API 网关

常见问题

腾讯云

【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
计费相关问题

最近更新时间：2024-01-22 16:28:51

API 网关服务收费吗?

API 网关服务于2020年2月13日23:59:59正式商业化售卖，请您及时对您的腾讯云账号进行 充值 操作避免服务中断。详情请参见 计费概述 。

API 网关产品的计费周期是什么?

API 网关产品的计费周期为小时。腾讯云每小时生成当前计费周期的 API 调用费用记录，出账时间通常在当前计费周期结束后30分钟内。

不足1GB的流量如何收取流量费用?

如果用户在一小时内产生了1GB + 200MB的可计费流量，系统会自动将不满1GB的200MB流量换算为 GB 进行计费。1GB + 200MB = 1 + 200/1024 = 1.1953GB，最终按照1.1953GB计算这一小时的流量费用。

每小时产生多个费用订单是正常的吗?

每小时产生多个费用订单是正常现象。API 网关产品采用阶梯计费的方式，如果一个小时内跨越多个收费阶梯，会有多个订单分别计费出单。

API 网关产品分地域计费吗?

API 网关产品的费用由两部分组成，分别是调用次数费用与流量费用。其中调用次数费用仅在共享版实例产生，全地域统一，不区分地域计费；而流量费用的收费标准各地域不同，按地域进行计费。详细的定价信息请您参见 计费概述 。

对扣费有疑问怎么处理?

如果您对扣费有疑问，请先参见 计费概述 文档了解 API 网关产品的计费规则，并通过控制台 费用账单 查看消费明细。
同时，API 网关后台也保存了近30天内每小时的推送用量信息，您可以通过 在线客服 的方式，由专业的技术人员帮您查询。

云市场购买的商品在哪些情况会计算调用次数?

云市场支持第三方服务商将自有商品上架进行售卖，其中对于交付方式为 API 的商品（ 点击查看 交付方式为 API 的商品），部分服务商使用了 API 网关作为其开放自有服务的工具，此处 API 网关向服务商收取调用次数费，具体参考 计费 > 调用次数费用 ，下文对 API 网关将在哪些情况下计算服务商的调用次数进行说明。

