# API Gateway

# FAQs

# Product Documentation

# Contents

# FAQs
# Billing

Last updated：2023-12-22 10:10:03

### Is API Gateway a paid service?

Billing for API Gateway started at 23:59:59, February 13, 2020. Please top up your Tencent Cloud account in time in order to avoid potential service suspension. For more information, please see Billing Overview.

### What is the billing cycle for API Gateway?

API Gateway is billed on an hourly basis. Tencent Cloud generates hourly bills for API calls, typically within 30 minutes after the end of the current billing cycle.

### How is traffic of less than 1 GB charged?

If you consume billable traffic of 1 GB and 200 MB within one hour, the system will automatically convert the traffic of 200 MB to GB for billing (1 GB and 200 MB = 1 + 200/1024 = 1.1953 GB) based on which traffic fees for the hour will be calculated.

### Is it normal if multiple bills are generated on an hourly basis?

It is normal if multiple bills are generated for one hour, as API Gateway is billed in a tiered manner. If multiple tiers are hit within one hour, then multiple bills will be generated separately.

### Is API Gateway billed separately in different regions?

API Gateway is billed based on two metrics: the number of calls and traffic. The number of calls is billed at the same price in all regions, while the traffic is billed at different prices in different regions. For detailed prices, please see Billing Overview.

### What should I do if I have doubt about any bill?

If you have doubt about any bill, please see Billing Overview for more information on how API Gateway is billed, and view the billing details in the Billing section in the console.
In addition, the usage information pushed on an hourly basis for the last 30 days is retained on the backend of API Gateway, and you can ask technical support for details by submitting a ticket.

# Console

Last updated：2023-12-22 10:10:14

### How do I determine the backend URL based on the backend path?

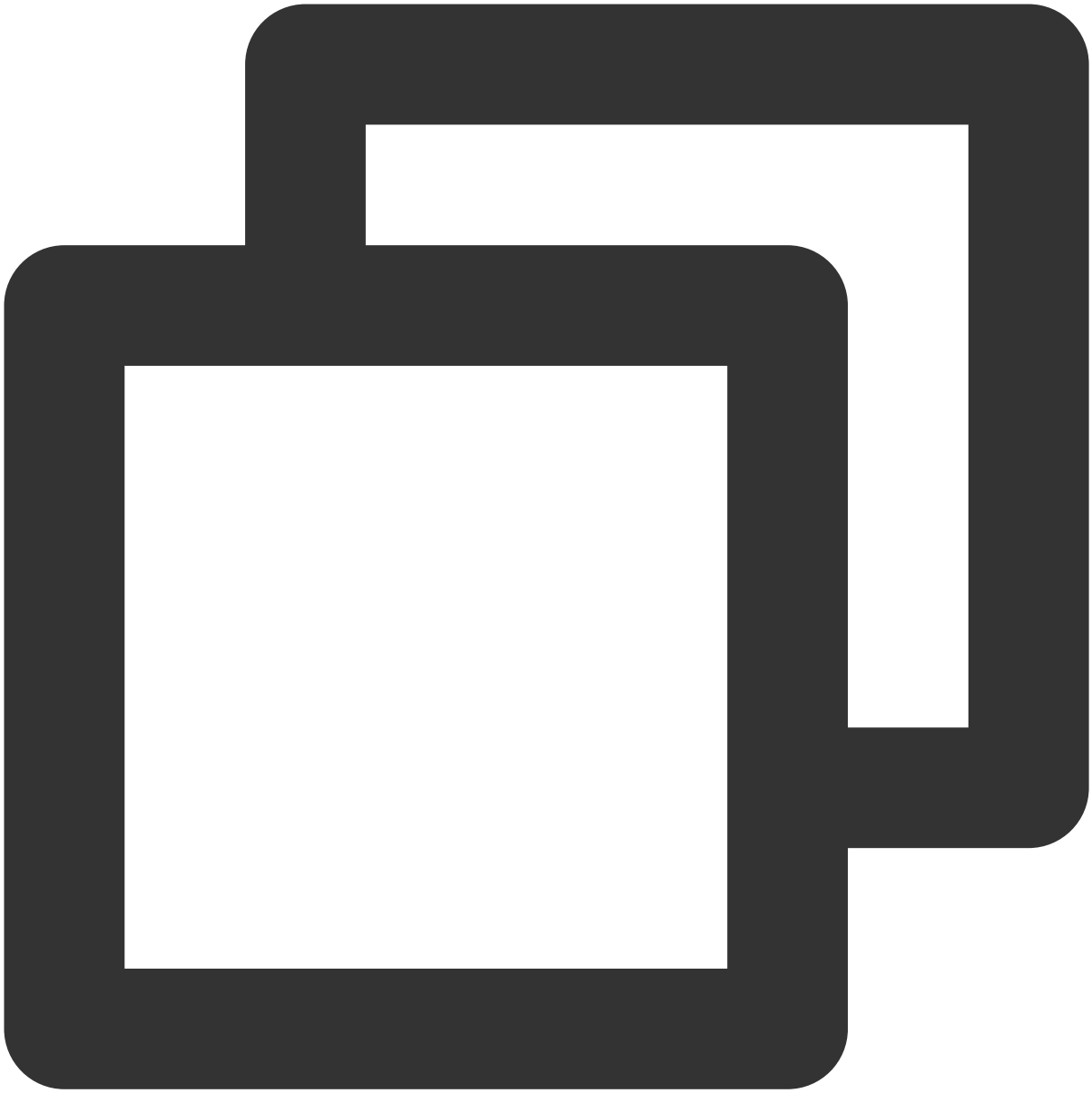
If the incoming request is `/product/apigw/document` , and the API with the frontend path of `/product/` is hit:
When the backend path is an empty string, the backend URL is `/apigw/document` .
When the backend path is `/tencent/` , cut off `/product/` and paste the rest behind the path in the backend, and then the backend URL becomes `/tencent/apigw/document` .

