <span class="hljs-built_in">string</span>> kv <span
class="hljs-keyword">in</span> headers)
{
Console.WriteLine(kv.Key + <span class="hljs-string">&quot;;: &quot;</span> +
kv.Value);
}
Console.WriteLine();
Console.WriteLine(requestPayload);
}
}

```

NodeJS

```

const crypto = require('crypto');

function sha256(message, secret = '', encoding) {
const hmac = crypto.createHmac('sha256', secret)
return hmac.update(message).digest(encoding)
}

function getHash(message, encoding = 'hex') {
const hash = crypto.createHash('sha256')
return hash.update(message).digest(encoding)
}

function getDate(timestamp) {
const date = new Date(timestamp * 1000)
const year = date.getUTCFullYear()
const month = ('0' + (date.getUTCMonth() + 1)).slice(-2)
const day = ('0' + date.getUTCDate()).slice(-2)
return <span class="hljs-subst">${year}</span>-<span class="hljs-subst">${month}
</span>-<span class="hljs-subst">${day}</span>
}

function main(){
// 密钥参数
// 需要设置环境变量 TencentCloud_Secret_Id, 值为示例的 AKID****

```

```
const SECRET_ID = process.env.TENCENTCLOUD_SECRET_ID
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
const SECRET_KEY = process.env.TENCENTCLOUD_SECRET_KEY

<span class="hljs-keyword">const</span> endpoint = <span class="hljs-string">
'cvm.tencentcloudapi.com'</span>
<span class="hljs-keyword">const</span> service = <span class="hljs-string">
'cvm'</span>
<span class="hljs-keyword">const</span> region = <span class="hljs-string">
'ap-guangzhou'</span>
<span class="hljs-keyword">const</span> action = <span class="hljs-string">
'DescribeInstances'</span>
<span class="hljs-keyword">const</span> version = <span class="hljs-string">
'2017-03-12'</span>
<span class="hljs-comment">//const timestamp = getTime()</span>
<span class="hljs-keyword">const</span> timestamp = <span class="hljs-number">
1551113065</span>
<span class="hljs-comment">//时间处理, 获取世界时间日期</span>
<span class="hljs-keyword">const</span> date = getDate(timestamp)

<span class="hljs-comment">// ***** 步骤 1: 拼接规范请求串 *****</span>
<span class="hljs-keyword">const</span> payload = <span class="hljs-string">
'{"Limit": 1, "Filters": [{"Values":
["\u672a\u547d\u540d"], "Name": "instance-na
me"}]}</span>

<span class="hljs-keyword">const</span> hashedRequestPayload = getHash(payload);
<span class="hljs-keyword">const</span> httpRequestMethod = <span class="hljs-string">
'POST'</span>
<span class="hljs-keyword">const</span> canonicalUri = <span class="hljs-string">
'/</span>
<span class="hljs-keyword">const</span> canonicalQueryString = <span class="hljs-string">
'</span>
<span class="hljs-keyword">const</span> canonicalHeaders = <span class="hljs-string">
'content-type:application/json; charset=utf-8</span>
+ <span class="hljs-string">
'host:</span> + endpoint + <span class="hljs-string">
'\n</span>
+ <span class="hljs-string">
'x-tc-action:</span> + action.toLowerCase() + <span class="hljs-string">
'\n</span>
<span class="hljs-keyword">const</span> signedHeaders = <span class="hljs-string">
'content-type;host;x-tc-action</span>

<span class="hljs-keyword">const</span> canonicalRequest = httpRequestMethod
+ <span class="hljs-string">
'\n</span>
```

```

+ canonicalUri + <span class="hljs-string">&quot;\n&quot;</span>
+ canonicalQueryString + <span class="hljs-string">&quot;\n&quot;</span>
+ canonicalHeaders + <span class="hljs-string">&quot;\n&quot;</span>
+ signedHeaders + <span class="hljs-string">&quot;\n&quot;</span>
+ hashedRequestPayload
<span class="hljs-built_in">console</span>.log(canonicalRequest)

<span class="hljs-comment">// ***** 步骤 2: 拼接待签名字符串 *****
*</span>
<span class="hljs-keyword">const</span> algorithm = <span class="hljs-string">&quot;TC3-HMAC-SHA256&quot;</span>
<span class="hljs-keyword">const</span> hashedCanonicalRequest = getHash(canonicalRequest);
<span class="hljs-keyword">const</span> credentialScope = date + <span class="hljs-string">&quot;/&quot;</span> + service + <span class="hljs-string">&quot;/&quot;</span> + <span class="hljs-string">&quot;tc3_request&quot;</span>
<span class="hljs-keyword">const</span> stringToSign = algorithm + <span class="hljs-string">&quot;\n&quot;</span> +
timestamp + <span class="hljs-string">&quot;\n&quot;</span> +
credentialScope + <span class="hljs-string">&quot;\n&quot;</span> +
hashedCanonicalRequest
<span class="hljs-built_in">console</span>.log(stringToSign)

<span class="hljs-comment">// ***** 步骤 3: 计算签名 *****</span>
<span class="hljs-keyword">const</span> kDate = sha256(date, <span class="hljs-string">&#x27;TC3&#x27;</span> + SECRET_KEY)
<span class="hljs-keyword">const</span> kService = sha256(service, kDate)
<span class="hljs-keyword">const</span> kSigning = sha256(<span class="hljs-string">&#x27;tc3_request&#x27;</span>, kService)
<span class="hljs-keyword">const</span> signature = sha256(stringToSign, kSigning, <span class="hljs-string">&#x27;hex&#x27;</span>)
<span class="hljs-built_in">console</span>.log(signature)

<span class="hljs-comment">// ***** 步骤 4: 拼接 Authorization *****
*****</span>
<span class="hljs-keyword">const</span> authorization = algorithm + <span class="hljs-string">&quot; &quot;</span> +
<span class="hljs-string">&quot;Credential=&quot;</span> + SECRET_ID + <span class="hljs-string">&quot;/&quot;</span> + credentialScope + <span class="hljs-string">&quot;,&quot;</span> +
<span class="hljs-string">&quot;SignedHeaders=&quot;</span> + signedHeaders +
<span class="hljs-string">&quot;,&quot;</span> +
<span class="hljs-string">&quot;Signature=&quot;</span> + signature
<span class="hljs-built_in">console</span>.log(authorization)

<span class="hljs-keyword">const</span> curlcmd = <span class="hljs-string">&quot;&quot;</span>

```

```

#x27;curl -X POST &#x27;</span> + <span class="hljs-string">&quot;https://&qu
ot;</span> + endpoint
+ <span class="hljs-string">&#x27; -H &quot;Authorization: &#x27;</span> + au
thorization + <span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;Content-Type: application/json; c
harset=utf-8&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;Host: &#x27;</span> + endpoint +
<span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;X-TC-Action: &#x27;</span> + acti
on + <span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;X-TC-Timestamp: &#x27;</span> + t
imestamp.toString() + <span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;X-TC-Version: &#x27;</span> + ver
sion + <span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&#x27; -H &quot;X-TC-Region: &#x27;</span> + regi
on + <span class="hljs-string">&#x27;&quot;&#x27;</span>
+ <span class="hljs-string">&quot; -d &#x27;&quot;</span> + payload + <span c
lass="hljs-string">&quot;&#x27;&quot;</span>
<span class="hljs-built_in">console</span>.log(curlcmd)

}
main()

```

C++

```

#include <algorithm>
#include <cstdlib>
#include <iostream>
#include <iomanip>
#include <sstream>
#include <string>
#include <stdio.h>
#include <time.h>
#include <openssl/sha.h>
#include <openssl/hmac.h>

using namespace std;

string get_data(int64_t &timestamp)
{
    string utcDate;
    char buff[20] = {0};
    // time_t timenow;
    struct tm sttime;
    sttime = *gmtime(&timestamp);

```

```
strftime(buff, sizeof(buff), "%Y-%m-%d", &stime);
utcDate = string(buff);
return utcDate;
}

string int2str(int64_t n)
{
    std::stringstream ss;
    ss << n;
    return ss.str();
}

string sha256Hex(const string &str)
{
    char buf[3];
    unsigned char hash[SHA256_DIGEST_LENGTH];
    SHA256_CTX sha256;
    SHA256_Init(&sha256);
    SHA256_Update(&sha256, str.c_str(), str.size());
    SHA256_Final(hash, &sha256);
    std::string NewString = "";
    for(int i = 0; i < SHA256_DIGEST_LENGTH; i++)
    {
        snprintf(buf, sizeof(buf), "%02x", hash[i]);
        NewString = NewString + buf;
    }
    return NewString;
}

string HmacSha256(const string &key, const string &input)
{
    unsigned char hash[32];

    HMAC_CTX *h;

    #if OPENSSSL_VERSION_NUMBER < 0x10100000L
    HMAC_CTX hmac;
    HMAC_CTX_init(&hmac);
    h = &hmac;
    #else
    h = HMAC_CTX_new();
    #endif
```