作为销售商品的卖家

也即服务商，可通过将自有服务 上架云市场 、上架后如有用户购买，可通过 云市场看板 查看对应的购买明细、调用明细等。

作为购买商品的买家

也即终端用户，可通过 买家中心 查看已购买商品的情况。

调用链路及扣除次数说明

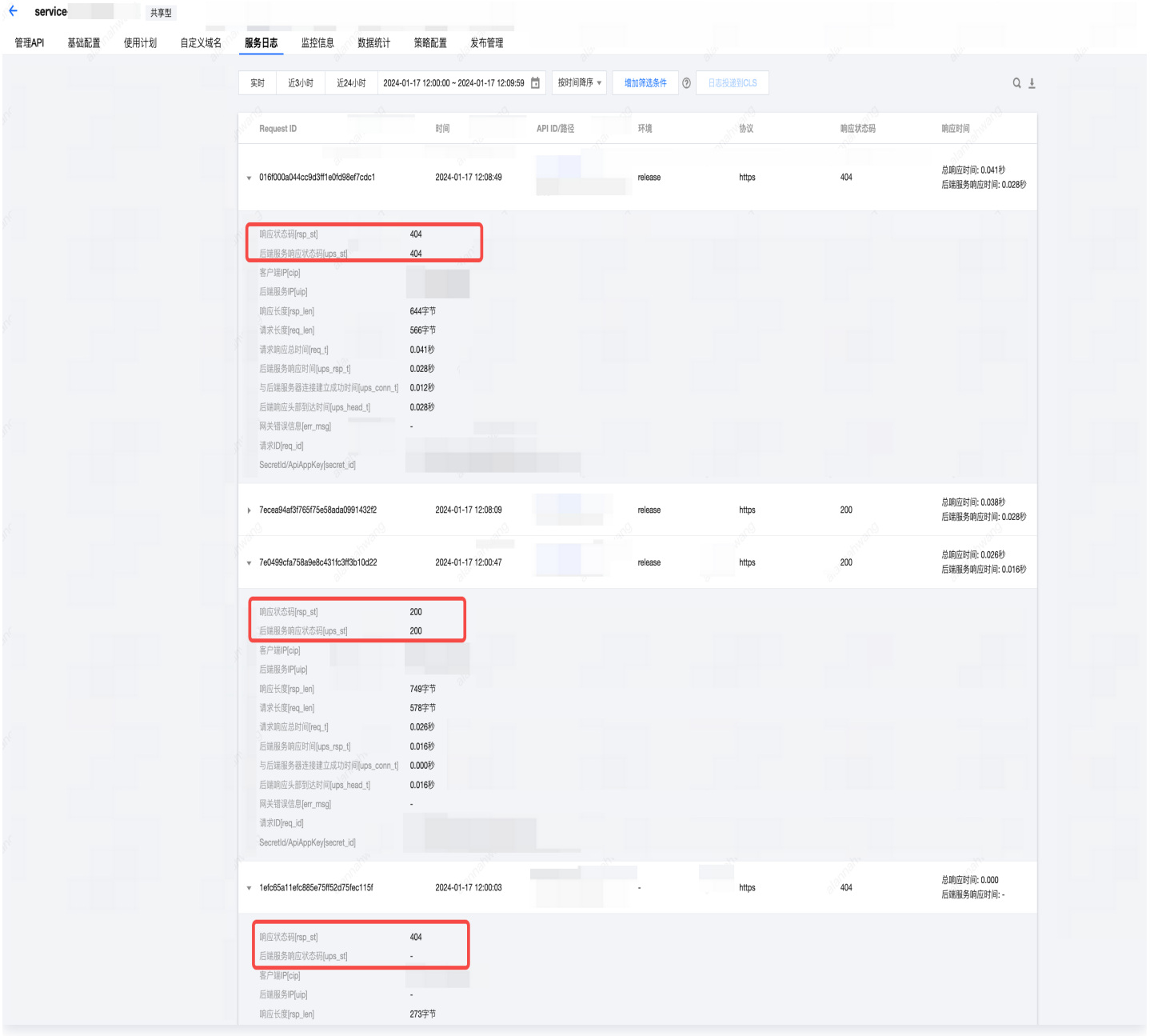
为方便说明，本文将完整链路分为3个关键节点。终端用户 —> API 网关 —> 云市场服务商的后端服务。

1. 终端用户发起调用请求。
2. 请求到达 API 网关，API 网关将请求到服务商后端，再将其后端响应透传至终端用户。
   如果服务商后端有返回，则透传后端状态码给终端用户。
   如果没到服务商后端，则返回 API 网关状态码给终端用户。
3. 对于 API 网关响应的状态码，如果**响应状态码[rsp_st]**为 `200` ，则计算调用次数。如果**响应状态码[rsp_st]**非 `200` ，则依据该请求的**后端服务响应状态码[ups_st]**来判断，是否计算调用次数，如果为空则不计算调用次数，如果非空则计算调用次数。

示例说明

以下分为3种情况作为示例。下文所示**服务日志**，可在服务商账号下登录 API 网关，在服务中通过 查看服务日志 。

> **说明：**
> 第1条请求，**响应状态码[rsp_st]**为 `404` ，但其原因在于**后端服务响应状态码[ups_st]**为 `404` ，计算调用次数。因请求经过 API 网关且成功故计算调用次数。具体原因是服务商后端响应了 `404` ，需由服务商排查其原因。其他由服务商后端响应的错误码，同理。
> 第2条请求，**响应状态码[rsp_st]**为 `200` ，成功响应，计算调用次数。
> 第3条请求，**响应状态码[rsp_st]**为 `404` ，但其原因在于**后端服务响应状态码[ups_st]**为 `-` ，不计算调用次数。表示请求到 API 网关时失败、未响应到服务商后端，具体原因是 API 网关响应了404，各种状态码请参考 HTTP错误码 。


