负载均衡（CLB）

产品文档

腾讯云TCE

版权所有：TCloudFinanceZone

目录

负载均衡（CLB） 4
- 产品简介 4
  - 产品概述 4
  - 产品优势 6
  - 应用场景 7
  - 技术原理 9
  - 实例类型 11
  - 使用约束 12
  - 监控指标 13
- 购买指南 14
  - 计费概述 14
  - 购买方式 15
- 快速入门 16
  - 负载均衡快速入门 16
  - IPv6 负载均衡快速入门 26
  - CentOS下部署Nginx 34
  - CentOS下部署Java Web 37
- 操作指南 44
  - 负载均衡实例 44
    - 创建负载均衡实例 44
    - 创建 IPv6 负载均衡实例 46
    - 创建 IPv6 NAT64 负载均衡实例 48
    - 删除负载均衡实例 50
    - 配置负载均衡安全组 51
    - 调整实例带宽配置 59
  - 负载均衡监听器 61
    - 负载均衡监听器概述 61
    - 配置TCP监听器 64
    - 配置UDP监听器 69
    - 配置HTTP监听器 74
    - 配置HTTPS监听器 81
    - 轮询方式 88
    - 健康检查 91
    - 会话保持 95
    - 证书配置 97
    - 七层重定向配置 101
    - 七层个性化配置 105
    - 七层转发域名和URL规则说明 110
    - CLB 支持 SNI 多域名证书 115
  - 后端云服务器 116
    - 后端云服务器概述 116
    - 添加、修改和解绑后端服务器 117
    - 绑定弹性网卡 121
    - 后端云服务器安全组配置说明 123
  - 监控与告警 125
    - 获取监控数据 125
    - 监控指标说明 126
    - 配置告警策略 129
    - 告警指标说明 132
  - 证书管理 134
    - 管理证书 134
    - 证书要求及转换证书格式 137
  - 日志管理 141
    - 查看操作日志 141
    - 配置访问日志 142
  - 访问管理 145
    - 概述 145
    - 授权定义 147
    - 策略示例 152
  - 配额管理 153
- 常见问题 155
  - 健康检查异常排查思路 155
  - 客户端timewait过多解决方案 157
  - 负载均衡HTTPS服务性能测试 160
  - 压力测试常见问题 163
- 最佳实践 165
  - 负载均衡开启Gzip配置及检测方法说明 165
  - HTTPS转发配置入门指南 168
  - 如何获取客户端真实IP 170
  - 多可用区高可用配置说明 175
  - SSL证书格式要求及格式转换说明 176
  - 均衡算法选择与权重配置实例 180
- API文档 183
  - 负载均衡（clb） 183
    - 版本（2018-03-17） 183
      - API 概览 183
      - 调用方式 186
        - 接口签名v1 186
        - 接口签名v3 193
        - 请求结构 202
        - 返回结果 203
        - 公共参数 206
      - 其他接口 208
        - 根据证书ID查询负载均衡 208
        - 设置负载均衡实例的安全组 210
        - 绑定或解绑一个安全组到多个负载均衡实例 212
      - 负载均衡相关接口 214
        - 自动生成负载均衡转发规则的重定向关系 214
        - 批量解绑四七层后端服务 216

- 批量修改监听器绑定的后端机器的转发权重 218
- 批量绑定虚拟主机或弹性网卡 219
- 创建负载均衡监听器 221
- 购买负载均衡实例 224
- 创建负载均衡七层监听器转发规则 229
- 删除证书 231
- 删除负载均衡监听器 233
- 删除负载均衡实例 235
- 删除负载均衡转发规则之间的重定向关系 237
- 删除负载均衡七层监听器的转发规则 239
- 从负载均衡监听器上解绑后端服务 241
- 查询用户和绑定的集群标签 243
- 查询证书列表 245
- 拉取配置绑定的server或location。 247
- 拉取配置列表 249
- 查询运营商信息 252
- 根据证书id获取绑定的监听器 254
- 查询负载均衡的监听器列表 256
- 查询负载均衡实例列表 259
- 查询负载均衡转发规则的重定向关系 261
- 查询子账号配额 263
- 获取负载均衡后端服务的健康检查状态 265
- 查询负载均衡绑定的后端服务列表 267
- 查询异步任务状态 269
- 修改负载均衡配置询价 271
- 手动添加负载均衡转发规则的重定向关系 273
- 修改证书备注 276
- 修改负载均衡七层监听器转发规则的域名级别属性 278
- 修改负载均衡监听器属性 281
- 修改负载均衡实例的属性 284
- 修改负载均衡七层监听器的转发规则 287
- 修改监听器绑定的后端机器的端口 290
- 修改监听器绑定的后端机器的转发权重 292
- 绑定后端机器到监听器上 294
- 替换证书 296
- 负载均衡维度的个性化配置相关操作 297
- 设置子账号配额 299
- 上传证书 301

- 数据结构 302
- 错误码 309

产品简介
产品概述

什么是负载均衡

负载均衡（Cloud Load Balancer）是对多台云服务器和裸金属服务器进行流量分发的服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

负载均衡服务通过设置虚拟服务地址（VIP），将位于同一地域的多台云服务器资源虚拟成一个高性能、高可用的应用服务池。根据应用指定的方式，将来自客户端的网络请求分发到云服务器池中。

负载均衡服务会检查云服务器池中云服务器实例的健康状态，自动隔离异常状态的实例，从而解决了云服务器的单点问题，同时提高了应用的整体服务能力。

云平台提供的负载均衡服务具备自助管理、自助故障修复 等功能，适用于企业、社区、电子商务、游戏等多种用户场景。

组成部分

一个提供服务的负载均衡组通常由以下部分组成：

- Cloud Load Balancer：负载均衡实例，用于流量分发。
- VIP(virtual IP)：负载均衡向客户端提供服务的 IP 地址。
- Backend/Real Server：后端一组云服务器实例，用于实际处理请求。
- VPC：整体网络环境。
  来自负载均衡外的访问请求，通过负载均衡实例并根据相关的策略和转发规则分发到后端服务器进行处理。

名词解释

术语	全称	说明
负载均衡器	Cloud Load Balancer	云平台提供的一种网络负载均衡服务，可以结合后端云服务器或裸金属服务器为用户提供基于 TCP/UDP 以及 HTTP/HTTPS负载均衡服务。
负载均衡监听器	Load Balance Listener	负载均衡服务监听器，包括监听端口、负载均衡策略和健康检查配置等，每个监听项对应后端的一个应用服务。
后端服务器	Real Server	接受负载均衡分发请求的一组云服务器或裸金属服务器实例，负载均衡服务将访问请求按照用户设定的规则转发到这一组后端服务器上进行处理。

术语	全称	说明
虚拟服务地址	Virtual IP	系统分配的服务地址，当前为 IP 地址。用户可以选择该服务地址是否对外公开，来分别创建公网和内网类型的负载均衡服务。

负载均衡的工作原理

基本工作原理

负载均衡器接受来自客户端的传入流量，并将请求路由到一个或多个可用区的后端云服务器实例上进行处理。

负载均衡服务主要由负载均衡监听器提供。监听器负责监听负载均衡实例上的请求、执行策略分发至后端服务器等服务，通过配置客户端 - 负载均衡和负载均衡 - 后端服务器两个维度的转发协议及协议端口，负载均衡可以将请求直接转发到后端云服务器上。

建议您跨多个可用区配置负载均衡器的后端服务器实例。如果一个可用区变得不可用，负载均衡器会将流量路由到其他可用区正常运行的实例上去，从而屏蔽可用区故障引起的服务中断问题。

请求路由选择

客户端请求通过域名访问服务，在请求发送到负载均衡器之前，DNS 服务器将会解析负载均衡域名，并将收到请求的负载均衡 IP 地址返回到客户端。当负载均衡监听器收到请求时，将会使用不同的负载均衡算法将请求分发到后端服务器中。目前云平台支持加权轮询、ip_hash和加权最小连接数等多种均衡算法。

监控后端服务状态

负载均衡器还可以监控后端实例的运行状况，从而确保只将流量路由到正常运行的实例上去。当负载均衡器检测到运行不正常的实例时，它会停止向该实例路由流量，然后会在它再次检测到实例正常运行之后重新向其路由流量。

相关服务

负载均衡与以下服务一起使用，可以提高应用程序的可用性和可扩展性：

- CVM 实例：应用程序在云上运行的虚拟服务器。
- 弹性伸缩：弹性地控制实例数量。在弹性伸缩中启用负载均衡实例，则伸缩的实例将自动加入负载均衡组，同时终止的实例将自动被移出负载均衡组。
- 云监控：帮助您监控负载均衡及所有后端实例的运行状况并执行所需操作。
- 域名解析：通过将您自定义的域名（如 www.example.com ）转换为网络通信所用的 IP 地址（如 192.0.2.1 ），快速便捷地将请求路由至负载均衡实例。
- BMS 实例：为用户提供的云上裸金属服务器。

产品优势

负载均衡服务主要由如下性能指标来评判：

- TPS（每秒新建连接数）：负载均衡实例每秒新建 TCP 连接的能力。
- 最大并发连接数：并发连接数指客户端向服务器发起请求并建立了 TCP 连接的总数。即每秒钟服务器连接的总 TCP 数量。
- QPS（query per second）：也可以叫 RPS，每秒请求。请求数指客户端在建立完连接后，向 HTTP 服务发出 GET/POST/HEAD 数据包。
- 吞吐量：负载均衡实例可支持的总的流量带宽。

云平台提供高性能的负载均衡服务：

- 负载均衡单集群提供超过1.2亿的最大并发连接数，轻松应对亿级 Web 业务访问量。
- 负载均衡单集群可处理峰值上百Gb/s的流量，每秒处理包量（PPS）可达上千万级。
- 对每个租户的流量进行严格隔离，并可联动安全产品提供防护能力。

应用场景

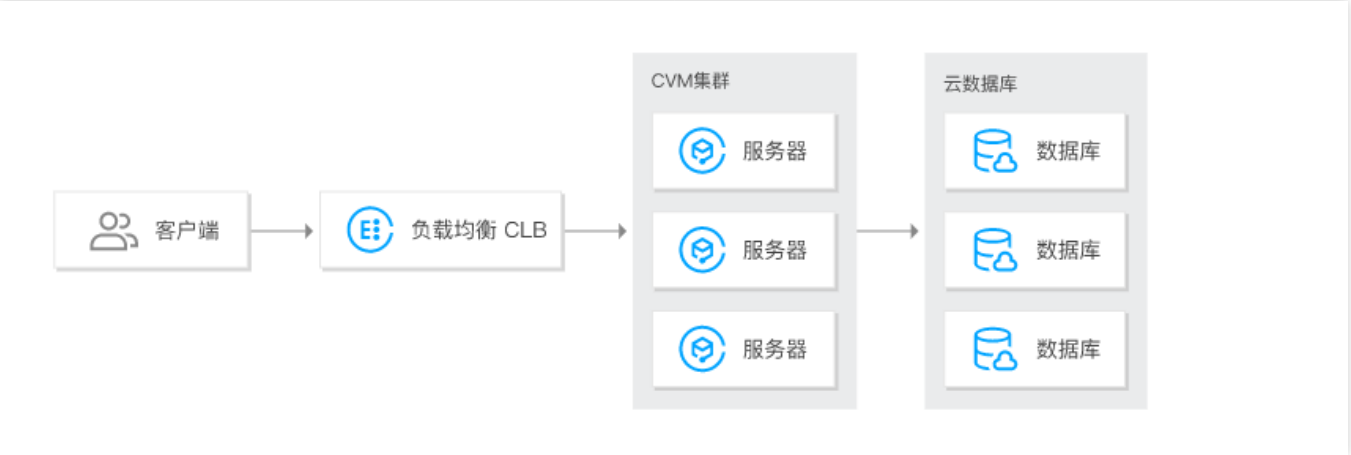
负载均衡主要适用于如下场景：

- 流量分发，将高访问量的业务通过负载均衡分发到多台云服务器上。
- 消除单点故障，当其中一部分云服务器不可用时，负载均衡可自动屏蔽故障的 CVM 实例，保障应用系统正常工作。
- 横向扩展，根据业务发展的需要，按需扩展应用系统的服务能力，适用于各种 Web Server和 App Server。
- 全局负载均衡，结合域名解析，可支持全局多地域负载均衡，保障异地容灾。

流量分发和消除单点故障

您可以通过负载均衡，将业务流量分发到多台云服务器上：

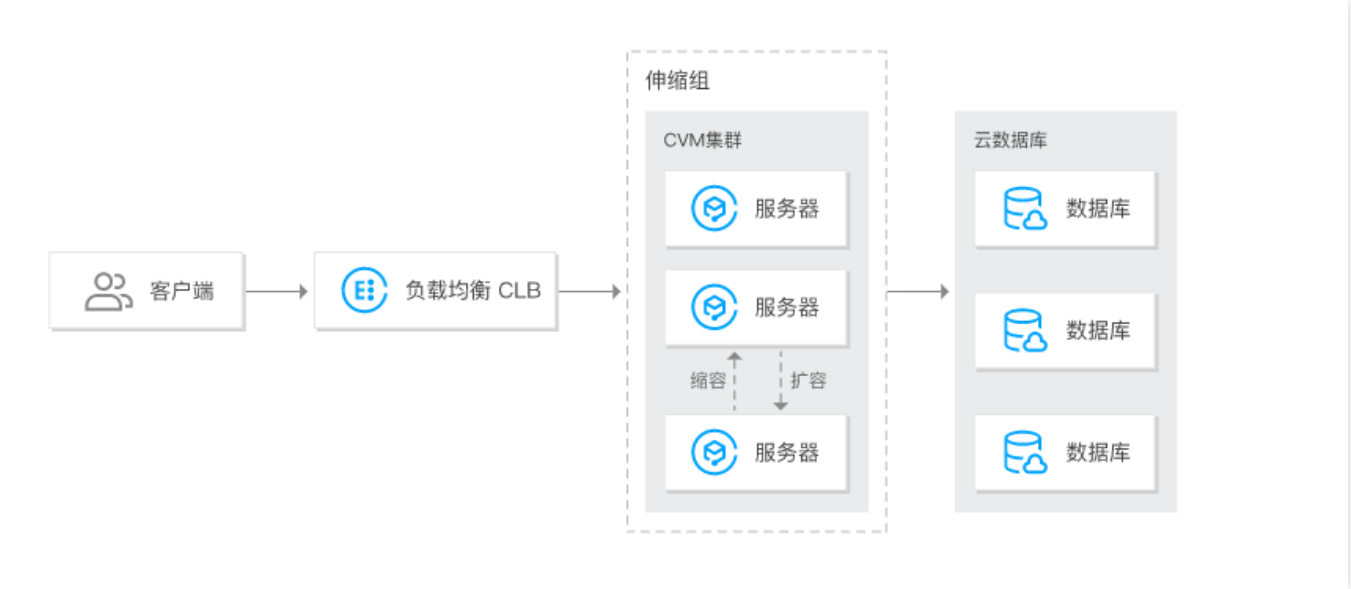
- 业务的客户端访问负载均衡。
- 多台云服务器构成一个高性能、高可用的服务池，负载均衡将业务流量转发到这批云服务器上。
- 当某台或某几台云服务器不可用时，负载均衡可自动屏蔽故障的 CVM 实例，将请求分发给正常运行的 CVM 实例，保障应用系统正常工作。
- 会话保持功能可将同一客户端的请求转发到同一台后端云服务器，提高访问效率。