```
<span class="hljs-built_in">HMAC_Init_ex</span>(h, &key[<span class="hljs-number">0</span>], key.<span class="hljs-built_in">length</span>(), <span class="hljs-built_in">EVP_sha256</span>(), <span class="hljs-literal">NULL</span>
);
<span class="hljs-built_in">HMAC_Update</span>(h, ( <span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</span>* )&input[<span class="hljs-number">0</span>], input.<span class="hljs-built_in">length</span>
());
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">int</span>
an> len = <span class="hljs-number">32</span>;
<span class="hljs-built_in">HMAC_Final</span>(h, hash, &len);

<span class="hljs-keyword">#if</span> OPENSSL_VERSION_NUMBER < 0x10100000L
HMAC_CTX_cleanup(h);
<span class="hljs-keyword">#else</span>
HMAC_CTX_free(h);
<span class="hljs-keyword">#endif</span>

std::stringstream ss;
ss &&& std:::<span class="hljs-built_in">setfill</span>(<span class="hljs-string">&#x27;0&#x27;</span>);
<span class="hljs-keyword">for</span> (<span class="hljs-keyword">int</span>
i = <span class="hljs-number">0</span>; i &lt; len; i++)
{
ss &&& hash[i];
}

<span class="hljs-keyword">return</span> (ss.<span class="hljs-built_in">str</span>
);
}

string HexEncode(const string &input)
{
static const char* const lut = "0123456789abcdef";
size_t len = input.length();

string output;
output.<span class="hljs-built_in">reserve</span>(<span class="hljs-number">2</span>
* len);
<span class="hljs-keyword">for</span> (<span class="hljs-keyword">size_t</span>
i = <span class="hljs-number">0</span>; i &lt; len; ++i)
{
```

```

<span class="hljs-keyword">const</span> <span class="hljs-keyword">unsigned</span>
<span class="hljs-keyword">char</span> c = input[i];
output.<span class="hljs-built_in">push_back</span>(lut[c >> <span class="hljs-number">4</span>]);
output.<span class="hljs-built_in">push_back</span>(lut[c & <span class="hljs-number">15</span>]);
}
<span class="hljs-keyword">return</span> output;

}

int main()
{
// 密钥参数
// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
string SECRET_ID = getenv("TENCENTCLOUD_SECRET_ID");
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
string SECRET_KEY = getenv("TENCENTCLOUD_SECRET_KEY");

string service = <span class="hljs-string">"&quot;cvm&quot;</span>;
string host = <span class="hljs-string">"&quot;cvm.tencentcloudapi.com&quot;</span>;
string region = <span class="hljs-string">"&quot;ap-guangzhou&quot;</span>;
string action = <span class="hljs-string">"&quot;DescribeInstances&quot;</span>;
>;
string version = <span class="hljs-string">"&quot;2017-03-12&quot;</span>;
<span class="hljs-keyword">int64_t</span> timestamp = <span class="hljs-number">1551113065</span>;
string date = <span class="hljs-built_in">get_data</span>(timestamp);

<span class="hljs-comment">// ***** 步骤 1: 拼接规范请求串 *****</span>
<span class="hljs-comment"></span>
string httpRequestMethod = <span class="hljs-string">"&quot;POST&quot;</span>;
string canonicalUri = <span class="hljs-string">"&quot;/&quot;</span>;
string canonicalQueryString = <span class="hljs-string">"&quot;&quot;</span>;
string lower = action;
std::<span class="hljs-built_in">transform</span>(action.<span class="hljs-built_in">begin</span>(), action.<span class="hljs-built_in">end</span>(), lower.<span class="hljs-built_in">begin</span>(), ::tolower);
string canonicalHeaders = <span class="hljs-built_in">string</span>( <span class="hljs-string">"&quot;content-type:application/json; charset=utf-8\n&quot;</span>
+ <span class="hljs-string">"&quot;host:&quot;</span> + host + <span class="hljs-string">"\n&quot;</span>;
+ <span class="hljs-string">"&quot;x-tc-action:&quot;</span> + lower + <span class="hljs-string">"&quot;\n&quot;</span>;

```

```

string signedHeaders = <span class="hljs-string">&quot;;content-type;host;x-tc
-action&quot;;</span>;
string payload = <span class="hljs-string">&quot;;{\&quot;;Limit\&quot;;: 1, \&
quot;;Filters\&quot;;: [{\&quot;;Values\&quot;;: [\&quot;;\\u672a\\u547d\\u540d\&qu
ot;;], \&quot;;Name\&quot;;: \&quot;;instance-name\&quot;;;}}&quot;;</span>;
string hashedRequestPayload = <span class="hljs-built_in">sha256Hex</span>(pa
yload);
string canonicalRequest = httpRequestMethod + <span class="hljs-string">&quo
t;;\n&quot;;</span>
+ canonicalUri + <span class="hljs-string">&quot;;\n&quot;;</span>
+ canonicalQueryString + <span class="hljs-string">&quot;;\n&quot;;</span>
+ canonicalHeaders + <span class="hljs-string">&quot;;\n&quot;;</span>
+ signedHeaders + <span class="hljs-string">&quot;;\n&quot;;</span>
+ hashedRequestPayload;
cout &lt;&lt;&lt; canonicalRequest &lt;&lt;&lt; endl;

<span class="hljs-comment">// ***** 步骤 2: 拼接待签名字符串 *****
*</span>
string algorithm = <span class="hljs-string">&quot;;TC3-HMAC-SHA256&quot;;</spa
n>;
string RequestTimestamp = <span class="hljs-built_in">int2str</span>(timestam
p);
string credentialScope = date + <span class="hljs-string">&quot;;/&quot;;</span>
+ service + <span class="hljs-string">&quot;;/&quot;;</span> + <span class="h
ljs-string">&quot;;tc3_request&quot;;</span>;
string hashedCanonicalRequest = <span class="hljs-built_in">sha256Hex</span>
(canonicalRequest);
string stringToSign = algorithm + <span class="hljs-string">&quot;;\n&quot;;</s
pan> + RequestTimestamp + <span class="hljs-string">&quot;;\n&quot;;</span> + c
redentialScope + <span class="hljs-string">&quot;;\n&quot;;</span> + hashedCano
nicalRequest;
cout &lt;&lt;&lt; stringToSign &lt;&lt;&lt; endl;

<span class="hljs-comment">// ***** 步骤 3: 计算签名 *****</s
pan>
string kKey = <span class="hljs-string">&quot;;TC3&quot;;</span> + SECRET_KEY;
string kDate = <span class="hljs-built_in">HmacSha256</span>(kKey, date);
string kService = <span class="hljs-built_in">HmacSha256</span>(kDate, servic
e);
string kSigning = <span class="hljs-built_in">HmacSha256</span>(kService, <sp
an class="hljs-string">&quot;;tc3_request&quot;;</span>);
string signature = <span class="hljs-built_in">HexEncode</span>(<span class
="hljs-built_in">HmacSha256</span>(kSigning, stringToSign));
cout &lt;&lt;&lt; signature &lt;&lt;&lt; endl;

<span class="hljs-comment">// ***** 步骤 4: 拼接 Authorization *****
*****</span>

```

```

string authorization = algorithm + <span class="hljs-string">&quot; &quot;</span> + <span class="hljs-string">&quot;Credential=&quot;</span> + SECRET_ID + <span class="hljs-string">&quot;/&quot;</span> + credentialScope + <span class="hljs-string">&quot;; &quot;</span> + <span class="hljs-string">&quot;SignedHeaders=&quot;</span> + signedHeaders + <span class="hljs-string">&quot;; &quot;</span> + <span class="hljs-string">&quot;Signature=&quot;</span> + signature;
cout &lt;&lt; authorization &lt;&lt; endl;

string curlcmd = <span class="hljs-string">&quot;curl -X POST https://&quot;</span> + host + <span class="hljs-string">&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;Authorization: &quot;</span> + authorization + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;Content-Type: application/json; charset=utf-8&quot;&quot;</span> + <span class="hljs-string">&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;Host: &quot;</span> + host + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;X-TC-Action: &quot;</span> + action + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;X-TC-Timestamp: &quot;</span> + RequestTimestamp + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;X-TC-Version: &quot;</span> + version + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -H \&quot;X-TC-Region: &quot;</span> + region + <span class="hljs-string">&quot;\&quot;\n&quot;</span> + <span class="hljs-string">&quot; -d &#x27;&quot;</span> + payload + <span class="hljs-string">&quot;\&#x27;&quot;</span>;
cout &lt;&lt; curlcmd &lt;&lt; endl;
<span class="hljs-keyword">return</span> <span class="hljs-number">0</span>;
};

```

C

