API Gateway

Verification and Security

Product Introduction

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Verification and Security Overview

Last updated：2018-09-27 15:18:30

Various API authentication methods and API defense policies are provided to protect your APIs, avoiding data loss and asset loss caused by malicious access, unauthorized access, application vulnerability and hacker attacks.
secret_id + secret_key Authentication and No Authentication are supported for API Gateway.

"secret_id + secret_key" Authentication

Last updated：2018-09-27 16:34:07

secret_id and secret_key can be used to authenticate and manage APIs. secret_id and secret_key come in pairs. Here they are called secret_id/secret_key pair.
secret_id/secret_key pair needs to be created first before the authentication. When publishing a service, you can select to use secret_id + secret_key for authentication, and then select the created secret_id/secret_key pair at the specific place.
A secret_id/secret_key pair can be used for several published services, and a published service can also use several secret_id/secret_key pairs.

The authentication using secret_id + secret_key can be done as follows:

Key Content

secret_id example: AKIDCgOPWjQ6BAxvHtyckhWABJVYSBj548pN, indicating which key is in use and involving in signature computing, visible in transmission.

secret_key example: ZxF2whO0RhuwnVCj5JMMAuqcDcN2oPrC, used for signature computing, invisible in transmission.

Computing Method

Content to be delivered at last

The HTTP request delivered at last contains at least two headers: Date/X-Date and Authorization. More headers in a request are also workable.

The value of Date Header is the time constructed by HTTP request in GMT, for example: Fri, 09 Oct 2015 00:00:00 GMT.

The value of X-Date header is the time constructed by HTTP request in GMT, for example: Mon, 19 Mar 2018 12:08:40 GMT. The value for timeout is 15 minutes.

The authorization header is like `Authorization: hmac id="secret_id", algorithm="hmac-sha1", headers="date source", signature="Base64(HMAC-SHA1(signing_str, secret_key))"` .

The various parts of Authorization are explained as follows:

hmac: A fixed part used to indicate the computing method.
ID: The value of secret_id in the key.

algorithm: The encryption algorithm. hmac-sha1 is supported now.
headers: Refer to headers that involve in signature computing, sorting by the order of actual calculation.
signature: The signature after computing.

Signature computing method

A signature has 2 parts and is calculated by the specified encryption algorithm. Take hmac-sha1 algorithm as an example:

Signature content

First generate the signature content, which consists of custom headers. It is recommended to include date at least in the header. But you can also include more headers.

Headers are converted according to the following requirements and then sorted in sequence:

- The header name is converted to lowercase and followed by **ASCII characters** and **ASCII space characters**.
- Attach the value of the header.
- If it is not the last header that needs to construct a signature, attach **ASCII new-line character** `\n` .

For example, there are two headers involved in constructing signature content:

```
Date:Fri, 09 Oct 2015 00:00:00 GMT
Source:AndriodApp
```

The generated signature content is as follows:

```
date: Fri, 09 Oct 2015 00:00:00 GMT
source: AndriodApp
```

Computing signature

Base64(HMAC-SHA1(signing_str, secret_key)) algorithm is used to compute the signature content generated in the previous step to generate a signature, that is:

- Using the signature content as input information, secret_key content as the key, compute through HMAC-SHA1 algorithm to get the encrypted signature content.
- Convert the calculated encrypted signature content to deliverable signature content using Base64.

Using signature

As shown in **Content to be delivered at last**, at "signature" in the Authorization header, enter the signature computed in the last step.

Notes

header matching

The "headers" in Authorization are the ones that involve in signature computing. It is recommended to convert the headers to the lowercase and separate by ASCII space.

Signature content generation

Please note the colon and space following the header while organizing the content. If either is lost, it may cause the authentication to fail.

Signature for common languages demo>>

Authentication Exempt

Last updated：2018-09-27 15:17:28

You can decide whether to select "No Authentication" when creating your API. If it is selected, the API gateway will pass the authentication and the bound usage plan will also take effect when receiving an anonymous request. If the key in the usage plan is used for signature authentication, the traffic limit in the usage plan will take effect; If anonymous users access, the maximum traffic limit of each API for Tencent Cloud will take effect.