service
共享型
管理API
基础配置
使用计划
自定义域名
服务日志
监控信息
数据统计
策略配置
发布管理
实时
近3小时
近24小时
2024-01-17 12:00:00 ~ 2024-01-17 12:09:59
按时间降序
增加筛选条件
日志投递到CLS
Request ID
时间
API ID/路径
环境
协议
响应状态码
响应时间
016f000a044cc9d3ff1e0fd98ef7cdc1
2024-01-17 12:08:49
release
https
404
总响应时间: 0.041秒
后端服务响应时间: 0.028秒
响应状态码[rsp_st] 404
后端服务响应状态码[ups_st] 404
客户端IP[cip]
后端服务IP[uip]
响应长度[rsp_len] 644字节
请求长度[req_len] 566字节
请求响应总时间[req_t] 0.041秒
后端服务响应时间[ups_rsp_t] 0.028秒
与后端服务器连接建立成功时间[ups_conn_t] 0.012秒
后端响应头部到达时间[ups_head_t] 0.028秒
网关错误信息[err_msg] -
请求ID[req_id]
SecretId/ApiAppKey[secret_id]
7ecea94af3f765f75e58ada0991432f2
2024-01-17 12:08:09
release
https
200
总响应时间: 0.038秒
后端服务响应时间: 0.028秒
7e0499cfa758a9e8c431fc3ff3b10d22
2024-01-17 12:00:47
release
https
200
总响应时间: 0.026秒
后端服务响应时间: 0.016秒
响应状态码[rsp_st] 200
后端服务响应状态码[ups_st] 200
客户端IP[cip]
后端服务IP[uip]
响应长度[rsp_len] 749字节
请求长度[req_len] 578字节
请求响应总时间[req_t] 0.026秒
后端服务响应时间[ups_rsp_t] 0.016秒
与后端服务器连接建立成功时间[ups_conn_t] 0.000秒
后端响应头部到达时间[ups_head_t] 0.016秒
网关错误信息[err_msg] -
请求ID[req_id]
SecretId/ApiAppKey[secret_id]
1efc65a11efc885e75ff52d75fec115f
2024-01-17 12:00:03
-
https
404
总响应时间: 0.000
后端服务响应时间: -
响应状态码[rsp_st] 404
后端服务响应状态码[ups_st] -
客户端IP[cip]
后端服务IP[uip] -
响应长度[rsp_len] 273字节

控制台相关问题

最近更新时间：2022-01-07 09:46:03

根据后端 path 如何确定后端 URL?

如果客户进来的请求是 `/product/apigw/document`，命中 前端 path 为 `/product/` 的 API:

- 如果后端 path 为空串，那么转给后端的 URL 就是 `/apigw/document`。
- 如果后端 path 的内容不为空为 `/tencent/`，那么就切掉 `/product/` 部分，剩下的黏在后端的 path 后面成为 `/tencent/apigw/document`。

API 命中优先级如何确定?

- 如果 API path 以 `=` 开始，代表精确匹配，优先级最高。
- 如果 API path 以 `^~` 开始，代表优先前缀匹配，后面不能跟正则表达式，优先级第二。
- 如果 API path 为正则表达式（包括有路径变量），优先级第三。
- 如果 API path 为普通串，字符串最长的优先级高，满足最长匹配。

API 网关支持 CORS 时如何配置?

在创建 API 时，若勾选了支持 CORS，则 API 网关支持跨域请求，默认配置如下：

```
#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-RateLimit,X-UsagePlan-Quota,Cache-
Control,Connection,Content-Disposition,Date,Keep-
Alive,Pragma,Via,Accept,Accept-Charset,Accept-Encoding,Accept-
Language,Authorization,Cookie,Expect,From,Host,If-Match,If-Modified-
Since,If-None-Match,If-Range,If-Unmodified-
Since,Range,Origin,Referer,User-Agent,X-Forwarded-For,X-Forwarded-
Host,X-Forwarded-Proto,Accept-Range,Age,Content-Range,Content-Security-
Policy,ETag,Expires,Last-Modified,Location,Server,Set-
Cookie,Trailer,Transfer-Encoding,Vary,Allow,Content-Encoding,Content-
Language,Content-Length,Content-Location,Content-Type")

#define CORS_DEFAULT_AC_EXPOSE_HEADERS  (CORS_DEFAULT_AC_ALLOW_HEADERS)
```

```
#define CORS_DEFAULT_AC_MAX_AGE  ("86400")
```

API 请求失败时如何处理?