```

#include <ctype.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#include <time.h>
#include <stdint.h>
#include <openssl/sha.h>
#include <openssl/hmac.h>

void get_utc_date(int64_t timestamp, char* utc, int len)
{

```

```
// time_t timenow;
struct tm sttime;
sttime = *gmtime(&timestamp);
strftime(utc, len, "%Y-%m-%d", &sttime);
}

void sha256_hex(const char* str, char* result)
{
char buf[3];
unsigned char hash[SHA256_DIGEST_LENGTH];
SHA256_CTX sha256;
SHA256_Init(&sha256);
SHA256_Update(&sha256, str, strlen(str));
SHA256_Final(hash, &sha256);
for(int i = 0; i < SHA256_DIGEST_LENGTH; i++)
{
snprintf(buf, sizeof(buf), "%02x", hash[i]);
strcat(result, buf);
}
}

void hmac_sha256(const char* key, int key_len,
const char* input, int input_len,
unsigned char* output, unsigned int* output_len)
{
HMAC_CTX *h;
#if OPENSSSL_VERSION_NUMBER < 0x10100000L
HMAC_CTX hmac;
HMAC_CTX_init(&hmac);
h = &hmac;
#else
h = HMAC_CTX_new();
#endif

HMAC_Init_ex(h, key, key_len, EVP_sha256(), <span class="hljs-literal">NULL</span>);
HMAC_Update(h, ( <span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</span>* )input, input_len);
HMAC_Final(h, output, output_len);

#if OPENSSSL_VERSION_NUMBER < 0x10100000L
HMAC_CTX_cleanup(h);
#else
HMAC_CTX_free(h);
#endif
}
```

```
}

void hex_encode(const char* input, int input_len, char* output)
{
    static const char* const lut = "0123456789abcdef";

    char add_out[128];
    char temp[2];
    for (size_t i = 0; i < input_len; ++i)
    {
        const unsigned char c = input[i];
        temp[0] = lut[c >> 4];
        strcat(add_out, temp);
        temp[0] = lut[c & 15];
        strcat(add_out, temp);
    }
    strncpy(output, add_out, 128);
}

void lowercase(const char * src, char * dst)
{
    for (int i = 0; src[i]; i++)
    {
        dst[i] = tolower(src[i]);
    }
}

int main()
{
    // 密钥参数
    // 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
    const char* SECRET_ID = getenv("TENCENTCLOUD_SECRET_ID");
    // 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
    const char* SECRET_KEY = getenv("TENCENTCLOUD_SECRET_KEY");
    const char* service = "cvm";
}
```

```

const char* host = "cvm.tencentcloudapi.com";
const char* region = "ap-guangzhou";
const char* action = "DescribeInstances";
const char* version = "2017-03-12";
int64_t timestamp = 1551113065;
char date[20] = {0};
get_utc_date(timestamp, date, sizeof(date));

```

```

<span class="hljs-comment">// ***** 步骤 1: 拼接规范请求串 *****</span>
</span>
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* http_request_method = <span class="hljs-string">&quot;POST&quot;</span>;
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* canonical_uri = <span class="hljs-string">&quot;/&quot;</span>;
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* canonical_query_string = <span class="hljs-string">&quot;&quot;</span>;
<span class="hljs-keyword">char</span> canonical_headers[<span class="hljs-number">100</span>] = {<span class="hljs-string">&quot;content-type:applicatio
n/json; charset=utf-8\nhost:&quot;</span>;
<span class="hljs-built_in">strcat</span>(canonical_headers, host);
<span class="hljs-built_in">strcat</span>(canonical_headers, <span class="hljs-string">&quot;\n-x-tc-action:&quot;</span>;
<span class="hljs-keyword">char</span> value[<span class="hljs-number">100</span>] = {<span class="hljs-number">0</span>};
lowercase(action, value);
<span class="hljs-built_in">strcat</span>(canonical_headers, value);
<span class="hljs-built_in">strcat</span>(canonical_headers, <span class="hljs-string">&quot;\n&quot;</span>;
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* signed_headers = <span class="hljs-string">&quot;content-type;host;x-tc-ac
tion&quot;</span>;
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* payload = <span class="hljs-string">&quot;{\&quot;Limit&quot;: 1, \&quot;
Filters&quot;: [{\&quot;Values&quot;: [\&quot;\u672a\u547d\u540d&quo
t;], \&quot;Name&quot;: \&quot;instance-name&quot;}}]&quot;</span>;
<span class="hljs-keyword">char</span> hashed_request_payload[<span class="hljs-number">100</span>] = {<span class="hljs-number">0</span>};
sha256_hex(payload, hashed_request_payload);

<span class="hljs-keyword">char</span> canonical_request[<span class="hljs-number">256</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(canonical_request, <span class="hljs-string">&quot;%s\n%s\n%s\n%s\n%s\n%s&quot;</span>, http_request_method,
canonical_uri, canonical_query_string, canonical_headers,
signed_headers, hashed_request_payload);
<span class="hljs-built_in">printf</span>(<span class="hljs-string">&quot;%s

```

```
\n&quot;;</span>, canonical_request);

<span class="hljs-comment">// ***** 步骤 2: 拼接待签名字符串 *****
*</span>
<span class="hljs-keyword">const</span> <span class="hljs-keyword">char</span>
>* algorithm = <span class="hljs-string">&quot;TC3-HMAC-SHA256&quot;;</span>;
<span class="hljs-keyword">char</span> request_timestamp[<span class="hljs-number">16</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(request_timestamp, <span class="hljs-string">&quot;%d&quot;;</span>, timestamp);
<span class="hljs-keyword">char</span> credential_scope[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">strcat</span>(credential_scope, date);
<span class="hljs-built_in">sprintf</span>(credential_scope, <span class="hljs-string">&quot;%s/%s/tc3_request&quot;;</span>, date, service);
<span class="hljs-keyword">char</span> hashed_canonical_request[<span class="hljs-number">100</span>] = {<span class="hljs-number">0</span>};
sha256_hex(canonical_request, hashed_canonical_request);
<span class="hljs-keyword">char</span> string_to_sign[<span class="hljs-number">256</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(string_to_sign, <span class="hljs-string">&quot;%s\n%s\n%s\n%s&quot;;</span>, algorithm, request_timestamp,
credential_scope, hashed_canonical_request);
<span class="hljs-built_in">printf</span>(<span class="hljs-string">&quot;%s
\n&quot;;</span>, string_to_sign);

<span class="hljs-comment">// ***** 步骤 3: 计算签名 *****</s
pan>
<span class="hljs-keyword">char</span> k_key[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(k_key, <span class="hljs-string">&quot;%s&quot;;</span>, <span class="hljs-string">&quot;TC3&quot;;</span>, SEC
RET_KEY);
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</s
pan> k_date[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">int</sp
an> output_len = <span class="hljs-number">0</span>;
hmac_sha256(k_key, <span class="hljs-built_in">strlen</span>(k_key), date, <s
pan class="hljs-built_in">strlen</span>(date), k_date, &output_len);
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</s
pan> k_service[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
hmac_sha256(k_date, output_len, service, <span class="hljs-built_in">strlen</
span>(service), k_service, &output_len);
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</s
```

```

pan> k_signing[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
hmac_sha256(k_service, output_len, <span class="hljs-string">&quot;tc3_request&quot;</span>, <span class="hljs-built_in">strlen</span>(<span class="hljs-string">&quot;tc3_request&quot;</span>), k_signing, &output_len);
<span class="hljs-keyword">unsigned</span> <span class="hljs-keyword">char</span>
pan> k_hmac_sha_sign[<span class="hljs-number">64</span>] = {<span class="hljs-number">0</span>};
hmac_sha256(k_signing, output_len, string_to_sign, <span class="hljs-built_in">strlen</span>(string_to_sign), k_hmac_sha_sign, &output_len);

<span class="hljs-keyword">char</span> signature[<span class="hljs-number">128</span>] = {<span class="hljs-number">0</span>};
hex_encode(k_hmac_sha_sign, output_len, signature);
<span class="hljs-built_in">printf</span>(<span class="hljs-string">&quot;%s\n&quot;</span>, signature);

<span class="hljs-comment">// ***** 步骤 4: 拼接 Authorization *****</span>
<span class="hljs-keyword">char</span> authorization[<span class="hljs-number">512</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(authorization, <span class="hljs-string">&quot;%s Credential=%s/%s, SignedHeaders=%s, Signature=%s&quot;</span>
>,
algorithm, SECRET_ID, credential_scope, signed_headers, signature);
<span class="hljs-built_in">printf</span>(<span class="hljs-string">&quot;%s\n&quot;</span>, authorization);