### How do I determine the API hit priority?

If the API path starts with `=` , it has the highest priority, and exact match is used.
If the API path starts with `^~` , it has the second priority and cannot contain regular expressions. The prefix match is used.
If the API path is a regular expression including path variables, it has the third priority.
If the API path is a normal string, the longest string has the highest priority. The longest match is used.

### How do I configure API Gateway to support CORS?

When creating an API, if you select "Support CORS", then API Gateway will support cross-origin requests. The default configuration is as follows:



```
#define CORS_DEFAULT_AC_ALLOW_ORIGIN  ("*")

#define CORS_DEFAULT_AC_ALLOW_METHODS  ("GET,POST,PUT,DELETE,HEAD,OPTIONS,PATCH")

#define CORS_DEFAULT_AC_ALLOW_CREDENTIALS  ("true")

#define CORS_DEFAULT_AC_ALLOW_HEADERS  ("X-Api-ID,X-Service-RateLimit,X-UsagePlan-R

#define CORS_DEFAULT_AC_EXPOSE_HEADERS  (CORS_DEFAULT_AC_ALLOW_HEADERS)

#define CORS_DEFAULT_AC_MAX_AGE  ("86400")
```

### What should I do if an API request fails?

After a user creates an API service, call failures often occur and the following prompt is returned:

```
{"message":"There is no api match uri[\\/api\\/v1\\/tool\\/123\\/ico] host [service-asoj98o0-1251762227.ap-guangzhou.apigateway.myqcloud.com]"}
```

Check whether the API service has been released in an environment.

A created API service can be called only after it is released in an environment. If it is modified, it won't take effect until it is released again.

If a service is released in different environments, the default call address should contain the environment name, such as:

```
service-asoj98o0-1251762227.ap-guangzhou.apigateway.myqcloud.com/release/user path
```

### How do I map the frontend and backend parameters if the API configuration contains path parameters?

When the frontend configuration contains a fixed string and path parameters, for example, the frontend path is `/{PathA}/{PathB}/detail`, if the incoming request is `/middleware/apigw/detail`, the value of PathA parameter delivered to the backend is `middleware`, and the value of PathB parameter is `apigw`.

When the frontend configuration contains a fixed string and path parameters, for example, the frontend path is `/{PathA}/product/{PathB}`, if the incoming request is `/middleware/product/apigw/detail`, the value of PathA parameter delivered to the backend is `middleware`, and the value of PathB parameter is `apigw/detail`.

When the frontend configuration only contains path parameters, for example, the frontend path is `/{PathA}/{PathB}`, if the incoming request is `/middleware/apigw/detail`, the value of PathA parameter delivered to the backend is `middleware/apigw`, and the value of PathB parameter is `detail`.

**Note:**

For microservice APIs, we recommend that you do not define both X-NameSpace-Code and X-MicroService-Name as the Path parameters. If you need to do so, please use a fixed string, for example, /{X-NameSpace-Code}/{X-MicroService-Name}/service.

# TKE

Last updated：2023-12-22 10:10:23

## How to enable private network access for a TKE cluster?

1. Log in to the TKE console, and click **Cluster** in the left sidebar.
2. Click the ID or name of the desired cluster to go to the cluster details page.
3. Click **Basic Information** in the left sidebar. You can view information such as the access address, public network/private network access status, and kubeconfig access credential of the cluster in the "Cluster APIServer information" section of the **Basic information** page.
4. Enable the **Private network access**. You need to configure a subnet. IP addresses are assigned from the configured subnet after private network access is successfully enabled.

**Note:**

Do not disable the private network access after you enable it. Otherwise, the API Gateway cannot access the APIServer of the cluster.