用户在创建 API 服务后，经常发现调用失败，返回类似提示：

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

此时请先检查这个 API 服务是否已经发布在某个环境中。

创建 API 后，必须发布服务到环境中方可进行调用。API 在被编辑后也需要重新发布才能生效。

另外，当服务发布在不同环境中，默认调用地址中需要带环境名称，如：

`service-asoj98o0-1251762227.ap-guangzhou.apigateway.myqcloud.com/release/用户路径`

对于使用 path 参数的 API，前后端参数如何映射?

- 如果前端配置包含固定串和 Path 参数，如前端路径为 `/{PathA}/{PathB}/detail`，如果客户进来的请求是 `/middleware/apigw/detail`，那么传给后端的 PathA 参数值为 middleware，PathB 参数值为 apigw。
- 如果前端配置包含固定串和 Path 参数，如前端路径为 `/{PathA}/product/{PathB}`，如果客户进来的请求是 `/middleware/product/apigw/detail`，那么传给后端的 PathA 参数值为 middleware，PathB 参数值为 apigw/detail。
- 如果前端配置仅使用 Path 参数，如前端路径为 `/{PathA}/{PathB}`，如果客户进来的请求是 `/middleware/apigw/detail`，那么传给后端的 PathA 参数值为 middleware/apigw，PathB 参数值为 detail。

> **说明**
> 对于微服务 API，不建议同时将 X-NameSpace-Code 和 X-MicroService-Name 定义为 Path 参数。如需同时定义为 Path 参数，请使用固定串分割，如 `/{X-NameSpace-Code}/{X-MicroService-Name}/service`。

TKE 相关问题

最近更新时间：2023-06-09 17:02:38

如何开启 TKE 集群内网访问功能?

1. 登录 容器服务控制台，在左侧导航栏中的**集群**，进入集群管理界面。
2. 单击需要连接的集群“ID/名称”，进入集群详情页。
3. 选择左侧导航栏中的**基本信息**，即可在基本信息页面中查看**集群 APIServer 信息**模块中该集群的访问地址、外网/内网访问状态、Kubeconfig 访问凭证内容等信息。如下图所示：

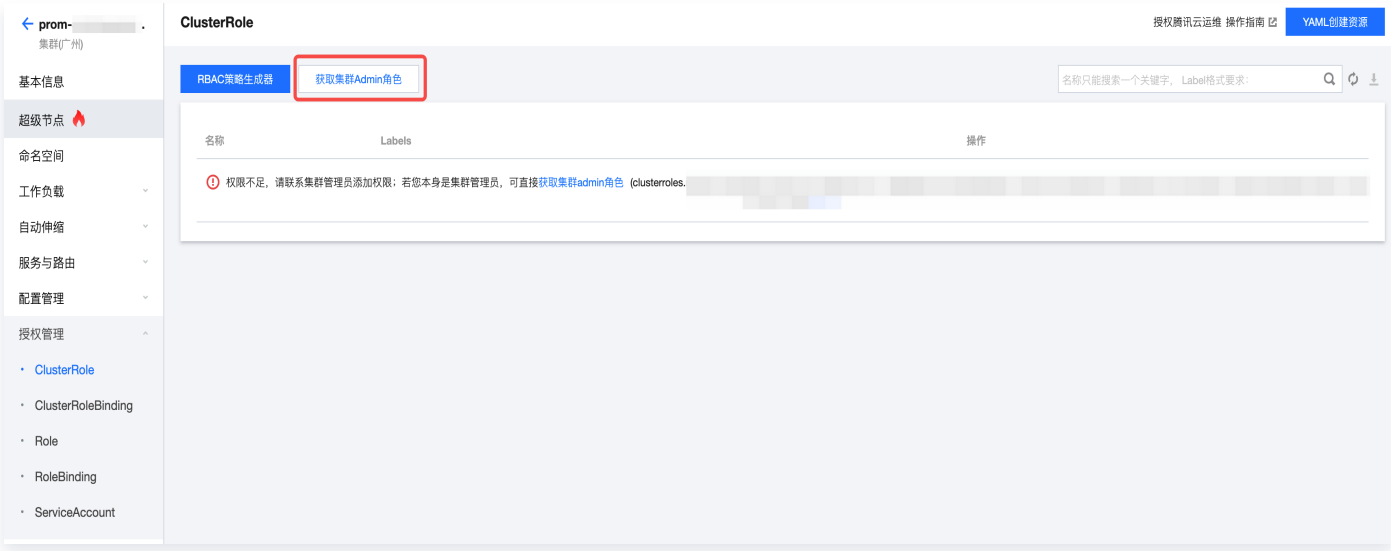
4. 单击内网访问的按钮**开启**。开启内网访问时，需配置一个子网，开启成功后将在已配置的子网中分配 IP 地址。

> **注意**
> 开启内网访问后，不能关闭，否则 API 网关会访问不到集群的 APIServer。

如何获取 TKE 集群 admin 角色?