<span class="hljs-keyword">char</span> curlcmd[<span class="hljs-number">10240</span>] = {<span class="hljs-number">0</span>};
<span class="hljs-built_in">sprintf</span>(curlcmd, <span class="hljs-string">&quot;curl -X POST https://%s\n \
-H \&quot;Authorization: %s&quot;\n \
-H \&quot;Content-Type: application/json; charset=utf-8&quot;\n \
-H \&quot;Host: %s&quot;\n \
-H \&quot;X-TC-Action: %s&quot;\n \
-H \&quot;X-TC-Timestamp: %s&quot;\n \
-H \&quot;X-TC-Version: %s&quot;\n \
-H \&quot;X-TC-Region: %s&quot;\n \
-d \&#x27;%s&#x27;&quot;</span>,
host, authorization, host, action, request_timestamp, version, region, payload);
<span class="hljs-built_in">printf</span>(<span class="hljs-string">&quot;%s\n&quot;</span>, curlcmd);
<span class="hljs-keyword">return</span> <span class="hljs-number">0</span>;

```

```
}
```

其他语言

- Lua: [GitHub](#)
- Swift: [GitHub](#)
- Dart: [GitHub](#)
- Shell(Bash): [GitHub](#)

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：2026-04-16 17:15:03

签名方法 v1 简单易用，但是功能和安全性都不如签名方法 v3，推荐使用签名方法 v3。

首次接触，建议使用 [API Explorer](#) 中的“签名串生成”功能，选择签名版本为“API 3.0 签名 v1”，可以生成签名过程进行验证，并提供了部分编程语言的签名示例，也可直接生成 SDK 代码。推荐使用腾讯云 API 配套的 7 种常见的编程语言 SDK，已经封装了签名和请求过程，均已开源，支持 [Python](#)、[Java](#)、[PHP](#)、[Go](#)、[NodeJS](#)、[.NET](#)、[C++](#)。

推荐使用 API Explorer

[点击调试](#)

您可以通过 API Explorer 的【签名串生成】模块查看每个接口签名的生成过程。

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【新建密钥】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。以下是使用签名方法 v1 生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKID*****
- SecretKey: *****

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	AKID*****
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
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

这里只展示了部分公共参数和接口输入参数，用户可以根据实际需要添加其他参数，例如 Language 和 Token 公共参数。

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' : 'AKID*****',
'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=AKID*****&Timestamp=1465
185768&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&L
imit=20&Nonce=11886&Offset=0&Region=ap-guangzhou&SecretId=AKID*****
*****&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 = '*****';


```

最终得到的签名串为：

```
7RAM2xfNMO9EiVTNmPg06MRnCvQ=
```

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 7RAM2xfNMO9EiVTNmPg06MRnCvQ=，最终得到的签名串请求参数（Signature）为：7RAM2xfNMO9EiVTNmPg06MRnCvQ%3D，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。当前支持的编程语言有：

- [Python](#)
- [Java](#)
- [PHP](#)
- [Go](#)
- [NodeJS](#)
- [.NET](#)
- [C++](#)

下面提供了不同产品的生成签名 demo，您可以找到对应的产品参考签名的生成：

- [Signature Demo](#)

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=AKID*****&Signature=7RAM2xfNM09EiVTNmPg`

`06MRnCvQ%3D&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，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";

    <span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> String <span class="hljs-title">sign</span><span class="hljs-params">(String s, String key, String method)</span> <span class="hljs-keyword">throws</span> Exception </span>{
    Mac mac = Mac.getInstance(method);
    SecretKeySpec secretKeySpec = <span class="hljs-keyword">new</span> SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
    mac.init(secretKeySpec);
    <span class="hljs-keyword">byte</span>[] hash = mac.doFinal(s.getBytes(CHARSET));
    <span class="hljs-keyword">return</span> DatatypeConverter.printBase64Binary(hash);
    }

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

```

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> String <span class="hljs-title">getUrl</span>
<span class="hljs-params">(TreeMap<String, Object> params)</span> <span class="hljs-keyword">throws</span> UnsupportedOperationException </span>{
String url = <span class="hljs-keyword">new</span> StringBuilder(<span class="hljs-string">&quot;https://cvm.tencentcloudapi.com/?&quot;</span>);
<span class="hljs-comment">// 实际请求的url中对参数顺序没有要求</span>
<span class="hljs-keyword">for</span> (String k : params.keySet()) {
<span class="hljs-comment">// 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</span>
url.append(k).append(<span class="hljs-string">&quot;=&quot;</span>).append(URLEncoder.encode(params.get(k).toString(), CHARSET)).append(<span class="hljs-string">&quot;&quot;</span>);
}
<span class="hljs-keyword">return</span> url.toString().substring(<span class="hljs-number">0</span>, url.length() - <span class="hljs-number">1</span>);
}

```

```

<span class="hljs-function"><span class="hljs-keyword">public</span> <span class="hljs-keyword">static</span> <span class="hljs-keyword">void</span> <span class="hljs-title">main</span><span class="hljs-params">(String[] args)</span>
<span class="hljs-keyword">throws</span> Exception </span>{
TreeMap<String, Object> params = <span class="hljs-keyword">new</span> TreeMap<String, Object>(); <span class="hljs-comment">// TreeMap可以自动排序</span>
<span class="hljs-comment">// 实际调用时应当使用随机数, 例如: params.put(&quot;Nonce&quot;, new Random().nextInt(java.lang.Integer.MAX_VALUE));</span>
params.put(<span class="hljs-string">&quot;Nonce&quot;</span>, <span class="hljs-number">11886</span>); <span class="hljs-comment">// 公共参数</span>
<span class="hljs-comment">// 实际调用时应当使用系统当前时间, 例如: params.put(&quot;Timestamp&quot;, System.currentTimeMillis() / 1000);</span>
params.put(<span class="hljs-string">&quot;Timestamp&quot;</span>, <span class="hljs-number">1465185768</span>); <span class="hljs-comment">// 公共参数</span>
<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的
AKID*****</span>
params.put(<span class="hljs-string">&quot;SecretId&quot;</span>, System.getenv(<span class="hljs-string">&quot;TENCENTCLOUD_SECRET_ID&quot;</span>)); <span class="hljs-comment">// 公共参数</span>
params.put(<span class="hljs-string">&quot;Action&quot;</span>, <span class="hljs-string">&quot;DescribeInstances&quot;</span>); <span class="hljs-comment">// 公共参数</span>
params.put(<span class="hljs-string">&quot;Version&quot;</span>, <span class="hljs-string">&quot;2017-03-12&quot;</span>); <span class="hljs-comment">// 公共参数</span>
params.put(<span class="hljs-string">&quot;Region&quot;</span>, <span class="hljs-string">&quot;</span>

```

```

=> <span class="hljs-string">&quot;ap-guangzhou&quot;</span>); <span class="hljs-comment"
t">// 公共参数</span>
params.put(<span class="hljs-string">&quot;Limit&quot;</span>, <span class="hljs-number"
ljs-number">20</span>); <span class="hljs-comment">// 业务参数</span>
params.put(<span class="hljs-string">&quot;Offset&quot;</span>, <span class="hljs-number"
="hljs-number">0</span>); <span class="hljs-comment">// 业务参数</span>
params.put(<span class="hljs-string">&quot;InstanceIds.0&quot;</span>, <span class="hljs-string"
class="hljs-string">&quot;ins-09dx96dg&quot;</span>); <span class="hljs-comment"
nt">// 业务参数</span>
<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的
*****</span>
params.put(<span class="hljs-string">&quot;Signature&quot;</span>, sign(getSt
tringToSign(params), System.getenv(<span class="hljs-string">&quot;TENCENTCLOU
D_SECRET_KEY&quot;</span>), <span class="hljs-string">&quot;HmacSHA1&quot;</s
pan>)); <span class="hljs-comment">// 公共参数</span>
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 os
import time

import requests

# 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
secret_id = os.environ.get("TENCENTCLOUD_SECRET_ID")
# 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
secret_key = os.environ.get("TENCENTCLOUD_SECRET_KEY")

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)
```

Golang

```
package main

import (
    "bytes"
    "crypto/hmac"
    "crypto/sha1"
    "encoding/base64"
    "fmt"
    "os"
    "sort"
    "strconv"
)

func main() {
    // 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
    secretId := os.Getenv("TENCENTCLOUD_SECRET_ID")
    // 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
    secretKey := os.Getenv("TENCENTCLOUD_SECRET_KEY")
```

```
params := map[string]string{
    "Nonce": "11886",
    "Timestamp": strconv.Itoa(1465185768),
    "Region": "ap-guangzhou",
    "SecretId": secretId,
    "Version": "2017-03-12",
    "Action": "DescribeInstances",
    "InstanceIds.0": "ins-09dx96dg",
    "Limit": strconv.Itoa(20),
    "Offset": strconv.Itoa(0),
}

<span class="hljs-keyword">var</span> buf bytes.Buffer
buf.WriteString(<span class="hljs-string">&quot;GET&quot;</span>)
buf.WriteString(<span class="hljs-string">&quot;cvm.tencentcloudapi.com&quot;</span>
</span>)
buf.WriteString(<span class="hljs-string">&quot;/&quot;</span>)
buf.WriteString(<span class="hljs-string">&quot;?&quot;</span>)

<span class="hljs-comment">// sort keys by ascii asc order</span>
keys := <span class="hljs-built_in">make</span> ([]<span class="hljs-keyword">string</span>, <span class="hljs-number">0</span>, <span class="hljs-built_in">len</span>(params))
<span class="hljs-keyword">for</span> k, _ := <span class="hljs-keyword">range</span> params {
    keys = <span class="hljs-built_in">append</span>(keys, k)
}
sort.Strings(keys)

<span class="hljs-keyword">for</span> i := <span class="hljs-keyword">range</span> keys {
    k := keys[i]
    buf.WriteString(k)
    buf.WriteString(<span class="hljs-string">&quot;=&quot;</span>)
    buf.WriteString(params[k])
    buf.WriteString(<span class="hljs-string">&quot;&quot;</span>)
}
buf.Truncate(buf.Len() - <span class="hljs-number">1</span>)

hashed := hmac.New(sha1.New, []<span class="hljs-keyword">byte</span>(secretKey))
hashed.Write(buf.Bytes())

fmt.Println(base64.StdEncoding.EncodeToString(hashed.Sum(<span class="hljs-literal">nil</span>)))
```

```
}
```