横向扩展

负载均衡结合 弹性伸缩，可为您按需创建和释放 CVM 实例。

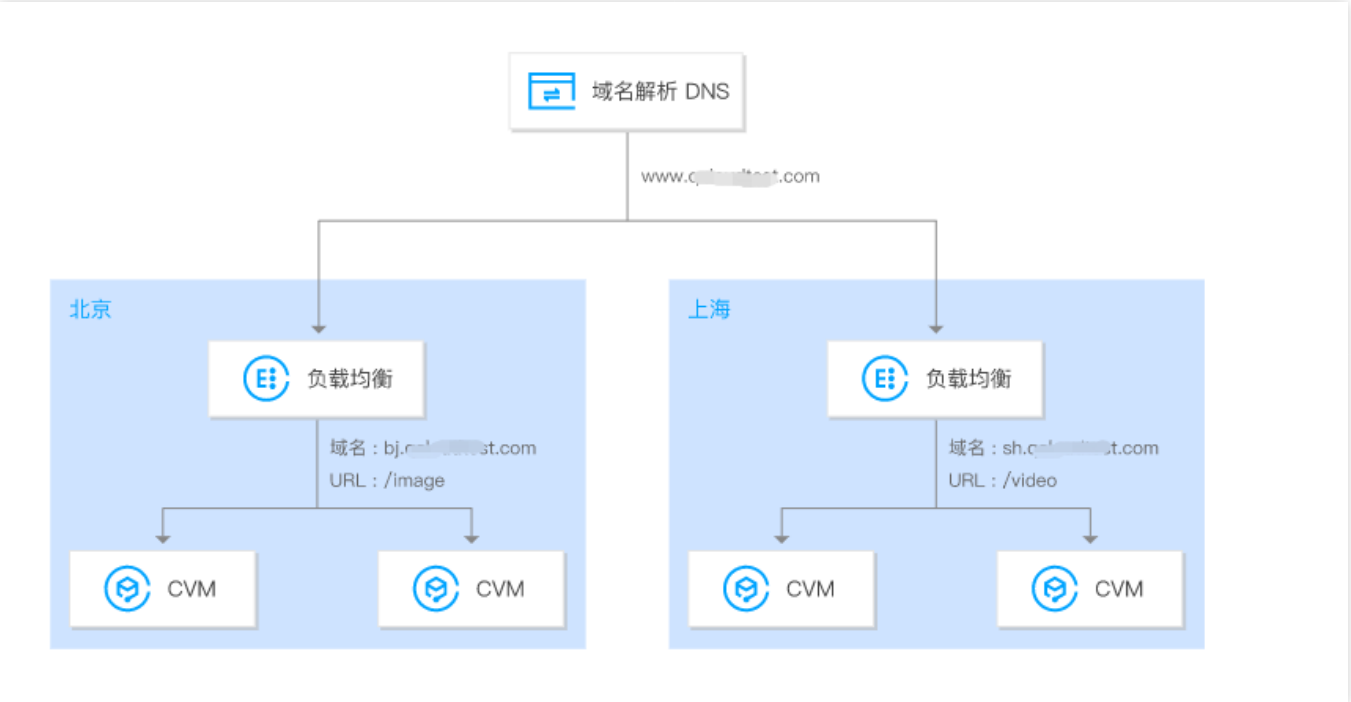
- 您可以设定弹性伸缩策略来管理 CVM 实例数量，完成对实例的环境部署，并保证业务平稳顺利运行。在需求高峰时，自动增加 CVM 实例数量，以保证性能不受影响。当需求较少时，则会减少 CVM 实例数量以降低成本。
- 电商行业的“双11”、“6.18”等大促活动，Web 访问量可能瞬间陡增10倍，且只持续短暂的数小时。使用负载均衡及弹性伸缩能最大限度的节省 IT 成本。



全局负载均衡

结合域名解析，您可以将业务流量解析到全局各个地域的负载均衡，保障异地多活和容灾。

- 您可以在不同地域部署负载均衡实例，并分别绑定对应地域的云服务器。
- 使用域名解析将域名解析到各个地域的负载均衡 VIP 下。
- 业务流量会通过域名解析和负载均衡转发到多个地域的多个云服务器上，以此实现全局负载均衡。
- 当某个地域不可用时，暂停对应地域负载均衡 VIP 的解析即可保障业务不受影响。



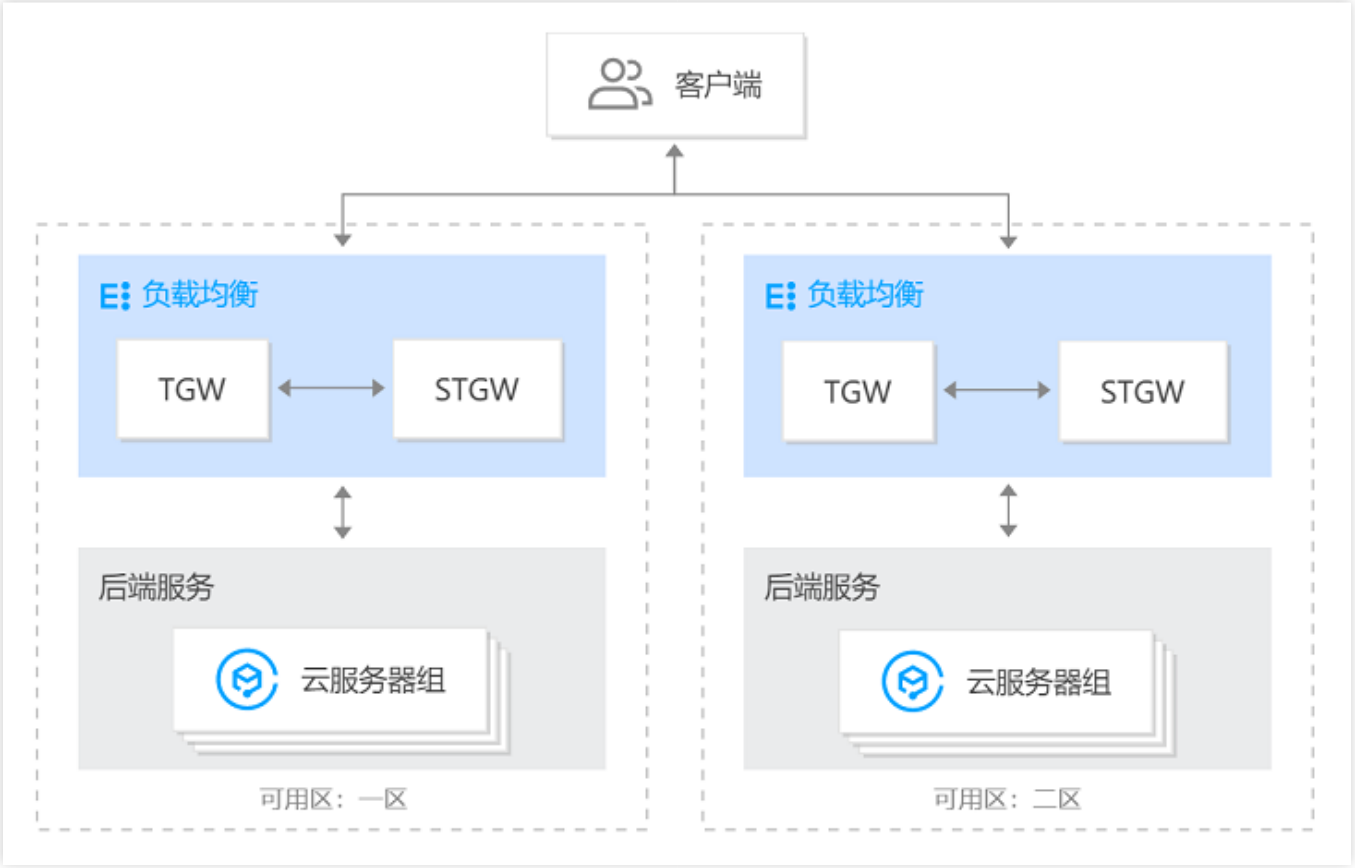
技术原理

负载均衡 CLB 提供四层（TCP 协议/UDP 协议）和七层（HTTP 协议/HTTPS 协议）负载均衡。您可以通过 CLB 将业务流量分发到多个后端服务器上，消除单点故障并保障业务可用性。CLB 自身采用集群部署，可实现会话同步，消除服务器单点故障，提升系统冗余，保证服务稳定，可在同一个地域部署多个机房，实现同城容灾。

基础架构

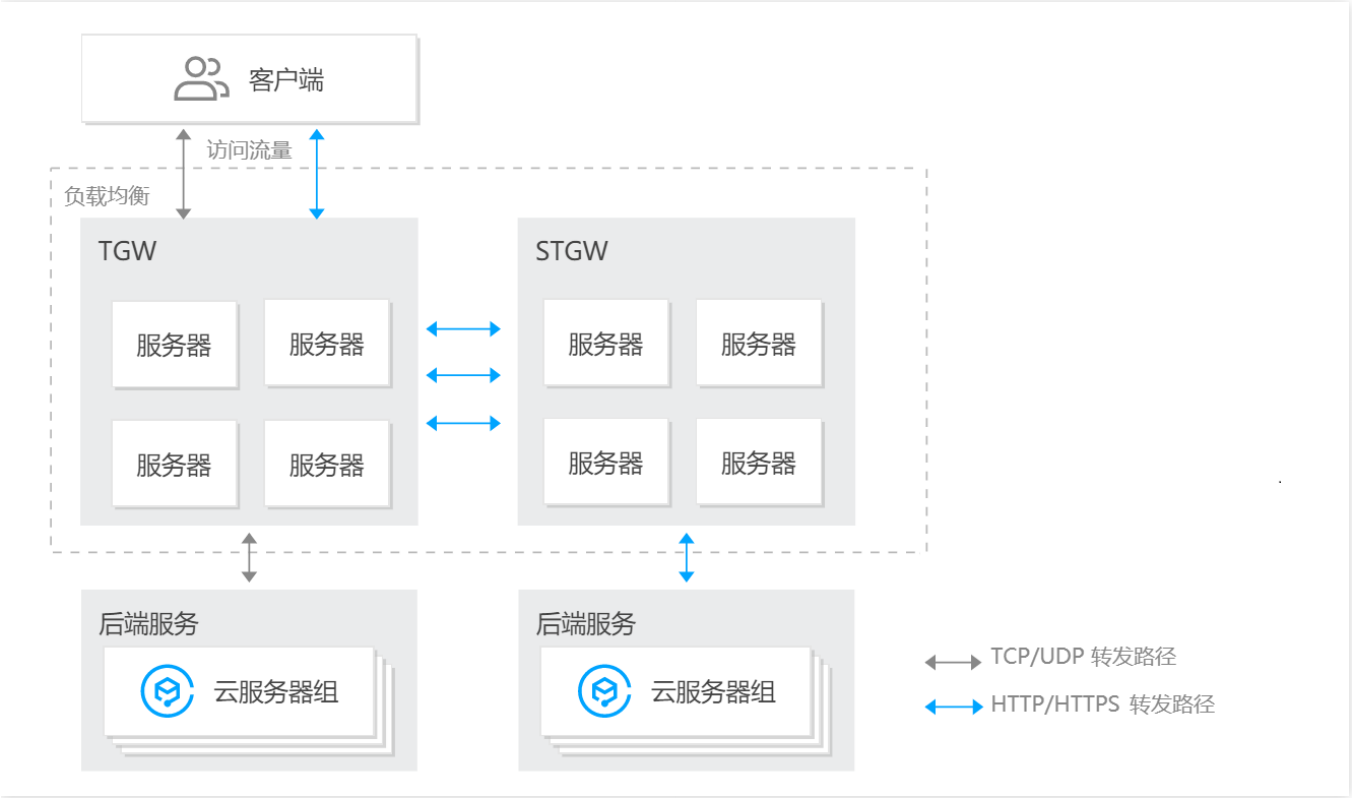
TCloudFinanceZone负载均衡当前提供四层和七层的负载均衡服务：

- 四层主要基于统一接入网关（TGW）来实现负载均衡，TGW 具有可靠性高、扩展性强、性能高、抗攻击能力强等特点，支持 Data Plane Development Kit（DPDK）高性能转发，单集群可支持亿级并发、千万级 PPS。
- 七层主要基于STGW实现负载均衡，STGW 是基于 Nginx 自研的支持大规模并发的七层负载均衡服务，承载了大量的七层业务流量。



转发路径

负载均衡负责转发业务流量，由后端服务实际处理业务请求。CLB 与后端 CVM 之间是通过内网进行通信的。TGW 和 STGW 均由多台服务器部署，通过集群来提供负载均衡服务。CLB 的转发路径如下图所示。



1. TCP/UDP协议：

- TCP/UDP 协议由 TGW 集群处理转发逻辑。
- 业务流量到达后，由 TGW 通过内网转发给后端 CVM，后端 CVM 的回包也是通过 TGW 返回给客户端。

2. HTTP/HTTPS 协议：

- 处理 HTTP/HTTPS 协议时，业务流量会先经过 TGW 集群，而后由 STGW 识别 HTTP 协议并转发给后端 CVM。
- 业务流量到达后，在内网中依次通过 TGW、STGW、后端 CVM，回包也依次逆向返回给客户端。

实例类型

负载均衡支持 TCP/UDP/HTTP/HTTPS 协议，提供基于域名和 URL 路径的均衡能力，支持灵活转发。

产品类型	负载均衡-公网	负载均衡-内网
七层转发（HTTP/HTTPS）	✓	✓
四层转发（TCP / UDP）	✓	✓
支持 HTTP/2 及 websocket（secure）	✓	✓
负载均衡策略	IP Hash（七层） 按权重轮询 加权最小连接数	IP Hash（七层） 按权重轮询 加权最小连接数
会话保持	✓	✓
健康检查	✓	✓
自定义转发规则（域名/URL）	✓	✓
转发到不同的后端端口	✓	✓
七层重定向功能（rewrite）	✓	✓

使用约束

负载均衡使用时的使用限制如下：

实例类型	资源	默认限制
负载均衡	一个账号在单地域可创建的公网实例数量	100
负载均衡	一个账号在单地域可创建的内网实例数量	100
负载均衡	一个实例可添加的监听器数量	50
负载均衡	一个实例中的监听器可选择的端口	端口为1 - 65535的整数
负载均衡	一个负载均衡实例中，HTTP/HTTPS 监听可配置的域名和 URL 转发规则数量	50
负载均衡	一个负载均衡实例的转发规则可绑定的服务器数量	100
负载均衡	一个负载均衡实例的前端端口可对应的后端端口数量	多个端口

监控指标

本文介绍负载均衡产品的租户端监控指标。

指标类型	指标/事件ID	指标名称	单位
数值监控	Intraffic	入带宽	Mb/s
数值监控	Outtraffic	出带宽	Mb/s
数值监控	Inpkg	入包量	个/秒
数值监控	Outpkg	出包量	个/秒
数值监控	Intraffic	入带宽	Mb/s
数值监控	Outtraffic	出带宽	Mb/s
数值监控	Inpkg	入包量	个/秒
数值监控	Outpkg	出包量	个/秒
数值监控	Connum	公网连接数	个/分钟
数值监控	NewConn	新增连接数	个/分钟

购买指南
计费概述

本文介绍负载均衡 CLB 的计费组成。

费用组成

负载均衡（CLB）的费用由两部分组成：CLB 实例费用、公网网络费用。

实例类型	实例费用	公网网络费用	说明
公网	✓	✓	在 CLB 上收取实例费用和公网网络费用。
内网	—	—	不收取实例费用和公网网络费用。

实例费用

负载均衡根据 IP 版本不同，分为 IPv4、IPv6 和 IPv6 NAT64 版本。其中IPv4 和 IPv6 版本的负载均衡实例可在购买页直接购买并支付实例费用，IPv6 NAT64 版本的负载均衡需在负载均衡控制台对 IPv6 实例进行转换并收取实例费用。

公网网络费用

负载均衡支持按流量计费的公网网络费用计费模式，每小时结算一次。带宽上限为2Gbps。

购买方式

本文介绍购买 CLB 负载均衡的具体操作。

1. 登录云控制台，选择【云产品】>【负载均衡】进入负载均衡控制台，单击左侧导航栏的【LB 实例列表】。
2. 在“LB 实例列表”页面，单击左上角的【新建】。
3. 在“负载均衡 CLB”购买页面，选择以下配置，单击【确认开通】。

参数	说明
地域	选择负载均衡实例的所属地域。
实例类型	仅支持应用型负载均衡。
网络类型	根据业务场景选择配置对外公开或对内私有的负载均衡服务，系统会根据您的选择分配公网或内网服务地址。 - 公网：公网负载均衡收取实例费和公网网络费。 - 内网：内网负载均衡免费。
可用区类型	分为单可用区和多可用区。多可用区分为主可用区和备可用区，主可用区是当前承载流量的可用区，备可用区默认不承载流量，主可用区不可用时才使用。为提高业务的高可用，建议选择多可用区。
IP 版本	可以选择 IPv4 或 IPv6 版本。
网络	选择一个私有网络 VPC。
实例规格	仅内网 IPv4 负载均衡支持选择实例规格，分为共享型和独占型。独占实例存在于您独占的物理集群上，不与其他用户共享集群。
所属运营商	支持电信、联通、移动运营商。
公网带宽	仅支持按流量计费模式。
带宽上限	带宽上限为2Gbps。
实例名	可选择创建后命名或立即命名。
购买数量	选择您需要购买的实例个数。

快速入门
负载均衡快速入门

负载均衡支持 TCP/UDP/HTTP/HTTPS 协议，提供基于域名和 URL 路径的灵活转发能力。本文将引导您如何快速使用IPv4负载均衡。

前提条件

1. 负载均衡只负责转发流量，不具备处理请求的能力。因此，您需要有处理用户请求的云服务器实例。
2. 在本示例中，只要具有两台云服务器实例即可，您也可以自行规划云服务器数量。本例中已经在一个地域下创建了云服务器实例 rs-1 和 rs-2 。
3. 本文以 HTTP 转发为例，云服务器上必须部署相应的 Web 服务器，如 Apache、Nginx、IIS 等。
   为了验证结果，示例在 rs-1 上部署了 Apache 并返回一个带有 “Hello Tomcat! This is rs-1!” 的 HTML，在 rs-2 上部署了 Apache 并返回一个带有 “Hello Tomcat! This is rs-2!” 的 HTML。更多云服务器部署内容，请参考 Linux（CentOS）下部署 Java Web 及 Windows 下安装配置 PHP。
4. 访问云服务器的公网 IP+路径，若显示结果为您部署好的页面，则表示服务部署成功。