1. 登录 容器服务控制台，在左侧导航栏中的**集群**，进入集群管理界面。
2. 单击需要连接的集群"ID/名称"，进入集群详情页。

3. 选择左侧导航栏中的**授权管理** > **ClusterRole**，单击主界面的**获取集群 Admin 角色**，即可获取集群 Admin 角色。



4. 如果获取集群 Admin 角色失败，一般是由于子账号没有 TKE 集群的 Cam 权限导致的，按照提示解决即可。

504 问题处理方法

最近更新时间：2023-12-15 16:24:41

调用 API 网关服务时，日志中出现“504 Gateway Time-out”如何处理?

当用户调用 API 网关服务时，如果日志中出现“504 Gateway Time-out”，可以从以下几个角度排查问题：

检查直接访问 API 网关后端服务是否正常

- 当后端服务是 HTTP 类型，且不在任何 VPC 内，直接通过外网访问查看是否超时。
- 当用户后端服务是 VPC 内的负载均衡资源时，使用相同 VPC 内的另一台 CVM 访问负载均衡的内网 IP，检查是否超时。
- 当用户后端服务是 TSF 时，通过 TSF 下同一个命名空间的服务实例对超时实例进行访问，检查是否超时。

在以上情况中，如果测试依然超时，考虑是后端服务存在问题，建议检查后端服务是否正常。

检查 API 网关以及后端服务设置的超时时间

用户在配置 API 网关的 API 时，需要在后端配置中添加超时时间，如果后端服务没有在超时时间内返回结果，网关会返回504错误。

检查安全组是否设置正确

对于 API 网关的共享实例，因外网VIP变更较频繁，如果用户设置了安全组，则可按照下列步骤检查：

- 当用户后端地址是 VPC 内的 CLB 时，查看关联的 CLB 绑定的 CVM 安全组是否放通了 API 网关的 IP。如果没有设置安全组，请查看后端地址是否还存在其他的端口网络限制。
  放通安全组方法：CLB 绑定的后端 CVM 安全组，需要放通 API 网关的内网 IP 网段，不同地域内网 IP 网段列表请参见 API 网关各地域内网网段以及外网 VIP 。端口需要放通部署在 CVM 上的服务的端口。安全组的设置方式请参见 安全组操作 。
- 当用户的 API 是微服务 API，且服务部署在 CVM 上时，需要在 CVM 上的安全组上放通客户端 IP，端口放通服务端口。
- 当用户的 API 是微服务 API，且服务部署在容器中时，由于容器的 pod 不一定固定在某个 CVM 上，建议将集群中的机器都放通相同的安全组，放通客户端 IP，端口放通容器的端口。
- 当用户的后端地址是一般的外网可访问 HTTP 地址时，也需要检查是否有设置防火墙、安全组等，需要放通网关的外网 VIP 。
- 当用户的后端是 VPC 通道，并且 VPC 通道绑定到了共享集群服务上，需要在后端 CVM 的安全组上放通客户端 IP，端口放通服务端口。