PHP

```
<?php
// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID*****
*****
$secretId = getenv("TENCENTCLOUD_SECRET_ID");
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 *****
***
$secretKey = getenv("TENCENTCLOUD_SECRET_KEY");
$params["Nonce"] = 11886;//rand();
$params["Timestamp"] = 1465185768;//time();
$params["Region"] = "ap-guangzhou";
$params["SecretId"] = $secretId;
$params["Version"] = "2017-03-12";
$params["Action"] = "DescribeInstances";
$params["InstanceIds.0"] = "ins-09dx96dg";
$params["Limit"] = 20;
$params["Offset"] = 0;

ksort($params);

$signStr = "GETcvm.tencentcloudapi.com/?";
foreach ( $params as $key => $value ) {
    $signStr = $signStr . $key . "=" . $value . "&";
}
$signStr = substr($signStr, 0, -1);

$signature = base64_encode(hash_hmac("sha1", $signStr, $secretKey, true));
echo $signature.PHP_EOL;
// need to install and enable curl extension in php.ini
// $params["Signature"] = $signature;
// $url = "https://cvm.tencentcloudapi.com/?".http_build_query($params);
// echo $url.PHP_EOL;
// $ch = curl_init();
// curl_setopt($ch, CURLOPT_URL, $url);
// $output = curl_exec($ch);
// curl_close($ch);
// echo json_decode($output);
```

Ruby

```
# -*- coding: UTF-8 -*-
# require ruby>=2.3.0
require 'time'
require 'openssl'
require 'base64'

# 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
secret_id = ENV["TENCENTCLOUD_SECRET_ID"]
# 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
secret_key = ENV["TENCENTCLOUD_SECRET_KEY"]

method = 'GET'
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, # Time.now.to_i
  'Version' => '2017-03-12',
}
sign = method + endpoint + '/?'
params = []
data.sort.each do |item|
  params << "#{item[0]}=#{item[1]}"
end
sign += params.join('&')
digest = OpenSSL::Digest.new('sha1')
data['Signature'] = Base64.encode64(OpenSSL::HMAC.digest(digest, secret_key, sign))
puts data['Signature']

# require 'net/http'
# uri = URI('https://' + endpoint)
# uri.query = URI.encode_www_form(data)
# p uri
# res = Net::HTTP.get_response(uri)
# puts res.body
```

DotNet

```

using System;
using System.Collections.Generic;
using System.Net;
using System.Security.Cryptography;
using System.Text;

public class Application {
public static string Sign(string signKey, string secret)
{
string signRet = string.Empty;
using (HMACSHA1 mac = new HMACSHA1(Encoding.UTF8.GetBytes(signKey)))
{
byte[] hash = mac.ComputeHash(Encoding.UTF8.GetBytes(secret));
signRet = Convert.ToBase64String(hash);
}
return signRet;
}
public static string MakeSignPlainText(SortedDictionary<string, string> requestPa
rams, string requestMethod, string requestHost, string requestPath)
{
string retStr = "";
retStr += requestMethod;
retStr += requestHost;
retStr += requestPath;
retStr += "?";
string v = "";
foreach (string key in requestParams.Keys)
{
v += string.Format("{0}={1}&", key, requestParams[key]);
}
retStr += v.TrimEnd('&');
return retStr;
}
}

```

```

<span class="hljs-function"><span class="hljs-keyword">public</span> <span cl
ass="hljs-keyword">static</span> <span class="hljs-keyword">void</span> <span
class="hljs-title">Main</span>(<span class="hljs-params"><span class="hljs-bu
ilt_in">string</span>[] args</span></span>
{
<span class="hljs-comment">// 密钥参数</span>
<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的
AKID*****</span>
<span class="hljs-built_in">string</span> SECRET_ID = Environment.GetEnvironm
entVariable(<span class="hljs-string">"TENCENTCLOUD_SECRET_ID"</span>);
}

```

```

<span class="hljs-comment">// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的
*****</span>
<span class="hljs-built_in">string</span> SECRET_KEY = Environment.GetEnvironmentVariable(<span class="hljs-string">&quot;TENCENTCLOUD_SECRET_KEY&quot;</span>);
</span>;

<span class="hljs-built_in">string</span> endpoint = <span class="hljs-string">&quot;cvm.tencentcloudapi.com&quot;</span>;
<span class="hljs-built_in">string</span> region = <span class="hljs-string">&quot;ap-guangzhou&quot;</span>;
<span class="hljs-built_in">string</span> action = <span class="hljs-string">&quot;DescribeInstances&quot;</span>;
<span class="hljs-built_in">string</span> version = <span class="hljs-string">&quot;2017-03-12&quot;</span>;
<span class="hljs-built_in">double</span> RequestTimestamp = <span class="hljs-number">1465185768</span>; <span class="hljs-comment">// 时间戳 2019-02-26 00:44:25, 此参数作为示例, 以实际为准</span>
<span class="hljs-comment">// long timestamp = ToTimestamp() / 1000;</span>
<span class="hljs-comment">// string requestTimestamp = timestamp.ToString();</span>
Dictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>> param = <span class="hljs-keyword">new</span> Dictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>> ();
param.Add(<span class="hljs-string">&quot;Limit&quot;</span>, <span class="hljs-string">&quot;20&quot;</span>);
param.Add(<span class="hljs-string">&quot;Offset&quot;</span>, <span class="hljs-string">&quot;0&quot;</span>);
param.Add(<span class="hljs-string">&quot;InstanceIds.0&quot;</span>, <span class="hljs-string">&quot;ins-09dx96dg&quot;</span>);
param.Add(<span class="hljs-string">&quot;Action&quot;</span>, action);
param.Add(<span class="hljs-string">&quot;Nonce&quot;</span>, <span class="hljs-string">&quot;11886&quot;</span>);
<span class="hljs-comment">// param.Add(&quot;Nonce&quot;, Math.Abs(new Random().Next()).ToString());</span>

param.Add(<span class="hljs-string">&quot;Timestamp&quot;</span>, RequestTimestamp.ToString());
param.Add(<span class="hljs-string">&quot;Version&quot;</span>, version);

param.Add(<span class="hljs-string">&quot;SecretId&quot;</span>, SECRET_ID);
param.Add(<span class="hljs-string">&quot;Region&quot;</span>, region);
SortedDictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>> headers = <span class="hljs-keyword">new</span> SortedDictionary<<span class="hljs-built_in">string</span>, <span class="hljs-built_in">string</span>>(param, StringComparer.Ordinal);
<span class="hljs-built_in">string</span> sigInParam = MakeSignPlainText(head

```

```

ers, <span class="hljs-string">&quot;GET&quot;</span>, endpoint, <span class
="hljs-string">&quot;/&quot;</span>);
<span class="hljs-built_in">string</span> sigOutParam = Sign(SECRET_KEY, sigI
nParam);
Console.WriteLine(sigOutParam);
}
}

```

NodeJS

```

const crypto = require('crypto');

function get_req_url(params, endpoint){
params['Signature'] = encodeURIComponent(params['Signature']);
const url_strParam = sort_params(params)
return "https://" + endpoint + "/" + url_strParam.slice(1);
}

function formatSignString(reqMethod, endpoint, path, strParam){
let strSign = reqMethod + endpoint + path + "?" + strParam.slice(1);
return strSign;
}

function sha1(secretKey, strsign){
let signMethodMap = {'HmacSHA1': "sha1"};
let hmac = crypto.createHmac(signMethodMap['HmacSHA1'], secretKey || "");
return hmac.update(Buffer.from(strsign, 'utf8')).digest('base64')
}

function sort_params(params) {
let strParam = "";
let keys = Object.keys(params);
keys.sort();
for (let k in keys) {
//k = k.replace(/_/g, '.');
strParam += ("%&" + keys[k] + "=" + params[keys[k]]);
}
return strParam
}

function main(){
// 密钥参数
// 需要设置环境变量 TENCENTCLOUD_SECRET_ID, 值为示例的 AKID****
const SECRET_ID = process.env.TENCENTCLOUD_SECRET_ID