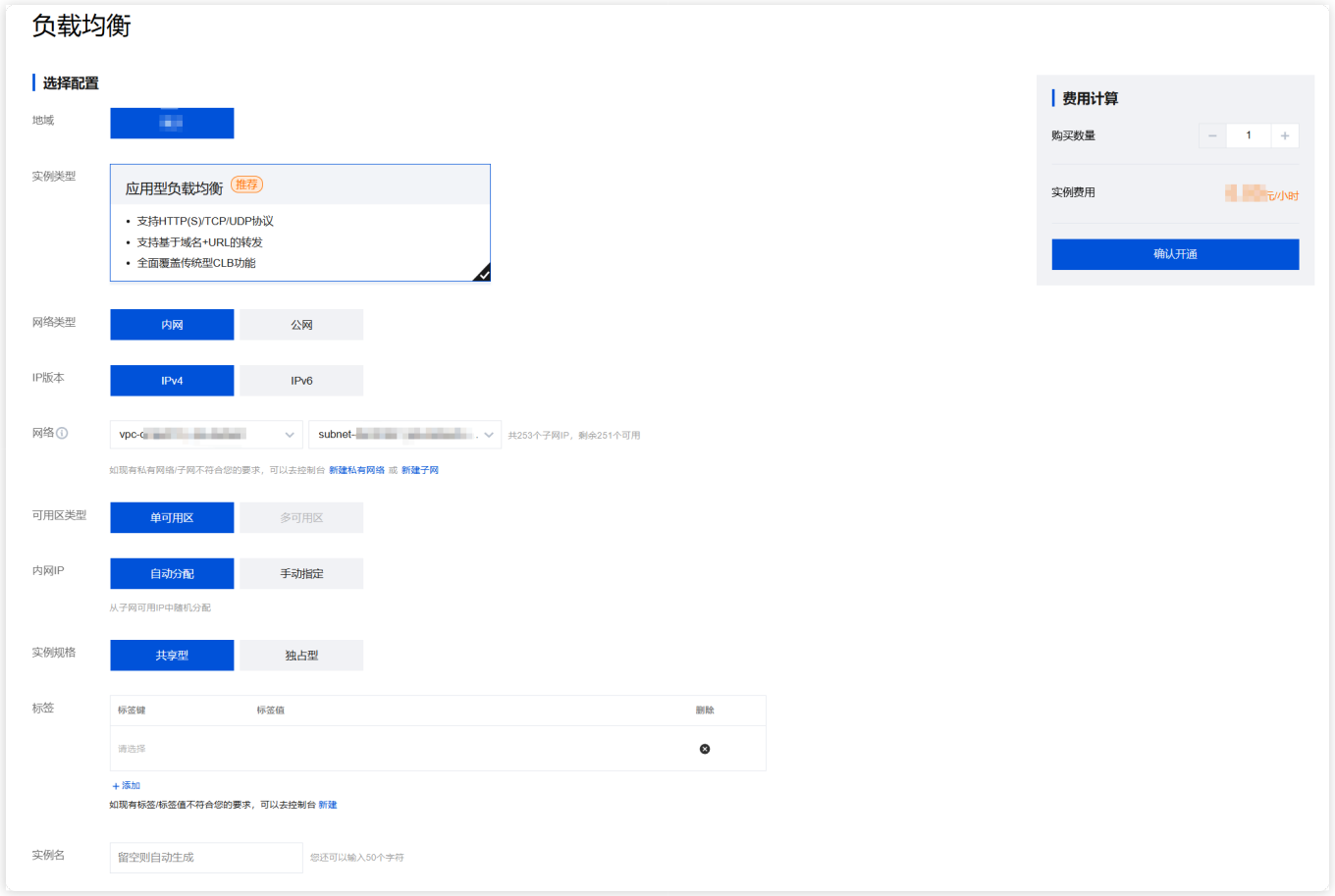
> 注意：
>
> 本示例中后端服务器部署的服务返回值不同，仅用于功能验证。实际情况下，为保持所有用户均有一致体验，后端服务器上一般是部署完全相同的服务。

创建负载均衡实例

1. 登录负载均衡控制台。

2. 选择地域，单击【新建】，进入负载均衡配置页面。

3. 配置负载均衡实例相关参数，本文配置举例如图所示，具体请根据实际情况配置。



> 说明：
>
> 公网IPv4负载均衡【所属运营商】支持多运营商选择，例如电信、联通、移动、外网CAP，您可根据实际情况进行设置。

4. 单击【确认开通】。成功创建实例后，在列表中可看到新建的实例。

创建负载均衡监听器

负载均衡监听器通过指定协议及端口来负责实际转发。本文以负载均衡转发客户端的 HTTP 请求配置为例。

配置 HTTP 监听协议和端口

1. 登录负载均衡控制台。
2. 在“LB 实例列表”页面中，找到已创建的负载均衡实例 clb-test ，单击实例 ID，进入负载均衡详情页。
3. 在“基本信息”模块，可以单击名称后的修改图标修改实例名称。
4. 在“监听器管理”中的【HTTP/HTTPS 监听器】下，单击【新建】，新建负载均衡监听器。

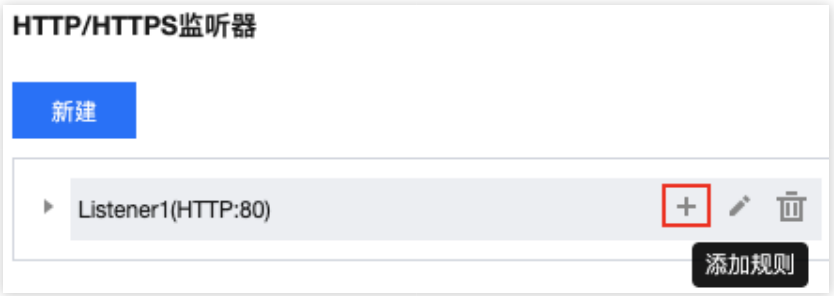
5. 在弹出的对话框中，配置以下参数，完成后单击【确定】。

参数	说明
名称	监听器名称。本示例中可自定义为“Listener1”。
监听器协议	监听器的协议和监听端口。 - 监听协议包含 HTTP 和 HTTPS，本例选择 HTTP。 - 监听端口是用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。其中，843、1020、1433、1434、3306、3389、6006、20000、36000、42222、48369、56000、65010端口为系统保留端口，暂不对外开放。 - 同一个负载均衡实例内，监听端口不可重复。
默认域名	可选择开启或关闭。 - 开启：当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名。 - 如果您的七层监听器已配置默认域名，未匹配其他规则的客户端请求会被转发到默认域名。

参数	说明
	- 如果您的七层监听器未配置默认域名，未匹配其他规则的客户端请求则会被转发到 CLB 加载的第一个域名，由于加载顺序与控制台配置顺序可能不一致，因此不一定是控制台配置的第一个。 - 关闭：当客户端请求没有匹配本监听器的任何域名时，请求将无法被转发。

配置监听器的转发规则

1. 在“监听器管理”中，选中新建的监听器 Listener1，单击【 + 】，开始添加规则。



2. 在弹出的转发规则对话框中，设置域名、URL 路径和均衡方式等基本配置信息，单击【下一步：健康检查】。
   - 域名：您的后端服务所使用的域名，本例使用 www.qcloudtest.com 。域名支持通配符，详情请参见 配置说明。
   - URL 路径：您的后端服务的访问路径，本例使用 /image/ 。
   - 均衡方式选择【按权重轮询】。

3. 配置健康检查：开启健康检查，检查域名使用默认的转发域名和转发路径，单击【下一步：会话保持】。

参数	说明
健康检查	可开启或关闭健康检查功能。建议您开启健康检查，帮助您自动检查并移除异常的后端 CVM 端口。
检查域名	健康检查域名： - 长度限制：1 - 80个字符。 - 默认为转发域名。 - 不支持正则表达式，当您的转发域名为通配域名时，需要指定某一固定域名（非正则）为健康检查域名。 - 支持的字符集为：a-z 0-9 . -。
检查目录	健康检查路径可设置为后端服务器根目录或指定的 URL： - 长度限制：1 - 200个字符。 - 默认为 /，且必须以 / 开头。 - 不支持正则表达式，建议指定某个固定 URL 路径（静态页面）进行健康检查。 - 支持的字符集为：a-z A-Z 0-9 . - _ / = ?。
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒。

参数	说明
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次。
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次。
HTTP 请求方式	健康检查的 HTTP 请求方式，可选：GET 或 HEAD，默认为 GET。 - 若使用 HEAD 方法，服务器仅返回 HTTP 头部信息，可降低后端开销，提升请求效率，对应的后端服务需支持 HEAD。 - 若使用 GET 方法，则后端服务支持 GET 即可。
正常状态码	当状态码为所选状态码时，认为后端服务器存活，即健康检查正常。可选：http_1xx、http_2xx、http_3xx、http_4xx 和 http_5xx，支持选择多个状态码。

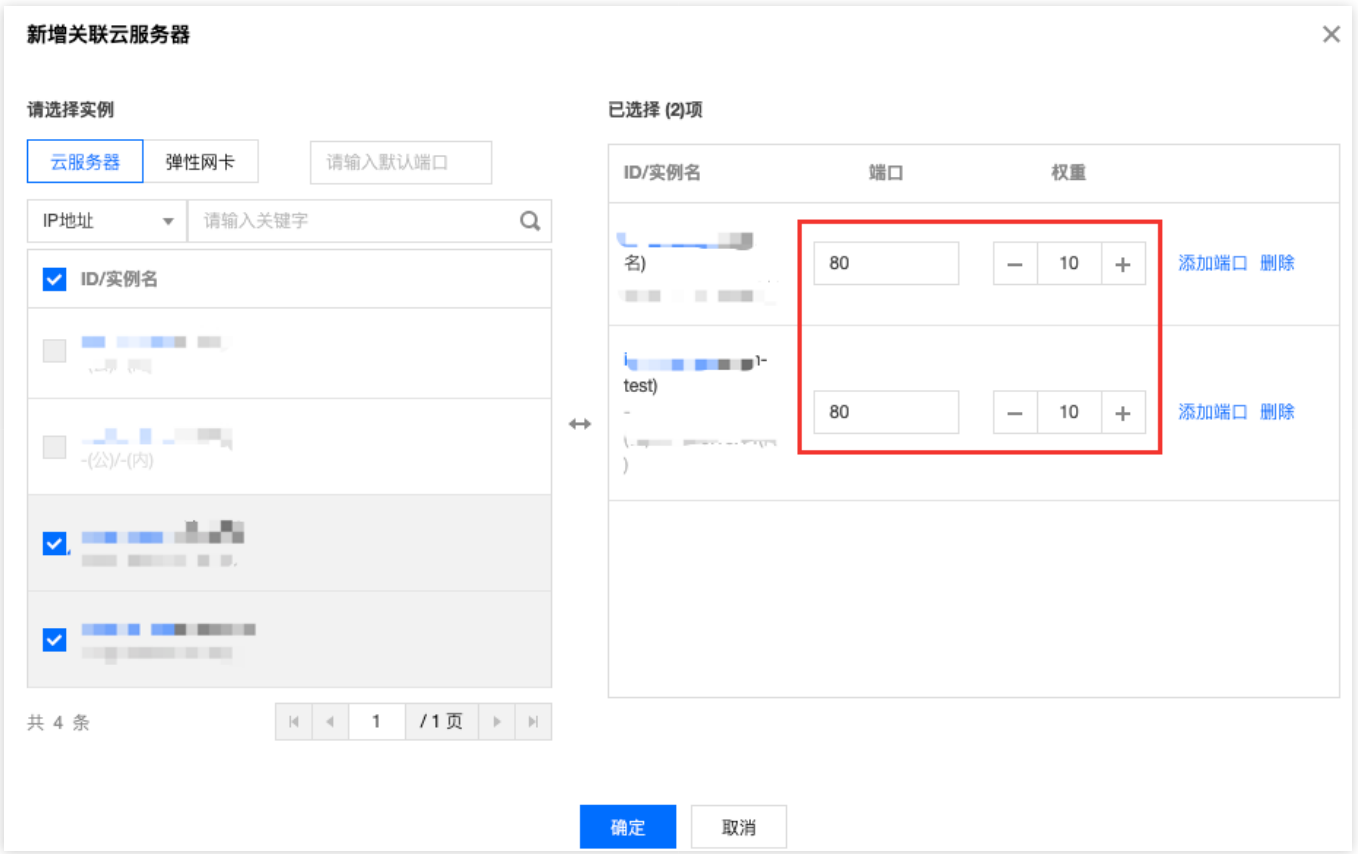
4. 会话保持：开启会话保持，设置保持时间，单击【提交】完成监听器转发规则的配置。
   有关负载均衡监听器的更多内容，请参考 负载均衡监听器概述。

> 注意：
>
> - 一个监听器（即监听协议：端口）可以配置多个域名，一个域名下可以配置多条 URL 路径，选中监听器或域名，单击【+】号即可创建新的规则。
> - 会话保持：如果用户关闭会话保持功能，选择轮询的方式进行调度，则请求依次分配到不同后端服务器上；如果用户开启会话保持功能，或关闭会话保持功能但选择 IP Hash 的调度方式，则请求持续分配到同一台后端服务器上。

绑定云服务器

1. 在“监听器管理”页面，选中新创建的监听器旁的三角图标展开监听器 Listener1，依次选中并展开域名、URL 路径，屏幕右侧区域显示 URL 路径绑定的云服务器信息，在此单击【绑定】。

2. 在弹出框中，选择与 CLB 同地域下的云服务器实例 rs-1 和 rs-2 ，设置云服务器端口均为“80”，云服务器权重均为默认值“10”。



3. 单击【确定】，完成绑定。
4. 展开监听器到 URL 路径维度，可以查看绑定的云服务器和其健康检查状态，当状态为“健康”时表示云服务器可以正常处理负载均衡转发的请求。

> 注意：
>
> 一条转发规则（监听协议 + 端口 + 域名 + URL 路径）可以绑定同一台云服务器的多个端口。如用户在 rs-1 的 80 和 81 端口部署了一样的服务，则 CLB 支持示例中的转发规则同时绑定 rs-1 的 80 和 81 端口，两个端口都会接收到 CLB 转发的请求。

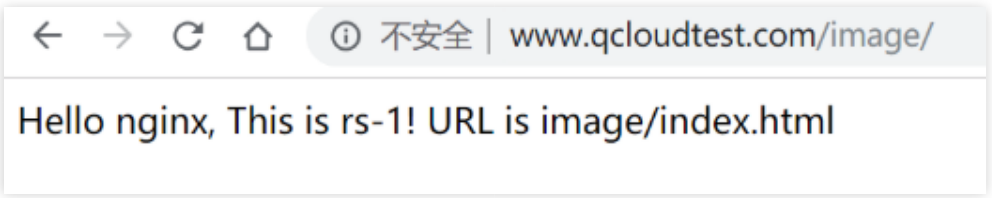
验证负载均衡服务

配置完成负载均衡后，可以验证该架构是否生效，即验证通过一个 CLB 实例下不同的 域名+URL 访问不同的后端云服务器，也即验证内容路由（content-based routing）的功能。

方法一：配置 hosts 将域名指向 CLB

1. 在 Windows 系统中，进入 C:\Windows\System32\drivers\etc 目录，修改 hosts 文件，把域名映射到 CLB 实例的 VIP 上。

2. 为了验证 hosts 是否配置成功，可以运行 cmd，用 ping 命令探测一下该域名是否成功绑定了 VIP，如有数据包，则证明绑定成功。
3. 在浏览器中输入访问路径 http://www.qcloudtest.com/image/ ，测试负载均衡服务。如下图所示，则表示本次请求被 CLB 转发到了 rs-1 这台 CVM 上，CVM 正常处理请求并返回。



4. 此监听器的轮询算法是“按权重轮询”，且两台 CVM 的权重都是“10”，刷新浏览器，再次发送请求，可以看到本次请求被 CLB 转发到了 rs-2 这台 CVM 上。

> 注意：
>
> image/ 后面 / 必须保留，代表 image 是默认的目录，而不是名为 image 的文件。

方法二：配置云解析将域名指向 CLB

1. 登录云控制台，单击【云产品】>【域名服务】>【VPCDNS】。
2. 单击您所购买的【域名】，在【域名解析管理】页面单击【添加记录】按钮，为域名添加 A 记录，输入以下内容：
   - 记录类型： A记录 。
   - 主机记录：即域名前缀。本例以解析所有前缀为例，设为 *.qcloudtest.com 。
   - 记录值：填写负载均衡 IP 地址。
   - 权重：设置为默认值“100”。
3. 添加完毕后，单击【确定】。
   域名解析将该记录在 Internet 上传播需要一段时间。为测试域名是否解析正常，可以在添加完解析记录一段时间后，直接访问绑定后的 CNAME 域名（如本例中的 www.qcloudtest.com ）来验证负载均衡。

IPv6 负载均衡快速入门

负载均衡支持 IPv4、IPv6 和 IPv6 NAT64 三个 IP 版本，IPv6 负载均衡支持 TCP/UDP/HTTP/HTTPS 协议，提供基于域名和 URL 路径的灵活转发能力。本文将引导您如何快速使用 IPv6 负载均衡。