> **说明**
> 由于 API 网关的共享实例属于多用户共享，无法保证外网 VIP 以及内网网段不变，建议用户使用密钥对鉴权以保证请求的安全。

> 或建议选购具备固定 VIP 的专享实例 。

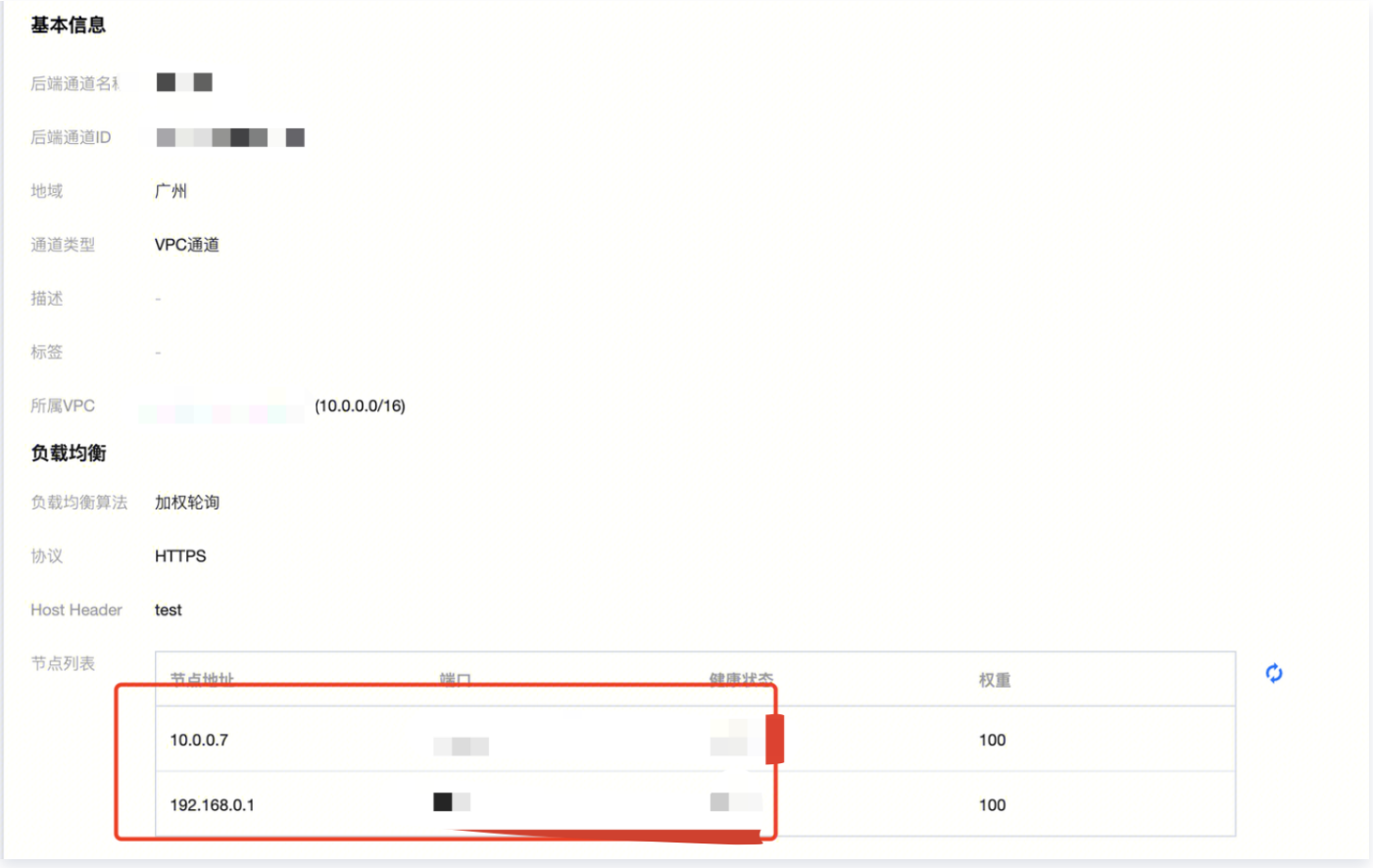
TKE通道504问题如何排查

504一般是后端超时或者地址不正确导致的报错。

1.检查是否后端超时

同一 VPC 下的其他节点请求后端服务，判断有无超时。
同时还需要确认有无安全组限制，如有则需要放通安全组。

2.检查是否后端地址和 APIGW节点列表不匹配



尝试重新更新 TKE 中的服务，再进行重试。
如果还存在问题，可 提交工单 以进行排查和解决解决。

HTTP 错误码

最近更新时间：2023-12-25 11:09:41

调用 API 网关有哪些常见错误?