```

```
// 需要设置环境变量 TENCENTCLOUD_SECRET_KEY, 值为示例的 ****
const SECRET_KEY = process.env.TENCENTCLOUD_SECRET_KEY

const endpoint = 'cvm.tencentcloudapi.com'
const Region = 'ap-guangzhou'
const Version = '2017-03-12'
const Action = 'DescribeInstances'
const Timestamp = 1465185768 // 时间戳 2016-06-06 12:02:48,
// 此参数作为示例, 以实际为准
const Timestamp = Math.round(Date.now() / 1000)

const Nonce = 11886 // 随机正整数
const nonce = Math.round(Math.random() * 65535)

let params = {}
params['Action'] = Action
params['InstanceIds.0'] = 'ins-09dx96dg'
params['Limit'] = 20
params['Offset'] = 0
params['Nonce'] = Nonce
params['Region'] = Region
params['SecretId'] = SECRET_ID
params['Timestamp'] = Timestamp
params['Version'] = Version

// 1. 对参数排序, 并拼接请求字符串
strParam = sort_params(params)

// 2. 拼接签名原字符串
const reqMethod = 'GET'
const path = '/'
strSign = formatSignString(reqMethod, endpoint, path, strParam)
// console.log(strSign)
```

```
<span class="hljs-comment">// 3. 生成签名串</span>
params[<span class="hljs-string">#x27;Signature#x27;</span>] = sha1(SECRET_
KEY, strSign)
<span class="hljs-built_in">console</span>.log(params[<span class="hljs-string">#x27;Signature#x27;</span>])

<span class="hljs-comment">// 4. 进行url编码并拼接请求url</span>
<span class="hljs-comment">// const req_url = get_req_url(params, endpoint)</
span>
<span class="hljs-comment">// console.log(params[&#x27;Signature#x27;])</spa
n>
<span class="hljs-comment">// console.log(req_url)</span>

}
main()
```

返回结果

最近更新时间：2026-04-16 17:15:45

云 API 3.0 接口默认返回 JSON 数据，返回非 JSON 格式的接口会在文档中做出说明。返回 JSON 数据时最大限制为 50 MB，如果返回的数据超过最大限制，请求会失败并返回内部错误。请根据接口文档中给出的过滤功能（例如时间范围）或者分页功能，控制返回数据不要过大。

注意：目前只要请求被服务端正常处理了，响应的 HTTP 状态码均为 200。例如返回的消息体里的错误码是签名失败，但 HTTP 状态码是 200，而不是 401。

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[提交工单](#)，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[提交工单](#)，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。完整的错误码列表请参考本产品“API 文档”目录下的“错误码”页面。

规则相关接口

上报自定义规则评估结果

最近更新时间：2026-04-16 17:09:33

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

上报自定义规则评估结果

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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：PutEvaluations。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
ResultToken	是	String	回调令牌。从自定义规则所选的scf云函数入参中取参数ResultToken值 云函数入参说明
Evaluations.N	是	Array of Evaluation	自定义规则评估结果信息。

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 上报自定义规则评估结果

上报自定义规则评估结果

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: PutEvaluations
<公共请求参数>

{
  "ResultToken": "Wm9yZlY3WmlKa3cxaW1oQlu-H3WA6JZnH46cUAN2DWG****",
  "Evaluations": [
    {
      "ComplianceResourceId": "disk-26itbqha",
      "ComplianceResourceType": "QCS::CBS::Disk",
      "ComplianceRegion": "ap-guangzhou",
      "ComplianceType": "NON_COMPLIANT",
      "Annotation": {
        "Configuration": "1",
        "DesiredValue": "2",
        "Operator": "equal",
        "Property": "age"
      }
    }
  ]
}
```

输出示例

```
{
  "Response": {
    "RequestId": "d947eba9-f908-4d2e-9b3d-63bde43abd1a"
  }
}
```

```
}  
}
```

5. 开发者资源

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 Node.js](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InvalidParameter	参数错误。
ResourceNotFound.AccountGroupsNotExist	账号组不存在。
ResourceNotFound.ResourceNotExist	资源不存在。
ResourceNotFound.RuleIsNotExist	规则不存在。

获取规则列表

最近更新时间：2026-04-16 17:10:22

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

获取规则列表

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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：ListConfigRules。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
Limit	是	Integer	每页数量。 取值范围：1~200
Offset	是	Integer	偏移量。 取值范围：最小值为0
OrderType	否	String	排序类型(规则名称)。 倒序：desc， 顺序：asc
RiskLevel.N	否	Array of Integer	风险等级。 1：高风险， 2：中风险， 3：低风险。

参数名称	必选	类型	描述
State	否	String	规则状态。 ACTIVE: 启用 UN_ACTIVE: 停用
ComplianceResult.N	否	Array of String	评估结果。 COMPLIANT: 合规 NON_COMPLIANT: 不合规
RuleName	否	String	规则名

3. 输出参数

参数名称	类型	描述
Total	Integer	总数
Items	Array of ConfigRule	详情
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 获取规则列表

获取规则列表

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ListConfigRules
<公共请求参数>

{
  "Offset": 0,
  "Limit": 10,
  "OrderType": "desc",
```

```
    "RiskLevel": [
      1
    ],
    "State": "ACTIVE",
    "ComplianceResult": [
      "COMPLIANT"
    ],
    "RuleName": "CAM"
  }
}
```

输出示例

```
{
  "Response": {
    "RequestId": "107f8d51-7095-4a6f-b374-a8aa7743584b",
    "Items": [
      {
        "AccountGroupId": "ca-324234",
        "AccountGroupName": "账号组",
        "Annotation": null,
        "CompliancePackId": "",
        "CompliancePackName": null,
        "ComplianceResult": "NON_COMPLIANT",
        "ConfigRuleId": "cr-HQxxxxxxxxhR0BxxxxGodh",
        "ConfigRuleInvokedTime": null,
        "CreateTime": "2024-11-15 14:21:47",
        "Description": "CAM用户下不存在已禁用的 AccessKey，则符合规则。",
        "ExcludeResourceIdsScope": [],
        "Identifier": "cam-user-invalid-ak-check",
        "IdentifierType": "SYSTEM",
        "InputParameter": [],
        "Labels": [
          "用户",
          "密钥"
        ],
        "ManageInputParameter": [],
        "ManageTriggerType": [
          "ConfigurationItemChangeNotification"
        ],
        "RegionsScope": [],
        "ResourceType": [
          "QCS::CAM::User"
        ],
        "RiskLevel": 3,
        "RuleName": "CAM用户下不存在已禁用的访问密钥AccessKey",
        "RuleOwnerId": 84935363164,
      }
    ]
  }
}
```

```
"ServiceFunction": null,
"SourceCondition": [],
"Status": "ACTIVE",
"TagsScope": [],
"TriggerType": [
  {
    "MaximumExecutionFrequency": null,
    "MessageType": "ConfigurationItemChangeNotification"
  }
],
"Total": 1
}
```

5. 开发者资源

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 Node.js](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InvalidParameter	参数错误。

账号组获取规则列表

最近更新时间：2026-04-16 17:10:41

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

账号组获取规则列表

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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：ListAggregateConfigRules。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
Limit	是	Integer	每页限制
Offset	是	Integer	偏移量
AccountGroupId	是	String	账号组ID
OrderType	否	String	排序类型, 倒序：desc, 顺序：asc
RiskLevel.N	否	Array of Integer	风险等级 1: 高风险。 2: 中风险。 3: 低风险。

参数名称	必选	类型	描述
State	否	String	规则状态
ComplianceResult.N	否	Array of String	评估结果
RuleName	否	String	规则名
RuleOwnerId	否	Integer	规则所属账号ID

3. 输出参数

参数名称	类型	描述
Total	Integer	总数
Items	Array of ConfigRule	详情
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 账号组获取规则列表

账号组获取规则列表

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ListAggregateConfigRules
<公共请求参数>

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

```
"OrderType": "",
"RiskLevel": [],
"State": "ACTIVE",
"ComplianceResult": [
  "COMPLIANT"
],
"RuleName": "",
"RuleOwnerId": 1,
"AccountGroupId": "ca-sdfs7734h24h3"
}
```