前提条件

1. 负载均衡只负责转发流量，不具备处理请求的能力。因此，您需要首先搭建处理用户请求的云服务器实例，并完成云服务器的 IPv6 配置。有关如何创建云服务器实例并启用 IPv6，请参见 快速搭建 IPv6 私有网络。
2. 本文以 HTTP 转发为例，云服务器上必须部署相应的 Web 服务器（如 Apache、Nginx、IIS 等），同时 Web 服务使用的端口需要监听 IPv6。

使用说明

- IPv6 负载均衡支持获取客户端 IPv6 源地址。
- 四层 IPv6 负载均衡支持直接获取客户端 IPv6 源地址。
- 七层 IPv6 负载均衡支持通过 HTTP 的 X-Forwarded-For 头域获取客户端 IPv6 源地址。
- 当前 IPv6 负载均衡是纯公网负载均衡，相同 VPC 的客户端无法通过内网访问该 IPv6 负载均衡。

步骤1：搭建云服务器并配置 IPv6

1. 登录云服务器控制台，完成 IPv6 的基础配置，详细操作请参见 快速搭建 IPv6 私有网络。

2. 在云服务器中，依次执行如下命令，部署并重启 Nginx 服务。

```
yum install nginx
service nginx restart
```

3. 查看部署在云服务器上的 Nginx 服务是否已经监听 IPv6。

   i. 执行如下命令进行查看。

```
netstat -tupln
```

```
[root@VM_0_14_centos ~]# netstat -tupln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      4314/nginx: master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      3175/sshd
tcp6       0      0 :::80                   :::*                    LISTEN      4314/nginx: master
udp        0      0 0.0.0.0:68              0.0.0.0:*                           2890/dhclient
udp        0      0 10.24.0.14:123          0.0.0.0:*                           3369/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*                           3369/ntpd
udp        0      0 0.0.0.0:56713           0.0.0.0:*                           4333/ntpdate
udp6       0      0 fe80::5054:ff:fe3d::546 :::*                                4119/dhclient
udp6       0      0 2402:4e00:1400:1217:123 :::*                                3369/ntpd
udp6       0      0 fe80::5054:ff:fe3d::123 :::*                                3369/ntpd
udp6       0      0 ::1:123                 :::*                                3369/ntpd
```

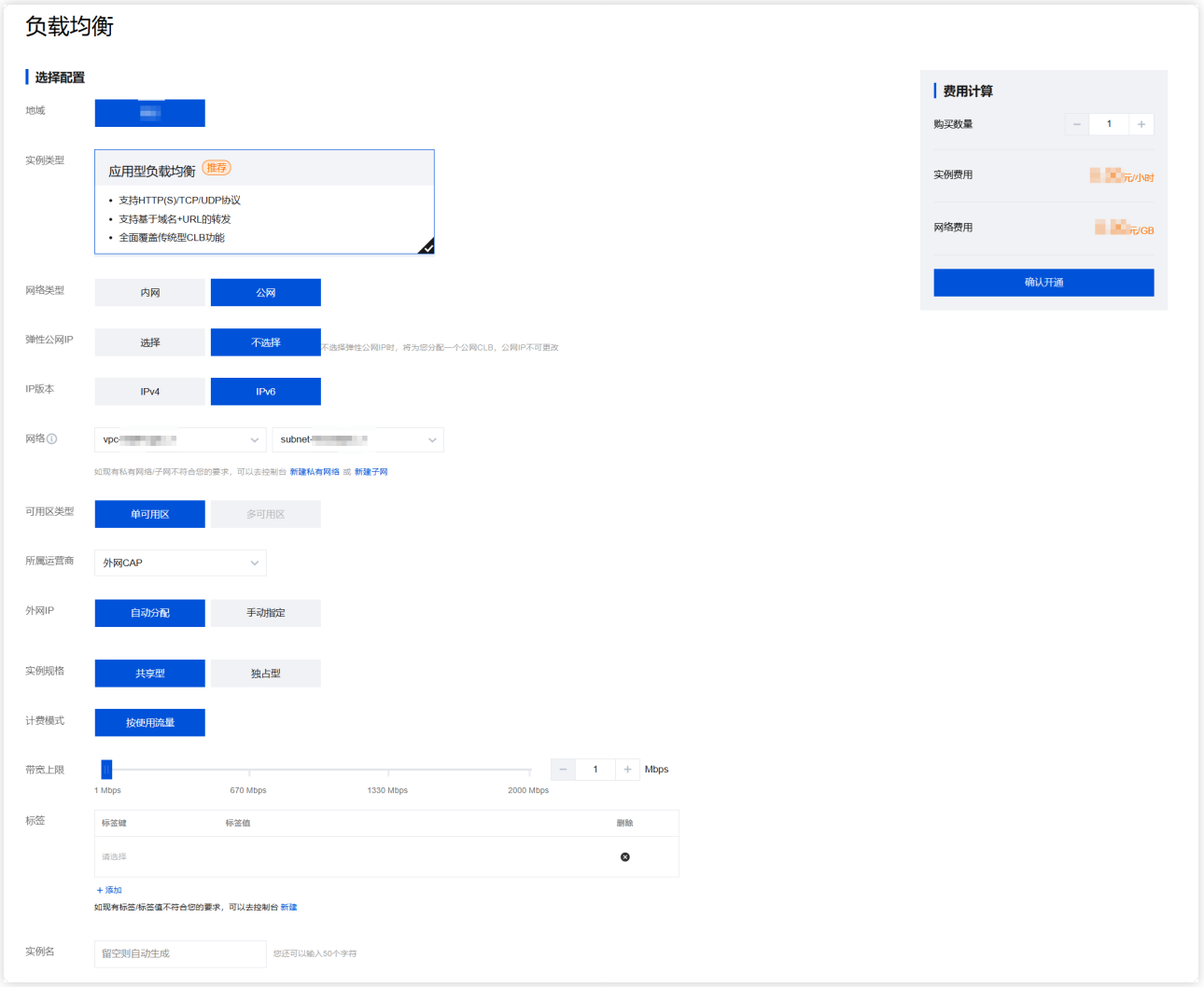
2. 执行如下命令，打开 Nginx 配置文件进行查看。

vim /etc/nginx/nginx.conf

```
    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/ngx_core_module.html#include
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    server {
        listen       80 default_server;
        listen       [::]:80 default_server;
        server_name  _;
        root         /usr/share/nginx/html;

        # Load configuration files for the default server block.
        include /etc/nginx/default.d/*.conf;

        location / {
        }

        error_page 404 /404.html;
            location = /40x.html {
        }

        error_page 500 502 503 504 /50x.html;
            location = /50x.html {
        }
    }

# Settings for a TLS enabled server.
#
#    server {
#        listen       443 ssl http2 default_server;
#        listen       [::]:443 ssl http2 default_server;
#        server_name  _;
#        root         /usr/share/nginx/html;
#
#        ssl_certificate "/etc/pki/nginx/server.crt";
#        ssl_certificate_key "/etc/pki/nginx/private/server.key";
#        ssl_session_cache shared:SSL:1m;
```

步骤2：创建 IPv6 负载均衡实例

1. 登录负载均衡控制台。
2. 在“LB实例列表”页面，单击【新建】进入负载均衡实例购买页面。
3. 在【负载均衡】实例购买页面，设置【网络类型】为【公网】，【可用区类型】为【单可用区】，【IP版本】为【IPv6】，【网络】请务必选择已经获取IPv6 CIDR的私有网络和子网，【所属运营商】为【外网CAP】。实例名和购买数量您选择默认或按需配置均可。然后单击【确认开通】。



4. 在【LB实例列表】即可看到新建的实例。

步骤3：创建 IPv6 负载均衡监听器

配置 HTTP 监听协议和端口

1. 在【LB实例列表】页面，选择已创建的负载均衡实例，单击实例ID，进入负载均衡详情页。
2. 在【基本信息】模块，可以单击名称后的修改图标修改实例名称。

3. 在【监听器管理】中的【HTTP/HTTPS 监听器】下，单击【新建】，新建负载均衡监听器。
4. 在弹出的对话框中，配置以下参数，完成后单击【确定】。

参数	说明
名称	监听器名称。本示例中可自定义为“Listener1”。
监听器协议	监听器的协议和监听端口。 - 监听协议包含 HTTP 和 HTTPS，本例选择 HTTP。 - 监听端口是用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。其中，843、1020、1433、1434、3306、3389、6006、20000、36000、42222、48369、56000、65010端口为系统保留端口，暂不对外开放。 - 同一个负载均衡实例内，监听端口不可重复。
默认域名	可选择开启或关闭。 - 开启：当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名。 - 如果您的七层监听器已配置默认域名，未匹配其他规则的客户端请求会被转发到默认域名。 - 如果您的七层监听器未配置默认域名，未匹配其他规则的客户端请求则会被转发到 CLB 加载的第一个域名，由于加载顺序与控制台配置顺序可能不一致，因此不一定是控制台配置的第一个。 - 关闭：当客户端请求没有匹配本监听器的任何域名时，请求将无法被转发。

配置监听器的转发规则

1. 在【监听器管理】中，选中刚才新建的监听器 IPv6test，单击【＋】，弹出【创建HTTP/HTTPS转发规则】对话框。
2. 在弹出的转发规则对话框中，设置域名、URL 路径和均衡方式等基本配置信息，单击【下一步：健康检查】。
   - 域名：您的后端服务所使用的域名，本例使用 www.qcloudtest.com 。域名支持通配符，详情请参见 配置说明。
   - URL 路径：您的后端服务的访问路径，本例使用 /image/ 。
   - 均衡方式选择【按权重轮询】。

3. 配置健康检查：开启健康检查，检查域名使用默认的转发域名和转发路径，单击【下一步：会话保持】。

4. 会话保持：开启会话保持并配置保持时间，单击【提交】。
   有关负载均衡监听器的更多内容，请参见 负载均衡监听器概述。

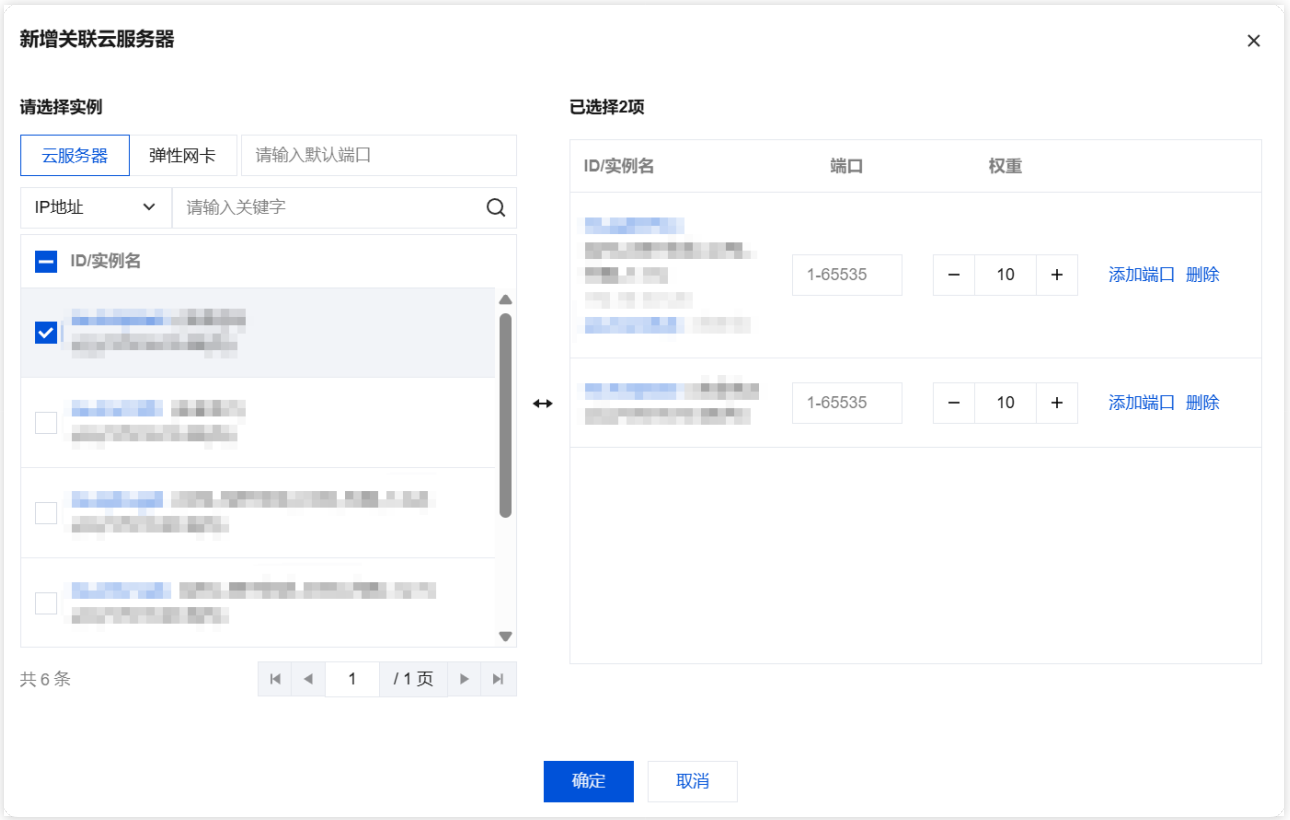
   > 说明：
   >
   > - 一个监听器（即监听协议：端口）可以配置多个域名，一个域名下可以配置多条 URL 路径，选中监听器或域名，单击【+】即可创建新的规则。
   > - 会话保持：如果用户关闭会话保持功能，选择轮询的方式进行调度，则请求依次分配到不同后端服务器上；如果用户开启会话保持功能，或关闭会话保持功能但选择 ip_hash 的调度方式，则请求持续分配到同一台后端服务器上去。

绑定云服务器

1. 在【监听器管理】页面，选中并展开刚才创建的监听器，选中域名、选中 URL 路径，右侧区域框为URL路径已绑定的云服务器 IPv6 信息列表，新增绑定请单击【绑定】。

2. 在弹框中，勾选需要绑定的云服务器，并设置云服务器的 Nginx 服务默认端口为80，设置权重（默认值10），单击【确定】。

   > 说明：
   >
   > CLB绑定的ENI时，ENI必须绑定在CVM上；没有绑定CVM的ENI不能被CLB绑定。



3. 成功绑定云服务器后：
   - 请确认端口状态是否为【健康】，如果为【健康】，请进行 步骤4：测试 IPv6 负载均衡。

   - 如果端口状态为【异常】，请确定监听器是否绑定了正确的云服务器的 Nginx 服务端口，同时登录云服务器检查端口已经正常监听 IPv6，可参见 步骤1中的第3步 进行查看。

步骤4：测试 IPv6 负载均衡

配置完成 IPv6 负载均衡后，可以验证该架构是否生效，即验证通过一个 CLB 实例下不同的域名 + URL 访问不同的后端云服务器，也即验证内容路由（content-based routing）的功能是否可用。

使用具有 IPv6 公网能力的客户端，访问域名或者负载均衡的 IPv6 地址，如果能够正常访问云服务器的 Web 服务，则表明 IPv6 负载均衡工作正常，示例步骤如下：

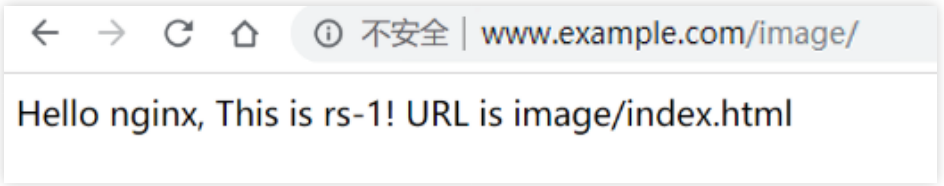
1. 在 Windows 系统中，进入 C:\Windows\System32\drivers\etc 目录，修改 hosts 文件，将域名映射到 CLB 实例的 VIP 上。

```
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
1                   www.example.com
```

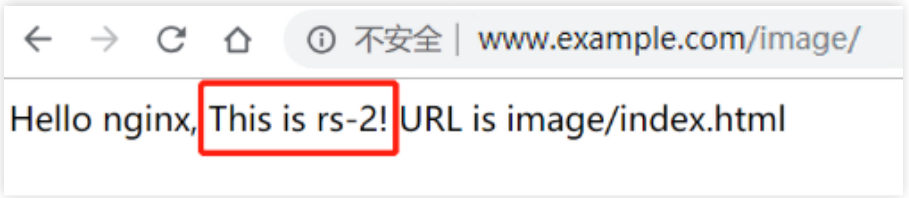
2. 为了验证 hosts 是否配置成功，可以运行 cmd，用 ping 命令探测一下该域名是否成功绑定了 VIP，如有数据包，则证明绑定成功。

```
C:\Users\v        >ping www.example.com

正在 Ping www.example.com [1              ] 具有 32 字节的数据:
来自 1              的回复: 字节=32 时间=7ms TTL=46
来自 1              的回复: 字节=32 时间=7ms TTL=46
来自 1              的回复: 字节=32 时间=7ms TTL=46
来自 1              的回复: 字节=32 时间=7ms TTL=46

1              的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 7ms, 最长 = 7ms, 平均 = 7ms
```