用户调用 API 网关时，常见的 HTTP 错误码及说明如下：

前台错误

错误码	日志中错误提示	说明
401	HMAC apikey is invalid for API.	APIKey 没有绑定到该 API。
401	HMAC signature cannot be verified, a valid x-date header is required for HMAC Authentication.	HMAC 认证时没有在 header 中带上 x-date，或者 HMAC 值非法。
401	HMAC signature cannot be verified, the x-date header is out of date for HMAC Authentication.	x-date 时间戳超时，默认为900s。
401	HMAC signature cannot be verified, a valid date or x-date header is required.	如果没有 x-date，则 header 中包含 date。
401	HMAC id or signature missing.	Authorization 中 ID 或者 signatrue 字段缺失。
401	HMAC do not support multiple HTTP header.	不支持一个 header 包含多个值的形式。
401	HMAC signature cannot be verified, a valid xxx header is required.	请求中缺少 xxx header。
401	HMAC algorithm xxx not supported.	HMAC 算法不支持 xxx，目前支持 hmac-sha1、hmac-sha256、hmac-sha384、hmac-sha512。
401	HMAC authorization format error.	Authorization 格式错误。
401	HMAC authorization headers is invalidate.	Authorization 缺少足够的参数，请参考 密钥对认证-最终发送内容 。

401	HMAC signature cannot be verified.	无法检验签名，可能原因为 APIKey 无法识别，通常是 APIKey 没有绑定到这个服务或者没有绑定到这个 API。
401	HMAC signature does not match.	签名不一致。
401	Oauth call authentication server fail.	调用认证服务器失败。
401	Oauth found no related Oauth api.	没有查到关联的 Oauth 认证 API，无法认证 id_token。
401	Oauth miss Oauth id_token.	请求缺少 id_token。
401	Oauth signature cannot be verified, a validate authorization header is required.	没有认证头部。
401	Oauth authorization header format error.	Oauth 头部格式错误。
401	Oauth found no authorization header.	没有找到认证头部。
401	Oauth found no id_token.	没有找到 id_token。
401	Oauth id_token verify error.	JWT 格式的 id_token 验证失败。
403	Found no validate usage plan.	没有找到对应的使用计划，禁止访问（开启使用计划时可能出现的错误）。
403	Cannot identify the client IP address, unix domain sockets are not supported.	无法识别源 IP。
403	Endpoint IP address is not allowed.	禁止访问的后端 IP。
403	Get xxx params fail.	从请求中获取参数出错。
403	need header Sec-WebSocket-Key.	实际请求缺少 header Sec-WebSocket-Key，配置了 websoket 的 API 会检验。

403	need header Sec-WebSocket-Version.	实际请求缺少 header Sec-WebSocket-Version，配置了 websoket 的 API 会检验。
403	header xxx is required.	实际请求缺少 header xxx。
403	path variable xxx is required.	配置了路径变量 `{xxx}` ，但是与实际请求的路径不能匹配。
403	querystring xxx is required.	实际请求缺少 querystring xxx。
403	req content type need application/x-www-form-urlencoded.	配置了 body 参数的请求必须是表单格式。
403	body param xxx is required.	实际请求缺少 body 参数 xxx。
403	Found no validate apiapp.	当前 API 没有绑定的应用认证密钥。
404	Not found micro service with key.	没有找到对应的微服务。
404	Not Found Host.	请求携带 host 字段，该字段值需要填服务器的域名，且为 String 类型。
404	Get Host Fail.	请求中携带的 host 字段值不是 String 类型。
404	Could not support method.	并不支持该请求方法类型。
404	There is no api match host[$host].	找不到请求服务器域名/地址。
404	There is no api match env_mapping[$env_mapping].	自定义域名后的 env_mapping 字段错误。
404	There is no api match default env_mapping[$env_mapping].	默认域名后的 env_mapping 字段需要是 test/prepub/release。
404	There is no api match uri[$uri].	在该请求地址对应的服务下找不到对应 URI 匹配的 API。
40	Not allow use HTTPS protocol或者	该请求地址对应的服务并不支持对应 HTTP 协议类

