云 API

常见问题

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。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。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

常见问题
- API 使用问题
- SDK 使用问题
- 证书使用问题

常见问题
API 使用问题

最近更新时间：2024-08-22 15:44:11

如何处理 C++ 运行单个签名文件报错?

在命令行运行 `g++ -o main sign.cpp` 命令时出现错误。如下图所示：

```
/tmp/cc5Dfj5N.o: 在函数‘sha256Hex(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)’中:
sign.cpp:(.text+0x278): 对‘SHA256_Init’未定义的引用
sign.cpp:(.text+0x2b1): 对‘SHA256_Update’未定义的引用
sign.cpp:(.text+0x2c7): 对‘SHA256_Final’未定义的引用
/tmp/cc5Dfj5N.o: 在函数‘HmacSha256(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > co
nst&)’中:
sign.cpp:(.text+0x430): 对‘HMAC_CTX_new’未定义的引用
sign.cpp:(.text+0x43c): 对‘EVP_sha256’未定义的引用
sign.cpp:(.text+0x481): 对‘HMAC_Init_ex’未定义的引用
sign.cpp:(.text+0x4bf): 对‘HMAC_Update’未定义的引用
sign.cpp:(.text+0x4e6): 对‘HMAC_Final’未定义的引用
sign.cpp:(.text+0x4f5): 对‘HMAC_CTX_free’未定义的引用
collect2: error: ld returned 1 exit status
```

执行以下命令，即可解决该问题。

```
g++ -o main sign.cpp -lssl -lcrypto
```

提示错误码 10060 时如何处理?

当出现 `Socket error 10060 - Connection timed out` 错误码提示时，实际是 Socket 编程接口给出的错误，表示网络连接超时。您的机器将无法和腾讯云云 API 服务器进行连通，请排查以下问题：

- 本地访问外网是否需要设置代理。
- 本地机器防火墙是否有限制外访的规则。
- 路由器是否有限制外访的规则。

腾讯云 API 的错误码有哪些?

腾讯云 API 的错误码通常分为公共错误码和非公共错误码：

- 公共错误码：您可以前往各产品文档中的 **API 文档** > **调用方式** > **返回结果**，在返回结果文档中进行查看。
- 非公共错误码：您可以在具体的接口文档中查看，例如，查看 创建实例 接口的错误码。

SDK 使用问题

最近更新时间：2024-08-22 15:44:11

Python 证书问题

在 Mac 操作系统安装 Python 3.6 或以上版本时，可能会遇到如下证书错误：

```
Error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: self
signed certificate in certificate chain (_ssl.c:1056).
```

解决方法

执行以下命令，安装证书即可解决问题。

> **说明：**
> Mac 操作系统下的 Python 不再使用系统默认的证书，且本身也不提供证书。在进行 HTTPS 请求时，需使用 `certifi` 库提供的证书。

```
sudo "/Applications/Python 3.6/Install Certificates.command"
```

PHP 证书问题

如果您的 PHP 环境证书有问题，可能会遇到如下报错信息：

```
cURL error 60: See http://curl.haxx.se/libcurl/c/libcurl-errors.html
```

解决方法

请参考以下步骤进行解决：

1. 前往 `https://curl.haxx.se/ca/cacert.pem` 下载证书文件 `cacert.pem`，将其保存到 PHP 安装路径下。
2. 编辑 `php.ini` 文件，删除 `curl.cainfo` 配置项前的分号注释符 `;`，值设置为保存的证书文件 `cacert.pem` 的绝对路径。
3. 重启依赖 PHP 的服务。

php_curl 扩展

此 SDK 依赖的 GuzzleHttp 需要开启 `php_curl` 扩展，查看环境上的 `php.ini` 环境确认是否已启用，例如在 Linux 环境下，PHP 7.1 版本，托管在 Apache 下的服务，可以打开 `/etc/php/7.1/apache2/php.ini`

文件中查看 `extension=php_curl.dll` 配置项是否已被注释，请删除此项配置前的注释符并重启 Apache。

Java 依赖冲突

目前 SDK 依赖 `okhttp 2.5.0` ，如果和其他依赖 `okhttp3` 的包混用时，可能会遇到如下报错信息：

```
Exception in thread "main" java.lang.NoSuchMethodError:
okio.BufferedSource.rangeEquals(JLokio/ByteString;)Z
```

解决方法

`okhttp3` 依赖 `okio 1.12.0` ，而 `okhttp` 依赖 `okio 1.6.0` ，Maven 在解析依赖时的规则是路径最短优先和顺序优先，如果 SDK 在 `pom.xml` 依赖中先被声明，则 `okio 1.6.0` 会被使用，从而出现报错。在 SDK 未升级到 `okhttp3` 前的解决步骤如下：

1. 在 `pom.xml` 中明确指定依赖 `okio 1.12.0` 版本。如有其他包需使用更高版本，则取两者最高版本即可。
2. 将 SDK 引用放在 `pom.xml` 文件的最后，若此前已进行编译，则需要先删除 Maven 缓存的 `okhttp` 包。以同时使用依赖 `okhttp3` 的 CMQ SDK 为例：

```
<dependency>
  <groupId>com.qcloud</groupId>
  <artifactId>cmq-http-client</artifactId>
  <version>1.0.7</version>
</dependency>
<dependency>
  <groupId>com.tencentcloudapi</groupId>
  <artifactId>tencentcloud-sdk-java</artifactId>
  <version>3.1.59</version>
</dependency>
```

.NET 依赖冲突

SDK 依赖的 `FluentClient` 使用的是3.2版本，但 `FluentClient` 目前发布了4.0版本且不兼容低版本，若在 `nuget` 中升级此包到4.0版本会导致无法调用或调用失败等问题。

旧版 SDK

旧版本 SDK 已不再维护，推荐使用新版 SDK。旧版本 SDK 存放在 `QcloudApi` 目录下，详情请参见 旧版 SDK 。

证书使用问题

最近更新时间：2024-09-11 14:17:41

DigiCert 根证书升级说明

受知名浏览器厂商 Mozilla 的根证书信任策略更新影响（全球所有 CA 的可信根证书使用年限是15年更换一次，超过时间的可信根证书将会逐步被 Mozilla 停止信任，详情请参见 官方说明 ），DigiCert 部分旧根证书将逐步升级为新根体系（G2）证书。由于腾讯云 API 的域名使用了 DigiCert 签发的证书，为保障用户请求不受影响，云 API 计划将旧证书升级为最新的 G2 根体系证书。为保障您的业务不受影响，建议及时验证与更新环境上的根证书及中间证书。

解决方案

1. 验证环境的根证书/中间证书，如果已兼容最新的 G2 根体系证书，则无需处理。如果不兼容，则需要更新证书。
2. 前往 DigiCert 官网 下载 最新的根证书和 ICA（Intermediate CA）证书，确认下载的证书包含 DigiCert Global Root G2，证书 `serialNo 03:3A:F1:E6:A7:11:A9:A0:BB:28:64:B1:1D:09:FA:E5` 。
3. 更新环境信任库证书，并再次验证兼容性。