3. 在浏览器中输入访问路径 http://www.example.com/image/ ，测试负载均衡服务。如下图所示，则表示本次请求被 CLB 转发到了 rs-1 这台 CVM 上，CVM 正常处理请求并返回。



4. 此监听器的轮询算法是“按权重轮询”，且两台 CVM 的权重都是“10”，刷新浏览器，再次发送请求，可以看到本次请求被 CLB 转发到了 rs-2 这台 CVM 上。



> 说明：
>
> image/ 后 / 必须保留，代表 image 是默认的目录，而不是名为 image 的文件。

CentOS下部署Nginx

软件版本

本文在示例步骤中的软件版本如下，在实际操作时，请您以实际软件版本为准。

- 操作系统：CentOS 7.5
- Nginx 版本：Nginx 1.16.1

安装 Nginx

1. 购买完成后，在云服务器的详情页面，单击【登录】，可以直接登录云服务器，输入自己的用户名密码后，开始搭建 Nginx 环境。有关如何创建云服务器实例，请参见 创建云服务器实例。

   ```
   # 安装 Nginx：
   yum -y install nginx
   # 查看 Nginx 版本
   nginx -v
   # 查看 Nginx 安装目录
   rpm -ql nginx
   # 启动 Nginx
   service nginx start
   ```

2. 访问该云服务器的公网 IP 地址，出现如下页面则表示 Nginx 部署完成。

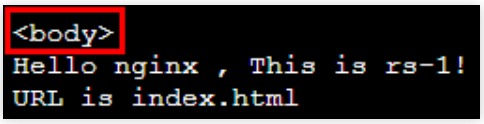
3. Nginx 的默认根目录 root 是 /usr/share/nginx/html ，直接修改 html 下的 index.html 静态页面，用来标识这个页面的特殊性，相关操作如下：

i. 执行如下命令，进入html 下的 index.html 静态页面：

bash
vim /usr/share/nginx/html/index.html

ii. 按“i”进入编辑模式，请在 <body></body> 标签内输入：

建议直接在<body>下方输入
Hello nginx , This is rs-1!
URL is index.html



3. 按 “Esc”，输入 :wq 保存编辑。

4. 负载均衡（原“应用型负载均衡”）可以根据后端服务器的路径来进行请求转发，在 /image 路径下部署静态页面，相关操作如下：

i. 依次执行如下命令，新建目录 image 并进入该目录：

mkdir /usr/share/nginx/html/image
cd /usr/share/nginx/html/image

ii. 执行如下命令，在 image 目录下创建 index.html 静态页面：

vim index.html

iii. 按“i”进入编辑模式，在页面中输入：

Hello nginx , This is rs-1!
URL is image/index.html

iv. 按 “Esc”，输入 :wq 保存编辑。

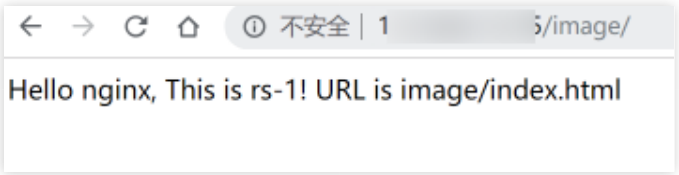
> 注意：
>
> Nginx 的默认端口是 80 ，如果想修改端口请修改配置文件并重启 Nginx。

验证 Nginx 服务

访问云服务器的公网 IP + 路径，如果可以显示出已部署好的静态页面，则证明 Nginx 部署成功。

- rs-1 的 index.html 页面：

- rs-1 的 /image/index.html 页面：



CentOS下部署Java Web

软件版本

本文在示例步骤中的软件版本如下，在实际操作时，请您以实际软件版本为准。

- 操作系统：CentOS 7.5
- Tomcat 版本：apache-tomcat-8.5.39
- JDK 版本：JDK 1.8.0_201

安装JDK

购买负载均衡服务后，在云服务器的详情页面，单击【登录】，可以直接登录云服务器，输入自己的用户名密码后，开始搭建 Java Web 环境。有关如何创建云服务器实例，请参见 云服务器-创建实例。

下载 JDK

输入如下命令：

```
mkdir /usr/java  # 创建 java 文件夹
cd /usr/java     # 进入 java 文件夹
```

```
# 上传 JDK 安装包（推荐）
推荐您使用  或其他工具将 JDK 安装包上传到上述 java 文件夹下，然后解压安装包。
或者
# 直接使用命令（推荐您使用上传 JDK 安装包的方法）： wget 下载链接，下载得到的压缩包无法解压，这是因为直接下载的压缩包默认没有接受 Oracle BSD 许可；每个人的 cookie 不一样，请前往https://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html页面同意许可协议并获取带有自己 cookie 的下载链接。
wget --no-check-certificate --no-cookies --header "Cookie: oraclelicense=accept-securebackup-cookie" https://download.oracle.com/otn-pub/java/jdk/8u201-b09/42970487e3af4f5aa5bca3f542482c60/jdk-8u201-linux-x64.tar.gz
```

```
# 解压
chmod +x jdk-8u201-linux-x64.tar.gz
tar -xzvf jdk-8u201-linux-x64.tar.gz
```

设置环境变量

1. 打开 /etc/profile 文件。

vi /etc/profile

2. 按下 i 键进入编辑模式，在该文件中添加如下信息。

```
# set java environment
export JAVA_HOME=/usr/java/jdk1.8.0_201
export CLASSPATH=$JAVA_HOME/lib/tools.jar:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib
export PATH=$JAVA_HOME/bin:$PATH
```

3. 按下 Esc 键退出编辑模式，输入 :wq 保存并关闭文件。

4. 加载环境变量。

source /etc/profile

查看 JDK 是否安装成功

运行 java -version 命令，显示 JDK 版本信息时，表示 JDK 已经安装成功。

```
[root@emma /]# java -version
java version "1.8.0_201"
Java(TM) SE Runtime Environment (build 1.8.0_201-b09)
Java HotSpot(TM) 64-Bit Server VM (build 25.201-b09, mixed mode)
```

安装 Tomcat

下载 Tomcat

输入如下命令：

```
# 镜像地址会改变，Tomcat 版本也会不断升级。如果下载链接失效，请您到 [Tomcat 官网](https://tomcat.apache.org/download-80.cgi)选择合适的安装包地址。
wget http://mirrors.tuna.tsinghua.edu.cn/apache/tomcat/tomcat-8/v8.5.39/bin/apache-tomcat-8.5.39.tar.gz
tar -xzvf apache-tomcat-8.5.39.tar.gz
mv apache-tomcat-8.5.39 /usr/local/tomcat/
```

在 /usr/local/tomcat/ 目录中包含如下文件：

- bin：脚本文件，包含启动和关闭 Tomcat 服务脚本。
- conf：各种全局配置文件，其中最重要的是 server.xml 和 web.xml。
- webapps：Tomcat 的主要 Web 发布目录，默认情况下把 Web 应用文件放于此目录。
- logs：存放 Tomcat 执行时的日志文件。

> 注意：
>
> 如果下载链接失效，请替换为 Tomcat 官网 的最新下载链接。

添加用户

```
# 创建一般用户 www来运行Tomcat
useradd www
# 创建网站根目录
mkdir -p /data/wwwroot/default
# 将需要部署的 Java Web 项目文件 WAR 包上传到网站根目录下，然后将网站根目录下文件权限改为 www。本示例将直接在网站根目录下新建一个 Tomcat 测试页面：
echo Hello Tomcat! > /data/wwwroot/default/index.jsp
chown -R www.www /data/wwwroot
```

设置 JVM 内存参数

1. 创建一个 /usr/local/tomcat/bin/setenv.sh 脚本文件。

   ```
   vi /usr/local/tomcat/bin/setenv.sh
   ```

2. 按下 i 键进入编辑模式，添加如下内容。

   ```
   JAVA_OPTS='-Djava.security.egd=file:/dev/./urandom -server -Xms256m -Xmx496m -Dfile.encoding=UTF-8'
   ```

3. 按 Esc 键退出编辑模式，输入 :wq 保存并退出编辑。

配置 server.xml

1. 切换到 /usr/local/tomcat/conf/ 目录。

   ```
   cd /usr/local/tomcat/conf/
   ```

2. 备份 server.xml 文件。

   ```
   mv server.xml server_default.xml
   ```

3. 创建一个新的 server.xml 文件。

   ```
   vi server.xml
   ```

4. 按下 i 键进入编辑模式，添加如下内容。

```
<?xml version="1.0" encoding="UTF-8"?>
<Server port="8006" shutdown="SHUTDOWN">
<Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
<Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
<Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener"/>
<Listener className="org.apache.catalina.core.AprLifecycleListener"/>
<GlobalNamingResources>
<Resource name="UserDatabase" auth="Container"
 type="org.apache.catalina.UserDatabase"
 description="User database that can be updated and saved"
 factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
 pathname="conf/tomcat-users.xml"/>
</GlobalNamingResources>
<Service name="Catalina">
<Connector port="8080"
 protocol="HTTP/1.1"
 connectionTimeout="20000"
 redirectPort="8443"
 maxThreads="1000"
 minSpareThreads="20"
 acceptCount="1000"
 maxHttpHeaderSize="65536"
 debug="0"
 disableUploadTimeout="true"
 useBodyEncodingForURI="true"
 enableLookups="false"
 URIEncoding="UTF-8"/>
<Engine name="Catalina" defaultHost="localhost">
<Realm className="org.apache.catalina.realm.LockOutRealm">
<Realm className="org.apache.catalina.realm.UserDatabaseRealm"
  resourceName="UserDatabase"/>
</Realm>
<Host name="localhost" appBase="/data/wwwroot/default" unpackWARs="true" autoDeploy="true">
<Context path="" docBase="/data/wwwroot/default" debug="0" reloadable="false" crossContext="tru
e"/>
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
prefix="localhost_access_log." suffix=".txt" pattern="%h %l %u %t &amp;quot;%r&amp;quot; %s %b" />
</Host>
</Engine>
</Service>
</Server>
```

5. 按 Esc 键退出编辑模式，输入 :wq 保存并退出编辑。

启动 Tomcat

方法一

进入 Tomcat 服务器的 bin 目录，然后执行 ./startup.sh 命令启动 Tomcat 服务器。

```
cd /usr/local/tomcat/bin
./startup.sh
```

运行结果如下：

```
[root@emma bin]# ./startup.sh
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr/java/jdk1.8.0_201
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar
Tomcat started.
```

方法二

1. 设置快捷启动，在任何地方都可以通过 service tomcat start 来启动 Tomcat。

```
wget https://github.com/lj2007331/oneinstack/raw/master/init.d/Tomcat-init
mv Tomcat-init /etc/init.d/tomcat
chmod +x /etc/init.d/tomcat
```

2. 运行以下命令，设置启动脚本 JAVA_HOME。

```
sed -i 's@^export JAVA_HOME=.*@export JAVA_HOME=/usr/java/jdk1.8.0_201@' /etc/init.d/tomcat
```

3. 设置自启动。

```
chkconfig --add tomcat
chkconfig tomcat on
```

4. 启动 Tomcat。

```
# 启动 Tomcat
service tomcat start
# 查看 Tomcat 运行状态
service tomcat status
# 关闭 Tomcat
service tomcat stop
```

运行结果如下：

```
[root@emma bin]# service tomcat start
Tomcat is already running (pid: 27293)
[root@emma bin]# service tomcat status
Tomcat is running with pid: 27293
[root@emma bin]# service tomcat stop
Stoping Tomcat
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr/java/jdk1.8.0_201
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bin/tomcat-juli.jar
waiting for processes to exit
```

5. 若提示没有权限，请切换为 root 用户并修改权限。

```
cd /usr/local
chmod -R 777 tomcat
```

6. 在浏览器地址栏中输入 http://公网IP:端口 （端口为 server.xml 中设置的 connector port ）进行访问。出现下图所示页面时表示安装成功。

配置安全组

如果访问不通，请检查安全组。如上示例中 server.xml 中的 connector port 是 8080，因此需在对应的云服务器所绑定的安全组上放通 TCP:8080。

添加入站规则
类型
来源
协议端口
策略
备注
自定义
0.0.0.0/0
TCP:8080
允许
Tomcat
删除
+ 新增一行
完成
取消

操作指南
负载均衡实例
创建负载均衡实例

本文介绍购买 CLB 负载均衡的具体操作。

1. 登录云控制台，选择【云产品】>【负载均衡】进入负载均衡控制台，单击左侧导航栏的【LB 实例列表】。
2. 在"LB 实例列表"页面，单击左上角的【新建】。
3. 在"负载均衡 CLB"购买页面，选择以下配置，单击【确认开通】。

参数	说明
地域	选择负载均衡实例的所属地域。
实例类型	仅支持应用型负载均衡。
网络类型	根据业务场景选择配置对外公开或对内私有的负载均衡服务，系统会根据您的选择分配公网或内网服务地址。 - 公网：公网负载均衡收取实例费和公网网络费。 - 内网：内网负载均衡免费。
弹性公网 IP	- 不选择弹性公网 IP 时，云平台将为您分配一个公网 CLB，公网 IP 不可更改。 - 选择弹性公网 IP 时，云平台将为您分配一个弹性公网 IP 和一个内网 CLB，EIP 和内网 CLB 支持按需绑定解绑。
IP 版本	可以选择 IPv4 或 IPv6 版本。
网络	选择一个私有网络 VPC。
可用区类型	分为单可用区和多可用区。 多可用区分为主可用区和备可用区，主可用区是当前承载流量的可用区，备可用区默认不承载流量，主可用区不可用时才使用。为提高业务的高可用，建议选择多可用区。
所属运营商	支持电信、联通、移动运营商。
实例规格	内外网 IPv4/IPv6 负载均衡均支持选择实例规格，分为共享型和独占型。 独占实例存在于您指定的物理集群上。
集群标签	内外网 IPv4/IPv6 负载均衡的实例规格为独占集群时，可以选择对应的集群标签。 分为四层集群标签和七层集群标签
本地专有集群	只有在 CDC 场景下才支持。 最终实例是创建在 CDC 的本地专用集群上。

参数	说明
外网IP	如果对实例有特定 IP 要求，可以手工指定 IP 地址，目前支持的 CLB 实例有： - 内外网 IPv4 实例 - 内外网 IPv6 实例
公网带宽	仅支持按流量计费模式。
带宽上限	带宽上限为2Gbps。
标签	选择标签键和标签值，也可选择新建标签，详情请参见创建标签。
实例名	可选择创建后命名或立即命名。
购买数量	选择您需要购买的实例个数。

创建 IPv6 负载均衡实例

概述

IPv6 负载均衡是基于 IPv6 单栈技术实现的负载均衡，和 IPv4 负载均衡协同工作，实现 IPv6/IPv4 双栈通信。IPv6 负载均衡绑定的是云服务器的 IPv6 地址，并对外提供 IPv6 VIP 地址。

IPv6 负载均衡优势

IPv6 负载均衡在助力业务快速接入 IPv6 时具有如下优势：

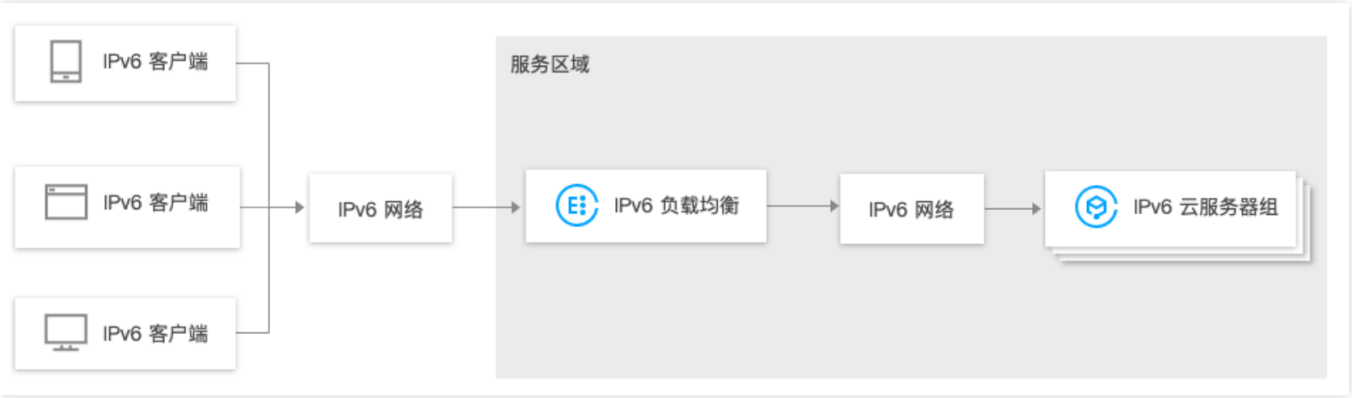
- 快速接入：秒级接入 IPv6，随买随用快速上线。
- 易于使用：IPv6负载均衡兼容原 IPv4 负载均衡的操作流程，零学习成本，低门槛使用。
- 端到端的 IPv6 通信：IPv6 负载均衡和云服务器之间通过 IPv6 通信，可以帮助部署在云服务器的应用快速进行 IPv6 改造，并实现端到端的 IPv6 通信。