## How to obtain the TKE cluster admin role?

1. Log in to the TKE console, and click **Cluster** in the left sidebar.
2. Click the ID or name of the desired cluster to go to the cluster details page.
3. Click **Authorization Management** > **ClusterRole** in the left sidebar. Click **Get cluster admin role** on the page.
4. Failure to obtain the cluster admin role is generally caused by the sub-account not having the Cam permission of the TKE cluster. If this is the case, proceed according to the prompts.

# 504 Error Solution

Last updated：2023-12-22 10:10:33

## What should I do if "504 Gateway Time-out" is displayed in logs when I call the API Gateway service?

If "504 Gateway Time-out" is displayed in logs when you call the API Gateway service, you can troubleshoot the problem in the following ways:

### Check whether the API Gateway backend service can be directly accessed

If the backend service is HTTP-based and is not in any VPC, you can access it over the public network to check whether the access times out.
If the backend service is a CLB resource in a VPC, access the private IP of the CLB instance from another CVM instance in the same VPC to check whether the access times out.
If the backend service is TSF, you can access the timed-out instance through another service instance in the same namespace under TSF to check whether the access times out.
If the access still times out in the above tests, the backend service may have problems. In this case, we recommend you check whether it is normal.

### Check the timeout period set in API Gateway and the backend service

When configuring an API in API Gateway, you need to add the timeout period in the backend configuration. If the backend service fails to return the result in the specified timeout period, the gateway will return the 504 error.

### Check whether the security group is set correctly

If the backend address points to a CLB instance in a VPC, check whether the CVM security group bound to the CLB instance opens the API Gateway IP. If no security group is set, check whether there are other port and network limits for the backend address.
Open IP in a security group: the backend CVM security group bound to the CLB instance needs to open the API Gateway private IP range. For private IP ranges in different regions, see Private IP Ranges and Public VIPs of API Gateway in Different Regions. The port of the service deployed on the CVM instance also needs to be opened. For more information on how to set the security group, see Security Group Operations.
If your API is a microservice API, and the service is deployed on a CVM instance, you need to open the client IP and service port in the security group on the CVM instance.
If your API is a microservice API, and the service is deployed in a container, as the container pod may not be fixed to a CVM instance, we recommend you configure the same security group for all servers in the cluster and open the client IP and container port in the security group.
If your backend address is a general HTTP address that can be accessed over the internet, you also need to check whether the firewall and security group are set and open the gateway public VIP.

If your backend is a VPC upstream bound to a shared cluster service, you need to open the client IP and service port in the security group in the backend CVM instance.

**Note:**

As the public VIP and private IP range of API Gateway may change, we recommend you use key pair authentication to ensure request security.

# HTTP Error Codes

Last updated：2023-12-22 10:10:46

### What are the common errors when API Gateway is called?

When you call API Gateway, you may encounter the following common HTTP error codes:

**Frontend errors**:

| Error Code | Log Message | Description |
| --- | --- | --- |
| 401 | HMAC apikey is invalid for API. | `APIKey` is not bound to this API. |
| 401 | HMAC signature cannot be verified, a valid x-date header is required for HMAC Authentication. | HMAC authentication does not include `x-date` in the header, or the HMAC value is invalid. |
| 401 | HMAC signature cannot be verified, the x-date header is out of date for HMAC Authentication. | The `x-date` timestamp timed out. It is 900s by default. |
| 401 | HMAC signature cannot be verified, a valid date or x-date header is required. | If there is no `x-date`, the header must contain `date`. |
| 401 | HMAC id or signature missing. | The ID or signature field is missing in `Authorization`. |
| 401 | HMAC do not support multiple HTTP header. | A header with multiple values is not supported. |
| 401 | HMAC signature cannot be verified, a valid xxx header is required. | xxx header is missing in the request. |
| 401 | HMAC algorithm xxx not supported. | HMAC algorithm does not support xxx, which currently supports HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, and HMAC-SHA512. |
| 401 | HMAC authorization format error. | Incorrect `Authorization` format. |
| 401 | HMAC authorization headers is invalidate. | `Authorization` lacks sufficient parameters. For more information, please see Key Pair Authentication - Eventually Delivered Content. |
| 401 | HMAC signature cannot be verified. | Unable to verify the signature, possibly because the `APIKey` cannot be recognized. This usually |