4	Not allow use HTTP protocol.	型。
404	Found no api.	请求没有匹配到 API。
405	Method Not Allowed.	不允许的 HTTP 请求方法。
426	Not allow use HTTPS protocol.	不允许用 HTTPS 协议。
426	Not allow use HTTP protocol.	不允许用 HTTP 协议。
426	Not allow use xxx protocol.	不允许用 xxx 协议。
429	API rate limit exceeded.	请求速率超过限速值，当前速率值可以查看请求的 header。
429	API quota exceeded.	配置超限，剩余的配额可以通过请求的 header 查看。
429	req is cross origin, api $uri need open cors flag on qcloud apigateway.	该请求是跨域请求，但对应的 API 并未打开跨域开关。
481	API config error.	API 配置错误。
481	TSF config error.	TSF 相关配置错误。
481	Get location of micro service info fail.	没有配置微服务名、微服务命名空间获取位置。
481	Only support the map_from like method.req.{path}.{}.	配置了微服务名、微服务空间的拉取位置，但是位置格式非法。
481	Found no valid cors config.	CORS 配置出错。
481	Oauth public key error.	配置的公钥证书错误。
481	Oauth id_token location forbidden.	不允许的 id_token 存放位置。

481	Oauth found no oauth config.	没有找到 Oauth 配置。
481	Oauth found no public key.	没有找到公钥。
481	Mock config error.	mock 的配置出错。
499	Client closed connection.	客户端主动中断连接。

后台错误

错误码	日志中错误提示	说明
500	Error occurred during query params.	query 参数处理出错。
500	Internal Server Error.	1. 其他 APIGW 内部逻辑错误。 2. 若 API 为 proxy 类型，访问了没有权限访问的后端地址也会报该错误。
502	Bad Gateway.	连接后端服务出错，可能情况： 1. 后端拒绝服务，全部请求都为502。 2. 后端高负载，导致部分请求响应为502。
503	Apigw balancer error	后端域名无法解析或者解析出错。 请检查api配置的后端域名是否有效、是否能正常解析。
504	Gateway Time-out.	后端服务器连接超时。

网络层错误

错误码	日志中错误提示	说明
-	SSL_ERROR_SYSCALL OPENSSL_internal:TLSV1 ALERT_INTERNAL_ERROR	ssl 协议握手失败，导致在API网关中建立连接时失败。也即服务未访问。 可能情况： 1. 证书是否正确 2. 服务是否未操作发布 3. 服务是否选择了HTTPS

安全与合规相关说明

最近更新时间：2024-11-05 14:59:02

政府监管机构和腾讯云对违规业务的处罚机制是什么？

用户在使用腾讯云产品时，应遵守国家法律、行政法规、各部门规章等规范性文件，并自行按照相关法律法规，向相关对象提供合法的产品及服务，履行相关义务。

1. 关于可能造成违规的信息类型，详细请参见 违规信息类型说明 。
2. 关于违反相关规定的行为，腾讯云有权进行处罚。详情请参见 云安全违规处罚等级划分说明 。
3. 特殊的，在您使用腾讯云产品或服务的有效期内，您可能需要对自己部署在腾讯云上的代码、数据、应用、组件、服务等进行安全评估工作。安全评估工作包括但不限于：漏洞扫描、渗透测试、压力测试、漏洞挖掘等（全文同），如果您计划进行安全评估工作，您需同意并遵守对应政策和规范，请参见 客户安全评估工作政策与规范 。
4. 特殊的，政府监管机构也可能直接下达对违规业务的处置决定，具体需以实际情况为准。在这类政府行为引发您的腾讯云服务不能正常使用和造成其他衍生损害，您需要自行承担责任，腾讯云无需就此承担责任。具体请参见 服务等级协议 中的相关免责条款。

为什么我的 API 网关服务会被发现有违规而影响访问？

API 网关实例规格分为共享型实例、专享型实例，如为共享型实例，在公网入口和出口等都是一组用户共享，详情请参见 实例规格 。

首先，当您使用共享型、专享型实例创建服务时，需要符合相关法律法规要求，若这些服务中的内容存在违规，腾讯云合规团队将对其进行处置。处置的信息将在 消息控制台 中的消息列表中进行通知；同时政府监管机构也可能下发处置决定。

其次，对于共享型实例在网络层面都是一组用户共享，也可能存在其他用户违规引发了政府监管机构和腾讯云合规团队的处置。而其中政府监管机构的处置机制如果是从**三大通信运营商层面**进行限制，则整个集群都可能被限制访问。

综上考虑，强烈建议您对重要核心业务优先采用专享型实例来管理您的业务服务、从而隔绝他人可能引发违规处罚的服务，详情请参见 专享型实例的计费规则 。