IPv6 负载均衡架构

负载均衡支持创建 IPv6 负载均衡（下文中也叫 IPv6 CLB）实例，TCloudFinanceZone会给 IPv6 CLB 实例分配一个 IPv6 公网地址（即 IPv6 版的 VIP），该 VIP 会将来自 IPv6 客户端的请求转发给后端的 IPv6 云服务器。

IPv6 CLB 实例不但可以快速接入 IPv6 公网用户访问，且通过 IPv6 协议和后端云服务器进行通信，能够帮助云上的应用快速改造 IPv6，并实现端到端的 IPv6 通信。

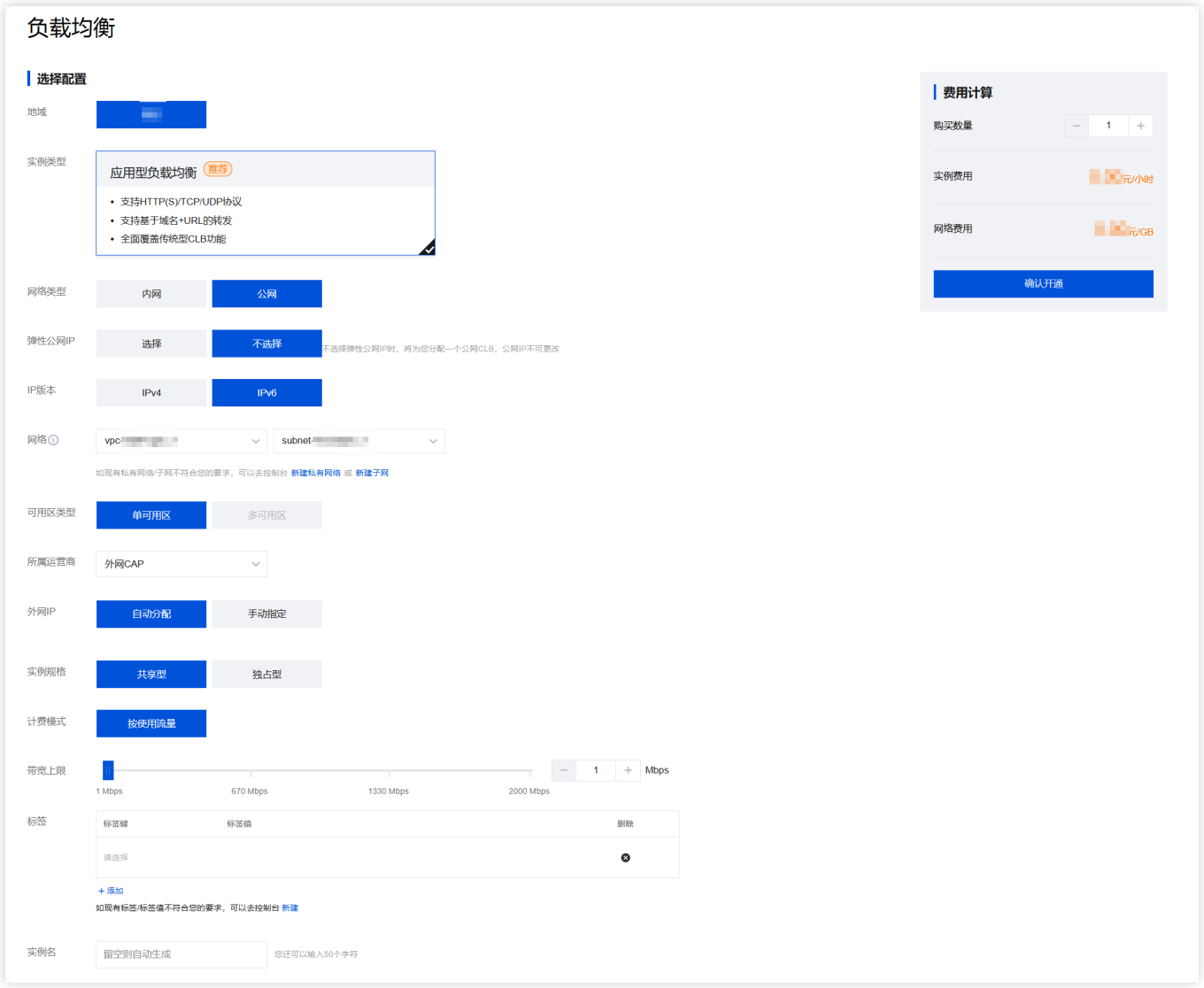
IPv6 负载均衡的架构如下图所示。



操作步骤

1. 登录负载均衡控制台。
2. 在“LB实例列表”页面，单击【新建】进入负载均衡实例购买页面。
3. 在【负载均衡 LB】实例购买界面，设置【网络类型】为【公网】，【可用区类型】为【单可用区】，【IP版本】为【IPv6】，【网络】请务必选择已经获取IPv6 CIDR的私有网络和子网，【所属运营商】为【外网CAP】，计费模式

为按使用流量计费，支持对VIP设置带宽上限，实例名和购买数量您选择默认或按需配置均可。然后单击【确认开通】。



4. 如果对实例有特定 IP 要求，可以手动指定 IP 地址，目前支持的 CLB 实例有：
    - 内网 IPv6 实例
    - 外网 IPv6 实例
5. 在【LB实例列表】即可看到新建的实例。

创建 IPv6 NAT64 负载均衡实例

> 说明：
>
> IPv6 NAT64 负载均衡不支持获取 Client IP。

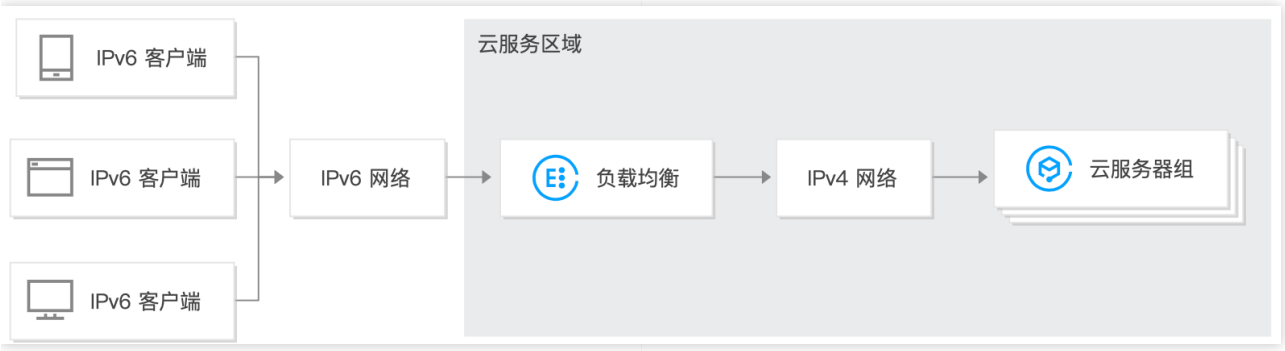
负载均衡支持创建 IPv6 NAT64 负载均衡实例，TCloudFinanceZone会给实例分配一个 IPv6 公网地址（即 IPv6 版的 VIP），该 VIP 会将来自 IPv6 客户端的请求转发给后端的 IPv4 云服务器。

什么是 IPv6 NAT64 负载均衡

IPv6 NAT64 负载均衡是基于 NAT64 IPv6 过渡技术实现的负载均衡器。通过 IPv6 NAT64 负载均衡器，后端云服务器无需做任何 IPv6 改造即可快速接入 IPv6 用户的访问。

IPv6 NAT64 负载均衡架构

IPv6 NAT64 负载均衡的架构如下图所示。



通过 IPv6 网络访问 IPv6 NAT64 负载均衡时，负载均衡能平滑地将 IPv6 地址转换为 IPv4 地址，适配原有的服务，快速实现 IPv6 的改造。

IPv6 NAT64 负载均衡优势

云平台 IPv6 NAT64 负载均衡在助力业务快速接入 IPv6 时具有如下优势：

- **快速接入：**秒级接入 IPv6，随买随用快速上线。
- **业务平滑过渡：**业务仅需改造客户端，无需改造后端服务，便可平滑接入 IPv6。IPv6 NAT64 负载均衡支持来自 IPv6 客户端的访问，并将 IPv6 报文转换成 IPv4 报文，后端云服务器上的应用程序无需感知 IPv6，仍以原有形式部署工作。
- **易于使用：**IPv6 NAT64 负载均衡兼容原 IPv4 负载均衡的操作流量，零学习成本，低门槛使用。

操作指南

创建 IPv6 NAT64 负载均衡

1. 登录负载均衡控制台。
2. 单击左侧导航栏的【IPv6转换实例】，进入【IPv6转换实例】界面。
3. 单击【新建】，系统弹出【申请IPv6转换实例】对话框。
    - 名称：填写实例名称。
    - 可用区：选择负载均衡实例所在可用区。

4. 单击【确定】完成实例创建。

使用 IPv6 NAT64 负载均衡

单击实例 ID，进入详情页，可新建转换规则。

删除负载均衡实例

当您确认负载均衡实例已无流量，不需要继续使用后，您可以通过负载均衡控制台或者 API 将实例删除。
实例删除后将彻底销毁，无法恢复。我们强烈建议您在删除实例之前，先解绑所有后端云服务器并观察一段时间后，再进行删除操作。

通过控制台删除负载均衡实例

1. 登录负载均衡控制台。
2. 找到您想删除的负载均衡实例，单击最右侧操作栏下的【删除】。
3. 弹出最终确认对话框，确认操作安全提示正常后，单击 【确定】即可删除。
   最终确认对话框如下图所示，我们强烈建议您确认绑定规则数为“0”、绑定的云服务器为“无”、操作安全提示为“绿色”后，再进行删除操作。

配置负载均衡安全组

创建负载均衡（CLB）后，您可以配置 CLB 的安全组来隔离公网流量。本文将介绍如何配置不同模式的 CLB 安全组。

使用限制

- 每个 CLB 最多绑定5个安全组，如需提升配额请联系云平台技术支持处理。
- CLB 的单个安全组，包含出规则、入规则、后端参数模版（ipm/ipmg/ppm/ppmg）完全展开，最多为 512 条。
- 内网 CLB 绑定 EIP 后，新增 CLB 上的安全组对来自 EIP 与内网 CLB 的流量生效。存量 CLB 上的安全组对来自 EIP 的流量不生效，对来自内网 CLB 的流量生效。
- 安全组默认放通只对本 VPC 内弹性网卡或者 CVM 类型的后端服务器生效，绑定 PaaS 服务（例如 CDB）作为后端服务器时，不支持安全组默认放通。

背景信息

安全组是一种虚拟防火墙，具备有状态的数据包过滤功能，控制实例级别的出入流量，详情请参见 安全组概述。
CLB 安全组为绑定在 CLB 实例上的安全组，CVM 安全组为绑定在 CVM 上的安全组，二者限制的对象不同。CLB的安全组配置，主要有如下两种模式：

- 开启安全组默认放通
- 关闭安全组默认放通

> 说明：
>
> - 默认情况下，IPv4 CLB 安全组默认放通为关闭状态，可在控制台开启 / 关闭。
> - 默认情况下，IPv6 CLB 安全组默认放通为开启状态，且无法关闭。

开启安全组默认放通

开启安全组默认放通后：

- 来自 CLB 的访问流量仅需通过 CLB 的安全组，后端云服务器会默认放通来自 CLB 的流量，后端云服务器不必对外暴露端口。
- 来自公网 IP（包括普通公网 IP 和 EIP）的流量，依然要经过 CVM 的安全组。
- 若 CLB 实例不配置安全组，则放通所有流量：CLB 实例的 VIP 上，仅配置了监听器的端口才能被访问，因此监听端口将放通所有 IP 的流量。
- 若需拒绝某个 Client IP 的流量，必须在 CLB 的安全组中拒绝访问；在 CVM 的安全组中拒绝某个 IP 的访问将不对来自 CLB 的流量生效，只对来自公网 IP（包括普通公网 IP 和 EIP）的流量生效。

关闭安全组默认放通

关闭安全组默认放通后：

- 通过 CLB 的业务流量会经过 CLB 安全组和 CVM 安全组的双重检查。
- 来自公网 IP（包括普通公网 IP 和 EIP）的流量，依然要经过 CVM 的安全组。
- 若 CLB 实例不配置安全组，则仅放通经过 CVM 安全组的流量。
- 若需拒绝某个 Client IP 的流量，可以在 CLB 和 CVM 其中任何一个的安全组中拒绝访问。
  关闭安全组默认放通的情况下，为保障健康检查功能，在 CVM 的安全组上需做如下配置：

1. 配置公网负载均衡
   您需要在后端 CVM 的安全组上放通 CLB 的 VIP，CLB 使用 VIP 来探测后端 CVM 的健康状态。
2. 配置内网负载均衡
   - 对于内网负载均衡，您需要在后端 CVM 的安全组上放通 CLB 的 VIP（用作健康检查）。

操作步骤

如下公网 CLB 的安全组配置示例，实现 CLB 上仅允许业务流量从80端口进入，并由 CVM 的8080端口提供服务，且不限制 Client IP，支持任意 IP 的访问。

> 注意：
>
> 本例使用公网 CLB，需要在后端 CVM 的安全组上放通 CLB 的 VIP 来做健康检查，当前 0.0.0.0/0 为任意 IP，已包括 CLB 的 VIP。

步骤1：创建负载均衡和监听器，绑定云服务器

详情请参见 负载均衡快速入门 。本次创建 HTTP:80 监听器，并绑定后端 CVM，后端 CVM 的服务端口为 8080。

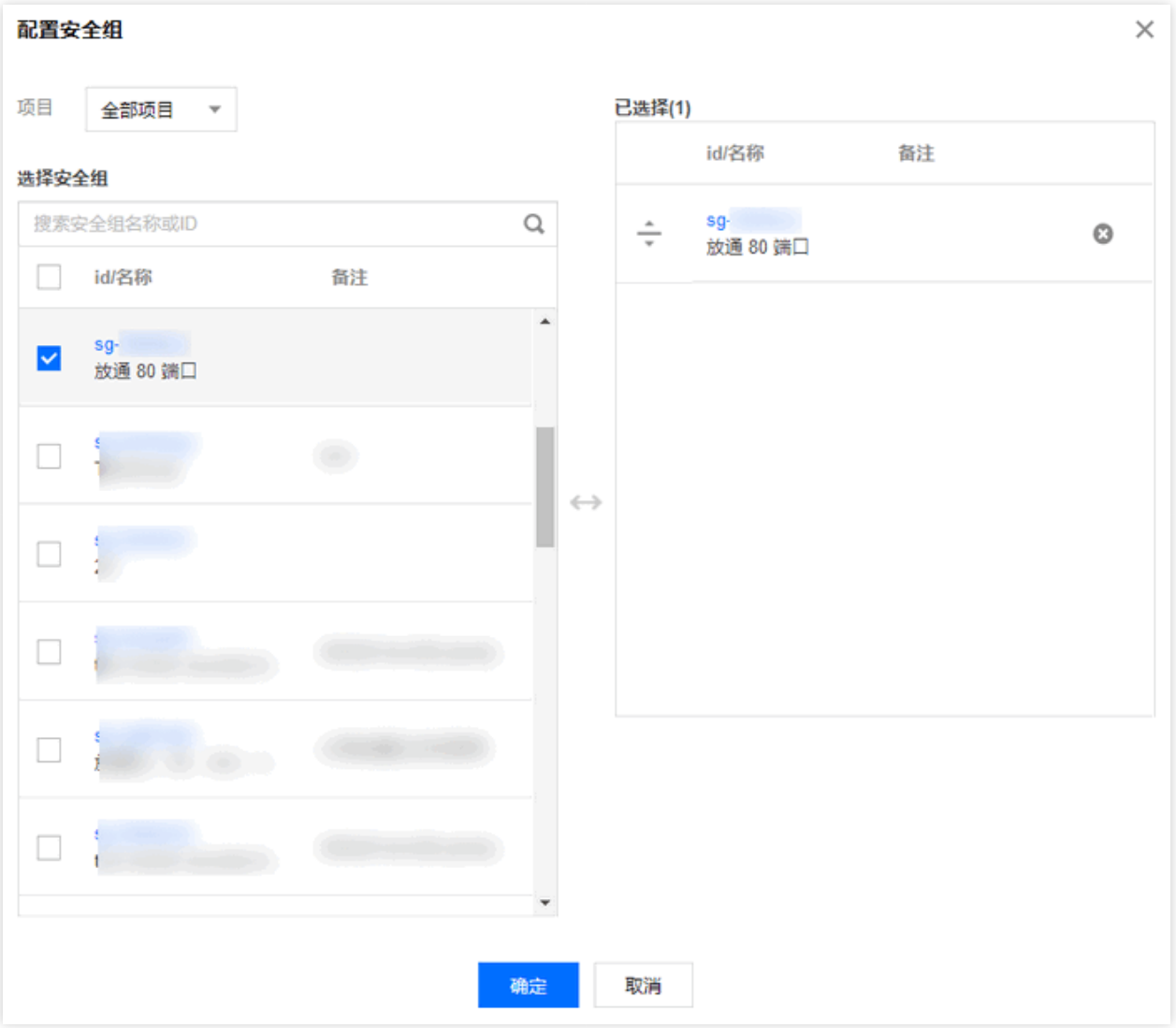
步骤2：配置 CLB 安全组

1. 配置负载均衡安全组规则
   在安全组控制台上配置安全组规则，在入站规则中放通所有 IP（即为 0.0.0.0/0 ）的80端口，并拒绝其他端口的流量。

> 说明：
>
> - 安全组规则，是从上至下依次筛选生效的，之前设置的允许规则通过后，其他的规则默认会被拒绝，请注意配置顺序，详见 安全组规则说明。
> - 安全组有入站规则和出站规则，上述配置限制的是入站流量，因此配置均为【**入站规则】**的配置，出站规则无需特殊配置。