| | | |
|---|---|---|
| | | happens if the `APIKey` is not bound to this service or API. |
| 401 | HMAC signature does not match. | The signature does not match. |
| 401 | Oauth call authentication server fail. | Failed to call the authentication server. |
| 401 | Oauth found no related Oauth api. | As the associated Oauth authentication API is not found, the `id_token` cannot be verified. |
| 401 | Oauth miss Oauth id_token. | The `id_token` is missing in the request. |
| 401 | Oauth signature cannot be verified, a validate authorization header is required. | Authentication header missing. |
| 401 | Oauth authorization header format error. | Incorrect Oauth header format. |
| 401 | Oauth found no authorization header. | Authentication header not found. |
| 401 | Oauth found no id_token. | `id_token` not found. |
| 401 | Oauth id_token verify error. | JWT-formatted `id_token` verification failed. |
| 403 | Found no validate usage plan. | No corresponding usage plan found. Access denied. (This error may occur if the usage plan feature is enabled.) |
| 403 | Cannot identify the client IP address, unix domain sockets are not supported. | Unable to identify the source IP. |
| 403 | Endpoint IP address is not allowed. | The backend IP is not allowed to access. |
| 403 | Get xxx params fail. | An error occurred while getting parameters from the request. |
| 403 | need header Sec-WebSocket-Key. | The `Sec-WebSocket-Key` header is missing in the actual request, which will be checked for APIs configured with WebSocket. |
| 403 | need header Sec-WebSocket-Version. | The `Sec-WebSocket-Version` header is missing in the actual request, which will be checked for APIs configured with WebSocket. |
| 403 | header xxx is required. | The xxx header is missing in the actual request. |
| | | |

| | | |
|---|---|---|
| 403 | path variable xxx is required. | The `{xxx}` path variable is configured but does not match the actual request path. |
| 403 | querystring xxx is required. | The xxx querystring is missing in the actual request. |
| 403 | req content type need application/x-www-form-urlencoded. | Requests with the `body` parameter must be in form format. |
| 403 | body param xxx is required. | The xxx body parameter is missing in the actual request. |
| 404 | Not found micro service with key. | No corresponding microservice found. |
| 404 | Not Found Host. | The request should have the `host` field, whose value should be the server's domain name in string type. |
| 404 | Get Host Fail. | The value of the `host` field in the request is not in string type. |
| 404 | Could not support method. | This request method type is not supported. |
| 404 | There is no api match host[$host]. | Request server domain name/address not found. |
| 404 | There is no api match env_mapping[$env_mapping]. | The `env_mapping` field after the custom domain name is incorrect. |
| 404 | There is no api match default env_mapping[$env_mapping]. | The value of the `env_mapping` field after the default domain name should be `test/prepub/release` . |
| 404 | There is no api match uri[$uri]. | The API that matches the URI is not found in the service corresponding to the request address. |
| 404 | Not allow use HTTPS protocol or Not allow use HTTP protocol. | The service corresponding to the requested address does not support the HTTP protocol type. |
| 404 | Found no api. | The request did not match an API. |
| 405 | Method Not Allowed. | HTTP request method not allowed |
| 426 | Not allow use HTTPS protocol. | HTTPS protocol not allowed. |
| 426 | Not allow use HTTPS protocol. | HTTP protocol not allowed. |
| 426 | Not allow use HTTPS protocol. | xxx protocol not allowed. |
| 429 | API rate limit exceeded. | The request rate limit is exceeded. The current rate can |

| | | |
|---|---|---|
| | | be viewed through the request header. |
| 429 | API quota exceeded. | The configuration quota is exceeded. Remaining quota can be viewed through the request header. |
| 429 | req is cross origin, api $uri need open cors flag on qcloud apigateway. | This is a cross-origin request, but the corresponding API has not enabled cross-origin access. |
| 481 | API config error. | API configuration error. |
| 481 | TSF config error. | TSF configuration error. |
| 481 | Get location of micro service info fail. | Microservice name and namespace are not configured to get location. |
| 481 | Only support the map_from like method.req.{path}.{}. | Microservice name and namespace are configured to get location, but the location format is invalid. |
| 481 | Found no valid cors config. | CORS configuration error. |
| 481 | Oauth public key error. | Public key certificate configuration error. |
| 481 | Oauth id_token location forbidden. | Forbidden `id_token` storage location. |
| 481 | Oauth found no oauth config. | Oauth configuration not found. |
| 481 | Oauth found no public key. | Public key not found. |
| 481 | Mock config error. | Mock configuration error. |
| 499 | Client closed connetion. | The client closed connection. |

**Backend errors**:

| Error Code | Log Message | Description |
|---|---|---|
| 500 | Error occurred during query params. | An error occurred while querying parameters. |
| 500 | Internal Server Error. | 1. Other APIGW internal logic error.<br>2. If the API is proxy type, accessing the backend address without access permission will also cause this error. |
| 502 | Bad Gateway. | Backend service connection error. Possible reasons:<br>1. The backend denied the service, and the 502 error occurred for all requests. |

| | | |
|---|---|---|
| | | 2. 2.Backend load was too high, and the 502 error occurred for some requests. |
| 504 | Gateway Time-out. | Backend server connection timed out. |