输出示例

```
{
  "Response": {
    "RequestId": "149e116a-90ef-45f3-9d5d-3d77fd1c9eb3",
    "Items": [
      {
        "RegionsScope": [
          "ap-shanghai"
        ],
        "TagsScope": [
          {
            "TagKey": "tag1",
            "TagValue": "tag2"
          }
        ],
        "ExcludeResourceIdsScope": [
          "ins-asdasd"
        ],
        "Annotation": null,
        "RuleOwnerId": 23424,
        "CompliancePackId": "cp-xzfv0vu007feuhwi8auv",
        "CompliancePackName": "合规1",
        "AccountGroupId": "ca-sdfs7734h24h3",
        "AccountGroupName": "账号组",
        "ComplianceResult": "NON_COMPLIANT",
        "ConfigRuleId": "cr-13vkg9c31dixgabkepxe",
        "ConfigRuleInvokedTime": null,
        "ManageTriggerType": [
          "SCHEDULE"
        ],
        "CreateTime": "2022-11-16 14:25:01",
        "Description": "账号访问管理中用户至少关联一个用户组，则符合规则。",
        "Identifier": "cam-user-group-bound",
        "IdentifierType": "SYSTEM",

```

```
"InputParameter": [],
"Labels": [],
"ManageInputParameter": [],
"ResourceType": [
  "QCS::CAM::User"
],
"RiskLevel": 3,
"RuleName": "CAM访问管理子用户必须关联用户组",
"ServiceFunction": null,
"SourceCondition": [
  {
    "DesiredValue": "1",
    "EmptyAs": "COMPLIANT",
    "Operator": "GreaterOrEquals",
    "Required": false,
    "SelectPath": "$User.GroupBindNum"
  }
],
"Status": "ACTIVE",
"TriggerType": [
  {
    "MaximumExecutionFrequency": "TwentyFour_Hours",
    "MessageType": "ScheduledNotification"
  }
]
],
"Total": 1
}
```

5. 开发者资源

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 Node.js](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InvalidParameter	参数错误。
ResourceNotFound.AccountGroupplsNotExist	账号组不存在。

资源相关接口

获取资源列表

最近更新时间：2026-04-16 17:09:04

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

获取资源列表

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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：ListDiscoveredResources。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
MaxResults	是	Integer	每页显示数量
Filters.N	否	Array of Filter	resourceName：资源名 resourceId：资源ID
Tags.N	否	Array of Tag	标签
NextToken	否	String	下一页token
OrderType	否	String	排序方式 asc、desc

3. 输出参数

参数名称	类型	描述
Items	Array of ResourceListInfo	详情
NextToken	String	下一页 注意：此字段可能返回 null，表示取不到有效值。
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 获取资源列表

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ListDiscoveredResources
<公共请求参数>

{
  "OrderType": "desc",
  "NextToken": "C3Ipt1Tj6hTlW0WKVO3NI",
  "MaxResults": 10,
  "Filters": [
    {
      "Values": [
        "ins-234234"
      ],
      "Name": "resourceName"
    }
  ],
  "Tags": [
    {
      "TagKey": "开发部",
      "TagValue": "运营部"
    }
  ]
}
```

```
]
}
```

输出示例

```
{
  "Response": {
    "Items": [
      {
        "ResourceStatus": "Running",
        "Tags": [
          {
            "TagKey": "开发部",
            "TagValue": "运营部"
          }
        ],
        "ResourceType": "cvm",
        "ResourceId": "ins-234er",
        "ResourceCreateTime": "2022-10-10 12:56:37",
        "ResourceRegion": "ap-guangzhou",
        "ResourceName": "云服务器",
        "ResourceZone": "ap-guangzhou-1",
        "ResourceDelete": 1,
        "ComplianceResult": "COMPLIANT"
      }
    ],
    "NextToken": "C3Ipt1Tj6hTlW0WKVO3NI",
    "RequestId": "4006b9ea-9b33-4b80-8496-6917c900b122"
  }
}
```

5. 开发者资源

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 Node.js](#)

- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InvalidParameter	参数错误。

资源详情

最近更新时间：2026-04-16 17:08:46

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

资源详情

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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：DescribeDiscoveredResource。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
ResourceId	是	String	资源ID
ResourceType	是	String	资源类型
ResourceRegion	是	String	资源地域

3. 输出参数

参数名称	类型	描述
ResourceId	String	资源Id

参数名称	类型	描述
ResourceType	String	资源类型
ResourceName	String	资源名
ResourceRegion	String	资源地域
ResourceZone	String	资源可用区
Configuration	String	资源配置
ResourceCreateTime	String	资源创建时间
Tags	Array of Tag	资源标签
UpdateTime	String	资源更新时间
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 获取资源详情

获取资源详情

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: DescribeDiscoveredResource
<公共请求参数>

{
  "ResourceId": "ins-2av11cxx",
  "ResourceType": "QCS::CVM::Instance",
  "ResourceRegion": "ap-guangzhou"
}
```

输出示例

```
{
  "Response": {
    "RequestId": "2ea2d804-d278-4631-b04d-70bd40e1a478",
    "Configuration": "{\"InstanceState\":\"RUNNING\",\"InstanceName\":\"未命名\",\"InstanceId\":\"ins-111\",\"InstanceType\":\"S5.SMALL2\",\"VirtualPrivateCloud\":{\"VpcId\":\"vpc-333\",\"SubnetId\":\"subnet-qxupkefw\",\"AsVpcGateway\":false,\"PrivateIpAddresses\":null,\"Ipv6AddressCount\":0},\"PrivateIpAddresses\":[\"111\"],\"PublicIpAddresses\":null,\"OsName\":\"TencentOS Server 4 for x86_64\",\"Memory\":2,\"CPU\":1,\"InternetAccessible\":{\"InternetChargeType\":\"\",\"InternetMaxBandwidthOut\":0,\"PublicIpAssigned\":false,\"BandwidthPackageId\":\"\"},\"ImageId\":\"img-333\",\"InstanceChargeType\":\"PREPAID\",\"SecurityGroupIds\":[\"sg-222\"],\"DataDisks\":null,\"SystemDisk\":{\"DiskType\":\"CLOUD_PREMIUM\",\"DiskId\":\"disk-auh4557w\"},\"ExpiredTime\":\"2024-12-28T08:07:12Z\",\"RenewFlag\":\"NOTIFY_AND_MANUAL_RENEW\",\"LatestOperation\":\"\",\"Placement\":{\"ProjectId\":0},\"LatestOperationState\":\"\",\"CamRoleName\":\"\"}\",
    "ResourceCreateTime": "2024-11-28 16:07:12",
    "ResourceId": "ins-2av11cxx",
    "ResourceName": "未命名",
    "ResourceRegion": "ap-guangzhou",
    "ResourceType": "QCS::CVM::Instance",
    "ResourceZone": "",
    "Tags": [],
    "UpdateTime": "2024-11-28 16:08:36"
  }
}
```

5. 开发者资源

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 Node.js](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InvalidParameter	参数错误。
ResourceNotFound.ResourceNotExist	资源不存在。

账号组获取资源列表

最近更新时间：2026-04-16 17:08:20

1. 接口描述

接口请求域名：config.intl.tencentcloudapi.com。

账号组获取资源列表

默认接口请求频率限制：20次/秒。

推荐使用 API Explorer

[点击调试](#)

API Explorer 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。您可查看每次调用的请求内容和返回结果以及自动生成 SDK 调用示例。

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： ListAggregateDiscoveredResources。
Version	是	String	公共参数 ，本接口取值：2022-08-02。
Region	是	String	公共参数 ，详见产品支持的 地域列表 。
MaxResults	是	Integer	每页显示数量
AccountGroupId	是	String	账号组ID
Filters.N	否	Array of Filter	resourceName：资源名 resourceId：资源ID resourceType： 资源类型
Tags.N	否	Array of Tag	标签
NextToken	否	String	下一页token
OrderType	否	String	排序方式 asc、desc

3. 输出参数

参数名称	类型	描述
Items	Array of AggregateResourceInfo	详情
NextToken	String	下一页 注意：此字段可能返回 null，表示取不到有效值。
RequestId	String	唯一请求 ID，由服务端生成，每次请求都会返回（若请求因其他原因未能抵达服务端，则该次请求不会获得 RequestId）。定位问题时需要提供该次请求的 RequestId。

4. 示例

示例1 获取资源列表

获取资源列表

输入示例

```
POST / HTTP/1.1
Host: config.intl.tencentcloudapi.com
Content-Type: application/json
X-TC-Action: ListAggregateDiscoveredResources
<公共请求参数>

{
  "AccountGroupId": "ca-sdfsdfsdf",
  "OrderType": "DESC",
  "Tags": [
    {
      "TagKey": "TAG1",
      "TagValue": "TAG3"
    }
  ],
  "MaxResults": 1,
  "Filters": [
    {
      "Values": [
        "CVM"
      ],
      "Name": "resourceType"
    }
  ]
}
```

```
    }  
  ],  
  "NextToken": "sdfsd sdf456457rsf"  
}
```