2. 将安全组绑定 CLB

   i. 登录 负载均衡控制台。
   ii. 在【LB**实例列表】**页面找到目标 CLB 实例，单击实例 ID。
   iii. 在实例详情页面单击【**安全组】**页签，在"已绑定安全组"模块单击【绑定】。
   iv. 在弹出的【**配置安全组】**窗口中，选择对应绑定到 CLB 上的安全组，单击【确定】。



CLB 安全组配置完成，对于访问 CLB 的流量，仅允许80端口的访问。

步骤3：配置安全组默认放通

您可以选择开启或关闭安全组默认放通，不同选择配置如下：

- 方式一：开启安全组默认放通，后端云服务器不必对外暴露端口。
- 方式二：关闭安全组默认放通，CVM 的安全组上也需放通 Client IP（本例中即为 0.0.0.0/0 ）。

方式一：开启安全组默认放通

1. 登录负载均衡控制台。
2. 在【LB**实例列表】**页面找到目标 CLB 实例，单击实例 ID。
3. 在实例详情页面，单击【**安全组】**页签。

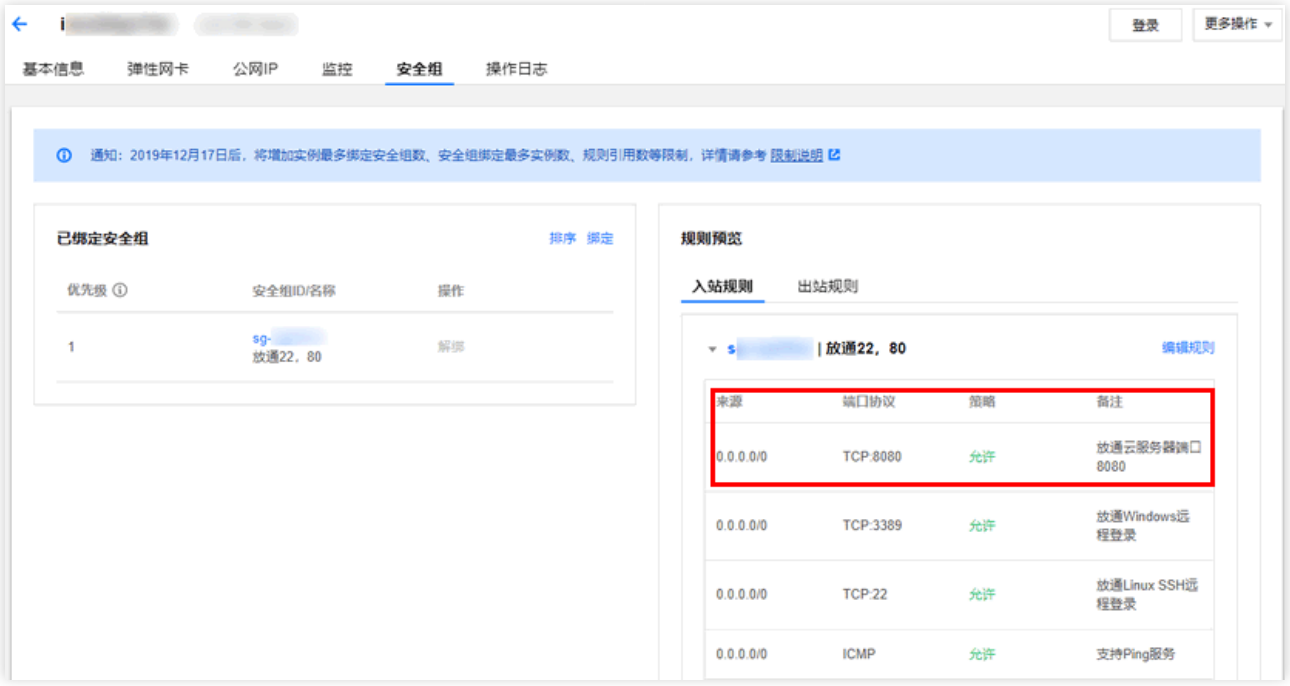
4. 在"安全组"页面，单击 ，启用默认放通。
5. 启用默认放通功能后，来自 CLB 的流量将仅验证如下【**规则预览】**中的安全组规则，CVM 的安全组对来自本 CLB 的流量默认放通。

方式二：关闭安全组默认放通

关闭默认放通，则需在 CVM 的安全组上放通 Client IP。对于通过 CLB 访问 CVM 的业务流量，仅允许从 CLB 的80端口进入，并由 CVM 的8080端口提供服务。

> 说明：
>
> 允许放通某个 Client IP 的流量，需要在 CLB 和 CVM 两个安全组上都放通，如果 CLB 上没有配置安全组，则仅需放通 CVM 上的安全组。

1. 配置云服务器安全组规则
   对于访问后端 CVM 的流量，通过配置云服务器安全组，限制仅允许服务端口的访问。
   在安全组控制台上配置安全组策略，在入站规则中放通所有 IP 的 8080 端口，为保障远程登录主机和 Ping 服务，在安全组上须放通 22、3389 和 ICMP 服务。
2. 将安全组绑定 CVM
   i. 在云服务器控制台上，单击 CLB 绑定的 CVM 的 ID，进入详情页。
   ii. 选择【**安全组】**标签页，在"已绑定安全组"模块单击【绑定】。
   iii. 在弹出的【**配置安全组】**窗口中，选择对应绑定到 CVM 上的安全组，单击【确定】。


登录
更多操作
基本信息
弹性网卡
公网IP
监控
安全组
操作日志
通知：2019年12月17日后，将增加实例最多绑定安全组数、安全组绑定最多实例数、规则引用数等限制，详情请参考 限制说明
已绑定安全组
排序 绑定
优先级
安全组ID/名称
操作
1
sg-
放通22，80
解绑
规则预览
入站规则
出站规则
| 放通22，80
编辑规则
来源
端口协议
策略
备注
0.0.0.0/0
TCP:8080
允许
放通云服务器端口8080
0.0.0.0/0
TCP:3389
允许
放通Windows远程登录
0.0.0.0/0
TCP:22
允许
放通Linux SSH远程登录
0.0.0.0/0
ICMP
允许
支持Ping服务

调整实例带宽配置

内外网CLB负载均衡实例，可按需调整网络带宽。

使用说明

IPv4 版本的内外网实例：支持调整网络带宽。
IPv6 版本的内外网实例：支持调整网络带宽。

带宽上限

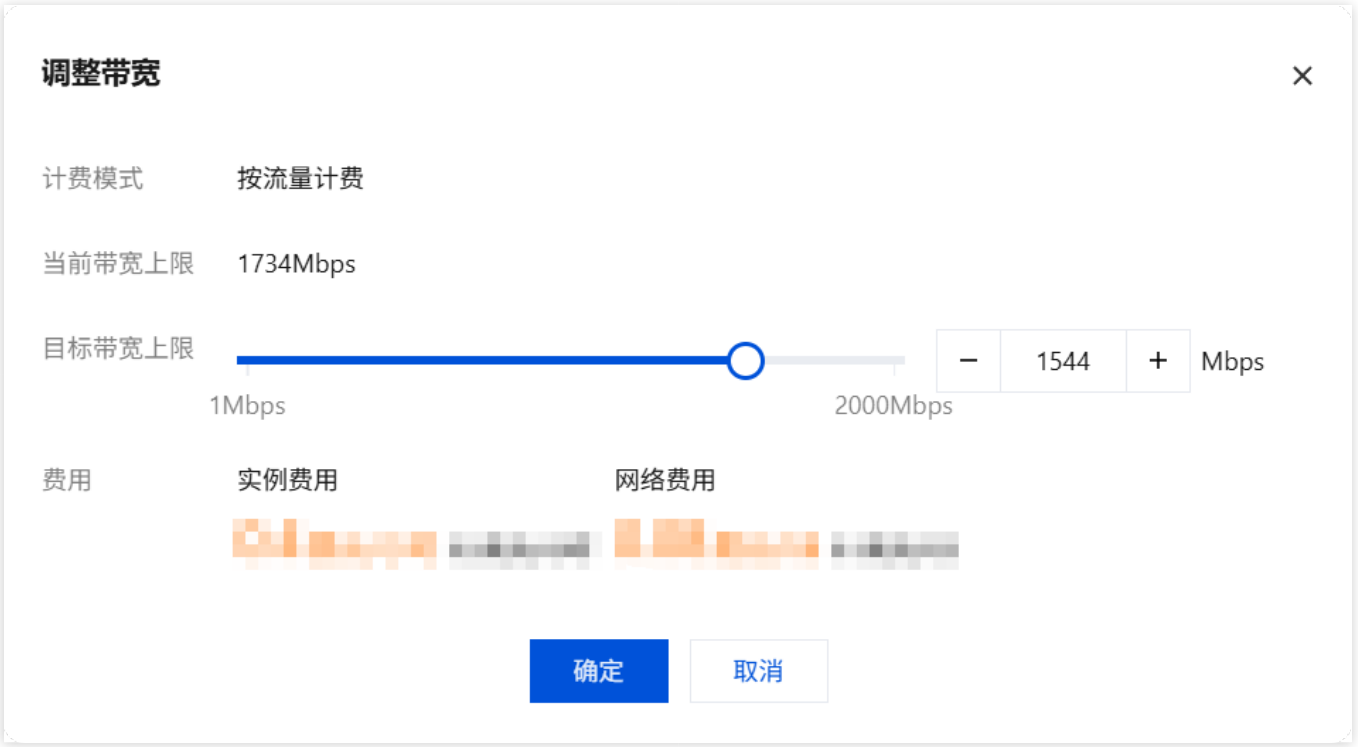
实例计费模式	网络计费模式	带宽上限的可设置范围（Mbps）
按量计费	按流量计费	0 - 2048（含2048）

> 说明：
>
> 如需更高带宽上限，请联系云平台技术支持处理。

调整带宽

1. 登录云控制台，选择【云产品】>【负载均衡】进入负载均衡控制台。
2. 在"LB实例列表"页面，选择所在地域，找到目标负载均衡实例，在操作栏选择【更多】 > 【调整宽带】。

3. 在弹出的对话框中，设置目标带宽上限值，并单击【确定】。



4. 内网CLB实例支持“不限制“带宽和”限制带宽“两种选择，请根据实际情况设置。

5. 设置完成后，可以在列表页查看该实例的带宽值。

负载均衡监听器
负载均衡监听器概述

创建负载均衡实例后，您需要为实例配置监听器。监听器负责监听负载均衡实例上的请求，并依据均衡策略来分发流量至后端服务器上。

负载均衡监听器需配置：

1. 监听协议和监听端口，负载均衡的监听端口，亦被称为前端端口，用来接收请求并向后端服务器转发请求的端口。
2. 监听策略，如均衡策略、会话保持 等。
3. 健康检查 策略。
4. 绑定后端服务，选择后端服务器的 IP 和端口，服务端口亦被称为后端端口，用来接收请求的端口。

支持的协议类型

负载均衡监听器可以监听负载均衡实例上的四层和七层请求，并将这些请求分发到后端服务器上，而后由后端服务器处理请求。四层和七层负载均衡的区别主要体现在：对用户请求进行负载均衡时，是依据四层协议还是七层协议来进行转发流量。

- 四层协议：传输层协议，主要通过 VIP + Port 接受请求并分配流量到后端服务器。
- 七层协议：应用层协议，基于 URL、HTTP 头部等应用层信息进行流量分发。
  TCloudFinanceZone负载均衡支持以下协议的请求转发：
- TCP（传输层）
- UDP（传输层）
- HTTP（应用层）
- HTTPS（应用层）

四层监听器

协议	说明	应用场景
TCP	面向连接的、可靠的传输层协议 - 传输的源端和终端需先三次握手建立连接，再传输数据 - 支持基于客户端 IP（源 IP）的会话保持 - 在网络层可以看到客户端 IP - 服务端可直接获取客户端 IP	适用于对可靠性和数据准确性要求高、对传输速度要求较低的场景，如文件传输、收发邮件、远程登录等。 详情请参见 配置 TCP 监听器。

协议	说明	应用场景
UDP	无连接的传输层协议 - 传输的源端和终端不建立连接，不需维护连接状态 - 每一条 UDP 连接都只能是点到点的 - 支持一对一，一对多，多对一和多对多的交互通信 - 支持基于客户端 IP（源 IP）的会话保持 - 服务端可直接获取客户端 IP	适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。 详情请参见 配置 UDP 监听器。

如果您使用四层监听器（即使用四层协议转发），负载均衡实例会在监听端口上建立与后端实例的 TCP 连接，直接将请求转发到后端服务器，此过程中不修改任何数据包（透传模式），转发效率极高。

七层监听器

协议	说明	应用场景
HTTP	应用层协议 - 支持基于请求域名和 URL 的转发 - 支持基于 Cookie 的会话保持	需要对请求的内容进行识别的应用，例如 Web 应用、App 服务等。 详情请参见 配置 HTTP 监听器。
HTTPS	加密的应用层协议 - 支持基于请求域名和 URL 的转发 - 支持基于 Cookie 的会话保持 - 统一的证书管理服务，CLB 完成解密操作 - 支持单项认证和双向认证	需加密传输的 HTTP 应用。 详情请参见 配置 HTTPS 监听器。

端口配置

监听端口（前端端口）	服务端口（后端端口）	说明
负载均衡提供服务时，接收请求并向后端服务器转发请求的端口。 用户可以为1 - 65535端口配置负载均衡，包括21（FTP）、25（SMTP）、80（HTTP）、443（HTTPS）等。	服务端口为云服务器提供服务的端口，接受并处理来自负载均衡的流量。 在一个负载均衡实例中，同一个负载均衡监听端口可以将流量转发到多个云服务器的多个端口上。	在同一个负载均衡实例内： 监听端口不可重复。例如，不可以同时创建监听器 TCP:80 和监听器 HTTP:80。 仅 TCP 和 UDP 协议的端口可重复。例如，可以同时创建监听器 TCP:80 和监听器 UDP:80。

监听端口（前端端口）	服务端口（后端端口）	说明
		服务端口可以在同一个负载均衡实例内重复。例如，监听器 HTTP:80 和监听器 HTTPS:443 可以同时绑定同一台云服务器的同一个端口。

配置TCP监听器

TCP 监听器简介

您可以在负载均衡实例上添加一个 TCP 监听转发来自客户端的 TCP 协议请求。TCP 协议适用于对可靠性和数据准确性要求高、对传输速度要求较低的场景，如文件传输、收发邮件、远程登录等。TCP 协议的监听器，后端服务器可直接获取客户端的真实 IP。

配置 TCP 监听器

步骤1：打开监听器管理页面

1. 登录负载均衡控制台。
2. 在左侧导航栏，选择【LB实例列表】。
3. 在 CLB 实例列表页单击需配置的实例 ID，进入实例详情页。
4. 单击【监听器管理】进入页面。

步骤2：配置监听器

在 TCP/UDP 监听器下，单击【新建】，在弹框中配置 TCP 监听器。

1. 基本配置

监听器基本配置	说明	示例
名称	监听器的名称	test-tcp-80
监听协议端口	监听器的协议和监听端口 - 监听协议：该监听器下 CLB 支持的协议包括 TCP、UDP，本例选择 TCP。 - 监听端口：用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。 - 同一个负载均衡实例内，监听端口不可重复。	TCP:80
均衡方式	TCP 监听器中，负载均衡支持按权重轮询（WRR）和加权最小连接数（WLC）两种调度算法。 - 按权重轮询：根据后端服务器的权重，依次将请求分发给不同的服务器。按权重轮询算法根据 新建连接数 来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 - 加权最小连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。	按权重轮询

创建 TCP 监听器基本配置如下图所示。

2. 健康检查

健康检查配置	说明	示例
健康检查状态	开启或关闭健康检查。TCP 监听器中，负载均衡实例向指定的服务器端口发送 SYN 包进行健康检查。	开启
检查协议	选择“TCP”表示配置 TCP 健康检查。	TCP
检查端口	非必填，不填写端口时默认为后端服务器端口。除需要指定特定端口以外，其余情况建议不填写。	
响应超时	- 健康检查响应的最大超时时间。 - 如果后端云服务器在超时时间内没有正确响应，则判定为健康检查异常。 - 可配置范围：2 - 60秒，默认值2秒。	2s
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒，默认值5秒。	5s
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次，默认值3次。	3次
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次，默认值3次。	3次