输出示例

```
{  
  "Response": {  
    "Items": [  
      {  
        "ResourceOwnerName": "昵称",  
        "ResourceStatus": "1",  
        "ResourceOwnerId": 1,  
        "Tags": [  
          {  
            "TagKey": "TAG2",  
            "TagValue": "33ATG5"  
          }  
        ],  
        "ResourceType": "cvm",  
        "ResourceId": "ins-324234",  
        "ResourceCreateTime": "234234234234",  
        "ResourceRegion": "ap-hangzhou",  
        "ResourceName": "服务器",  
        "ResourceZone": "ap-guanghzou",  
        "ResourceDelete": 1,  
        "ComplianceResult": "COMPLIANCE"  
      }  
    ],  
    "NextToken": "0f6ac54682ee49d5b0",  
    "RequestId": "3d105d8-5820-434f-9fac-76f92"  
  }  
}
```

5. 开发者资源

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 Node.js](#)
- [Tencent Cloud SDK 3.0 for .NET](#)
- [Tencent Cloud SDK 3.0 for C++](#)

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
InternalServerError	内部错误。
InvalidParameter	参数错误。
ResourceNotFound.AccountGroupsNotExist	账号组不存在。

数据结构

最近更新时间：2026-04-16 17:05:37

AggregateResourceInfo

资源列列表信息

被如下接口引用：ListAggregateDiscoveredResources。

名称	类型	描述
ResourceType	String	资源类型
ResourceName	String	资源名称
ResourceId	String	资源ID
ResourceRegion	String	地域
ResourceStatus	String	资源状态
ResourceDelete	Integer	是否删除 1:已删除 0:未删除
ResourceCreateTime	String	资源创建时间
Tags	Array of Tag	标签信息
ResourceZone	String	可用区
ComplianceResult	String	合规状态
ResourceOwnerId	Integer	资源所属用户ID
ResourceOwnerName	String	用户昵称

Annotation

合规详情

被如下接口引用：ListAggregateConfigRules, ListConfigRules, PutEvaluations。

名称	类型	必选	描述
Configuration	String	是	资源当前实际配置。长度为0~256位字符，即资源不合规配置
DesiredValue	String	是	资源期望配置。长度为0~256位字符，即资源合规配置
Operator	String	否	资源当前配置和期望配置之间的比较运算符。长度为0~16位字符，自定义规则上报评估结果此字段可能为空
Property	String	否	当前配置在资源属性结构体中的JSON路径。长度为0~256位字符，自定义规则上报评估结果此字段可能为空

ConfigRule

规则详情

被如下接口引用：ListAggregateConfigRules, ListConfigRules。

名称	类型	描述
Identifier	String	规则标识
RuleName	String	规则名
InputParameter	Array of InputParameter	规则参数
SourceCondition	Array of SourceConditionForManage	规则触发条件
ResourceType	Array of String	规则支持的资源类型，规则仅对指定资源类型的资源生效。
Labels	Array of String	规则所属标签
RiskLevel	Integer	规则风险等级 1:低风险 2:中风险 3:高风险
ServiceFunction	String	规则对应的函数
CreateTime	String	创建时间 格式：YYYY-MM-DD h:i:s
Description	String	规则描述

名称	类型	描述
Status	String	ACTIVE: 启用 NO_ACTIVE: 停止
ComplianceResult	String	合规: 'COMPLIANT' 不合规: 'NON_COMPLIANT' 无法应用规则: 'NOT_APPLICABLE'
Annotation	Annotation	["", ""]
ConfigRuleInvokedTime	String	规则评估时间 格式: YYYY-MM-DD h:i:s
ConfigRuleId	String	规则ID
IdentifierType	String	CUSTOMIZE: 自定义规则、 SYSTEM: 托管规则
CompliancePackId	String	合规包ID
TriggerType	Array of TriggerType	触发类型 ScheduledNotification: 周期触发、 ConfigurationItemChangeNotification: 变更触发
ManageInputParameter	Array of InputParameterForManage	参数详情
CompliancePackName	String	合规包名称
RegionsScope	Array of String	关联地域
TagsScope	Array of Tag	关联标签
ExcludeResourceIdsScope	Array of String	规则对指定资源ID无效, 即不对该资源执行评估。
AccountGroupId	String	账号组ID
AccountGroupName	String	账号组名称
RuleOwnerId	Integer	规则所属用户ID
ManageTriggerType	Array of String	预设规则支持的触发方式 ScheduledNotification: 周期触发 ConfigurationItemChangeNotification: 变更触发

Evaluation

自定义规则评估结果

被如下接口引用：PutEvaluations。

名称	类型	必选	描述
ComplianceResourceId	String	是	已评估资源ID。长度为0~256个字符
ComplianceResourceType	String	是	已评估资源类型。 支持： QCS::CVM::Instance、QCS::CBS::Disk、 QCS::VPC::Vpc、QCS::VPC::Subnet、 QCS::VPC::SecurityGroup、QCS::CAM::User、 QCS::CAM::Group、QCS::CAM::Policy、 QCS::CAM::Role、QCS::COS::Bucket
ComplianceRegion	String	是	已评估资源地域。 长度为0~32个字符
ComplianceType	String	是	合规类型。取值： COMPLIANT：合规、 NON_COMPLIANT：不合规
Annotation	Annotation	否	不合规资源的补充信息。

Filter

资源列表筛选

被如下接口引用：ListAggregateDiscoveredResources, ListDiscoveredResources。

名称	类型	必选	描述
Name	String	否	查询字段名称 资源名称：resourceName 资源ID：resourceId 资源类型： resourceType 资源地域：resourceRegion 删除状态：resourceDelete 0未删除，1已删除 resourceRegionAndZone地域/可用区
Values	Array of String	否	查询字段值

InputParameter

参数值

被如下接口引用：ListAggregateConfigRules, ListConfigRules。

名称	类型	必选	描述
ParameterKey	String	是	参数名
Type	String	否	参数类型。必填类型：Require, 可选类型：Optional。
Value	String	否	参数值

InputParameterForManage

规则入参

被如下接口引用：ListAggregateConfigRules, ListConfigRules。

名称	类型	必选	描述
ValueType	String	否	值类型。数值：Integer, 字符串：String
ParameterKey	String	否	参数Key
Type	String	否	参数类型。必填类型：Require, 可选类型：Optional。
DefaultValue	String	否	默认值
Description	String	否	描述

ResourceListInfo

资源列列表信息

被如下接口引用：ListDiscoveredResources。

名称	类型	描述
ResourceType	String	资源类型
ResourceName	String	资源名称
ResourceId	String	资源ID

名称	类型	描述
ResourceRegion	String	地域
ResourceStatus	String	资源状态
ResourceDelete	Integer	1:已删除 2: 未删除
ResourceCreateTime	String	资源创建时间
Tags	Array of Tag	标签信息
ResourceZone	String	可用区
ComplianceResult	String	合规状态

SourceConditionForManage

管理端规则条件

被如下接口引用：ListAggregateConfigRules, ListConfigRules。

名称	类型	必选	描述
EmptyAs	String	否	条件为空，合规：COMPLIANT，不合规：NON_COMPLIANT，无法应用：NOT_APPLICABLE
SelectPath	String	否	配置路径
Operator	String	否	操作运算符
Required	Boolean	否	是否必须
DesiredValue	String	否	期望值

Tag

标签

被如下接口引用：DescribeDiscoveredResource, ListAggregateConfigRules, ListAggregateDiscoveredResources, ListConfigRules, ListDiscoveredResources。

名称	类型	必选	描述
TagKey	String	否	标签key
TagValue	String	否	标签value

TriggerType

规则支持触发类型

被如下接口引用：ListAggregateConfigRules, ListConfigRules。

名称	类型	必选	描述
MessageType	String	是	触发类型
MaximumExecutionFrequency	String	否	触发时间周期

错误码

最近更新时间：2026-04-16 17:07:59

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
ActionOffline	接口已下线。
AuthFailure.InvalidAuthorization	请求头部的 <code>Authorization</code> 不符合腾讯云标准。
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。

错误码	说明
AuthFailure.SignatureFailure	签名错误。签名计算错误，请对照调用方式中的签名方法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。
InternalServerError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误（包括参数格式、类型等错误）。
InvalidParameterValue	参数取值错误。
InvalidRequest	请求 body 的 multipart 格式错误。
IpInBlacklist	IP 地址在黑名单中。
IpNotInWhitelist	IP 地址不在白名单中。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数。
NoSuchProduct	产品不存在
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
RequestLimitExceeded.GlobalRegionUinLimitExceeded	主账号超过频率限制。
RequestLimitExceeded.IPLimitExceeded	IP 限频。
RequestLimitExceeded.UinLimitExceeded	主账号限频。
RequestSizeLimitExceeded	请求包超过限制大小。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。

错误码	说明
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
ResponseSizeLimitExceeded	返回包超过限制大小。
ServiceUnavailable	当前服务暂时不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误，用户多传未定义的参数会导致错误。
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
ResourceNotFound.AccountGroupsNotExist	账号组不存在。
ResourceNotFound.ResourceNotExist	资源不存在。
ResourceNotFound.RulesNotExist	规则不存在。