健康检查具体配置如下图所示：

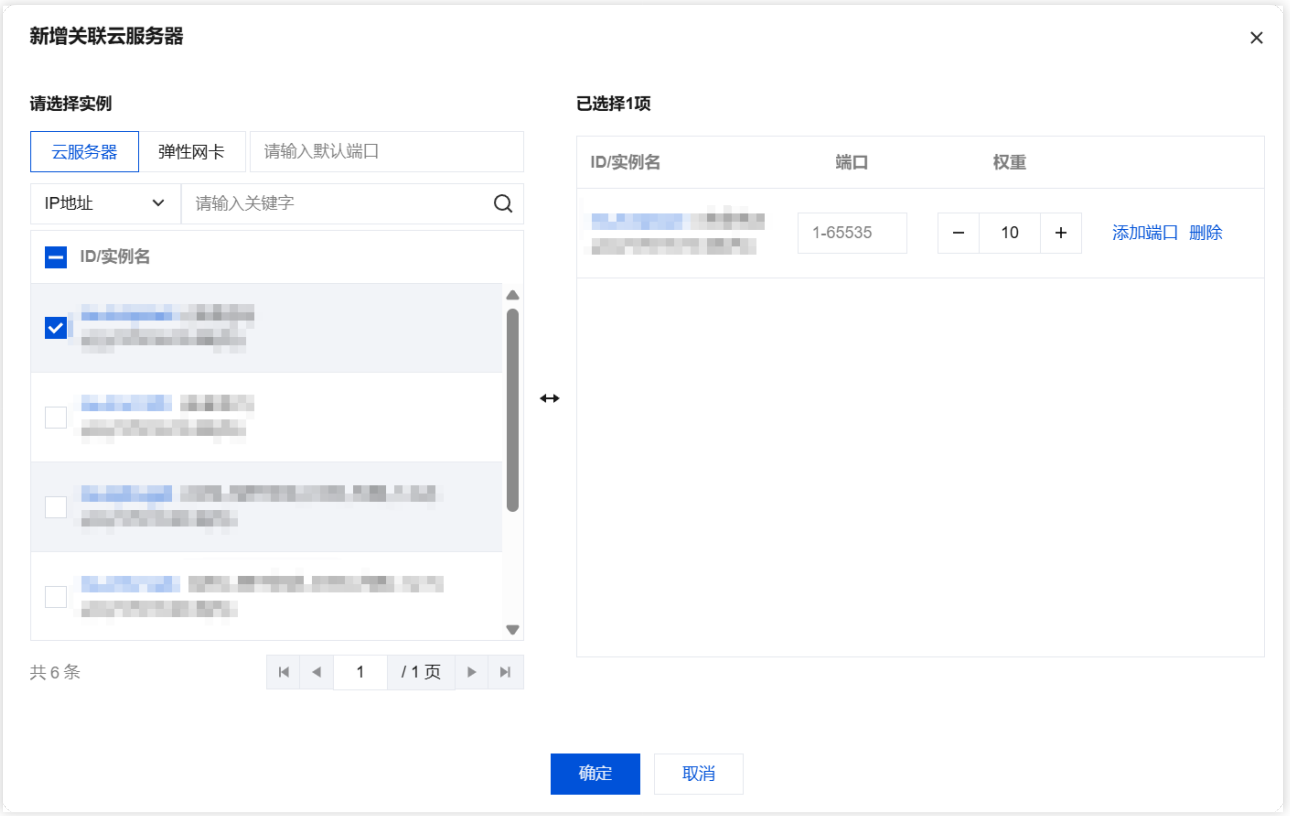
3. 会话保持

会话保持配置	说明	示例
会话保持状态	开启或关闭会话保持。 - 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端服务器上。 - TCP 协议是基于客户端 IP 地址的会话保持，即来自同一 IP 地址的访问请求转发到同一台后端服务器上。 - 按权重轮询的调度支持会话保持，加权最小连接数调度不支持开启会话保持功能。	开启
会话保持时间	会话保持时间 - 当超过保持时间，连接内无新的请求，将会自动断开会话保持。 - 可配置范围30 - 3600秒。	30s

会话保持具体配置如下图所示。

步骤3：绑定后端云服务器

1. 在【监听器管理】页面，单击已创建成功的监听器，如上述 TCP:80 监听器，即可在监听器右侧查看已绑定的后端服务。
2. 单击【绑定】，在弹出框中选择需绑定的后端服务器，并配置服务端口和权重。
   - 添加端口功能：在右侧"已选择"云服务器框内，单击【添加端口】，即可添加同一个云服务器的多个端口，如同时添加 CVM 的 80、81、82 三个端口。
   - 默认端口功能：先填写【默认端口】，再选择云服务器，每台云服务器的端口均为默认端口。



完成步骤1到步骤3之后，TCP 监听器规则已配置完毕。

步骤4：修改/删除监听器（可选）

如果您需要修改或删除已创建的监听器，请在【监听器管理】页面，单击已创建完毕的监听器，单击修改或删除图标来完成操作。

配置UDP监听器

UDP 监听器简介

您可以在负载均衡实例上添加一个 UDP 监听转发来自客户端的 UDP 协议请求。UDP 协议适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。UDP 协议的监听器，后端服务器可直接获取客户端的真实 IP。

配置 UDP 监听器

步骤1：打开监听器管理页面

1. 登录负载均衡控制台。
2. 在左侧导航栏，选择【LB实例列表】。
3. 在 CLB 实例列表页单击需配置的实例 ID，进入实例详情页。
4. 单击【监听器管理】标签页。

步骤2：配置监听器

在 TCP/UDP 监听器下，单击【新建】，在弹出框中配置 UDP 监听器。

1. 基本配置

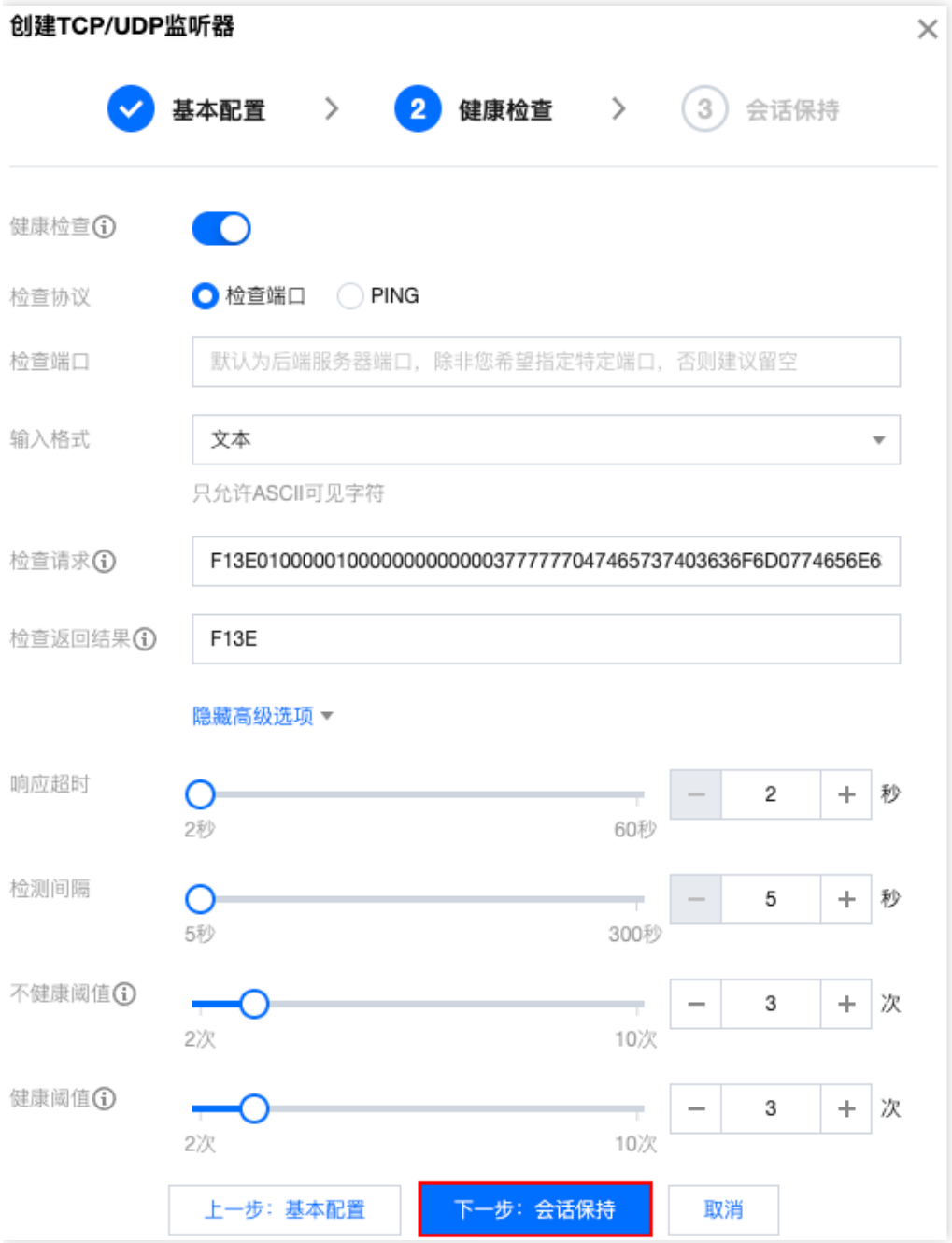
创建UDP 监听器具体基本配置如下图所示。

监听器基本配置	说明	示例
名称	监听器的名称	test-udp-8000

监听器基本配置	说明	示例
监听协议端口	监听器的协议和监听端口。 - 监听协议：该监听器下CLB 支持的协议包括 TCP、UDP，本例选择 UDP。 - 监听端口：用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。同一个负载均衡实例内，监听端口不可重复。	UDP:8000
均衡方式	UDP 监听器中，负载均衡支持按权重轮询（WRR）和加权最小连接数（WLC）两种调度算法。 - 按权重轮询算法：根据后端服务器的权重，依次将请求分发给不同的服务器。按权重轮询算法根据新建连接数来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 - 加权最小连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。	按权重轮询

2. 健康检查

健康检查具体配置如下图所示。



参数	说明
健康检查	可开启或关闭健康检查功能。建议您开启健康检查，帮助您自动检查并移除异常的后端 CVM 端口。
检查协议	- 选择"检查端口"表示 VIP（即负载均衡向客户端提供服务的 IP 地址）向后端 CVM 发送 UDP 探测报文，通过 Ping 后端 CVM 的 IP 地址来获取后端 CVM 的状态信息。 - 选择"PING"表示通过 Ping 后端 CVM 的 IP 地址来获取后端 CVM 的状态信息。
检查端口	非必填，不填写端口时默认为后端服务器端口。除需要指定特定端口以外，其余情况建议不填写。
输入格式	支持文本和十六进制输入。 输入格式为文本是将文本转换成二进制进行请求发送和返回结果对比。

参数	说明
	输入格式为十六进制是将十六进制转换成二进制进行请求发送和返回结果对比。
检查请求	自定义健康检查请求内容。例如探测 DNS 服务的检查请求示例为：F13E010000010000000000000377777704746573740363 6F6D0774656E63656E7403636F6D0000010001。
检查返回结果	自定义健康检查请求时，必须配置健康检查返回结果。例如探测 DNS 服务的检查返回结果示例为：F13E。
健康检查状态	开启或关闭健康检查。UDP 监听器中，负载均衡实例向服务器发 Ping 进行健康检查。
响应超时	- 健康检查响应的最大超时时间。 - 如果后端云服务器在超时时间内没有正确响应，则判定为健康检查异常。 - 可配置范围：2 - 60秒，默认值2秒。
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒，默认值5秒。
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次，默认值3次。
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次，默认值3次。

3. 会话保持

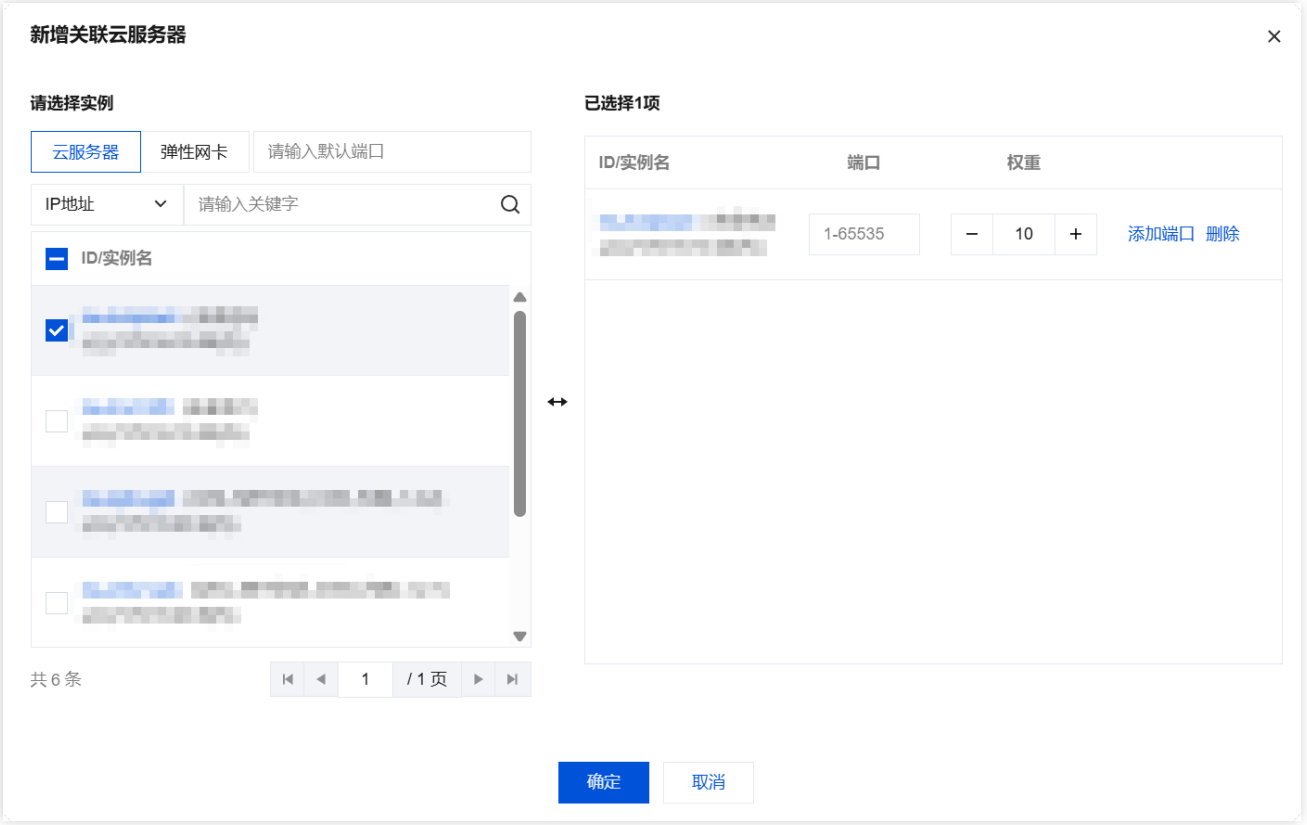
会话保持具体配置如下图所示。

会话保持配置	说明	示例
会话保持状态	开启或关闭会话保持。 - 开启会话保持后，负载均衡监听器会将来自同一客户端的访问请求分发到同一台后端服务器上。	开启

会话保持配置	说明	示例
	- UDP 协议是基于客户端 IP 地址的会话保持，即来自同一 IP 地址的访问请求转发到同一台后端服务器上。 - 按权重轮询调度支持会话保持，加权最小连接数调度不支持开启会话保持功能。	
会话保持时间	- 当超过保持时间，连接内无新的请求，将会自动断开会话保持。 - 可配置范围30 - 3600秒。	30s

步骤3：绑定后端云服务器

1. 在【监听器管理】页面，单击已创建完毕的监听器，如上述 UDP:8000 监听器，即可在监听器右侧查看已绑定的后端服务。
2. 单击【绑定】，在弹出框中选择需绑定的后端服务器，并配置服务端口和权重。



完成步骤1到步骤3之后，UDP 监听器规则已配置完毕。

步骤4：修改/删除监听器

如果您需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器，选择修改或删除来完成操作。

配置HTTP监听器

HTTP 监听器简介

您可以在负载均衡实例上添加一个 HTTP 监听转发来自客户端的 HTTP 协议请求。HTTP 协议适用于需要对请求的内容进行识别的应用，如 Web 应用、App 服务等。

配置 HTTP 监听器

步骤1：打开监听器管理页面

1. 登录负载均衡控制，在左侧导航栏，单击【LB实例列表】。
2. 在 CLB 实例列表页单击目标实例 ID。
3. 在实例详情页单击【监听器管理】标签页。

步骤2：配置监听器

在 HTTP/HTTPS 监听器模块下，单击【新建】，在弹出框中配置 HTTP 监听器。

1. 创建监听器

参数	说明
名称	监听器名称。本示例中可自定义为“Listener1”。
监听器协议	监听器的协议和监听端口。 - 监听协议包含 HTTP 和 HTTPS，本例选择 HTTP。 - 监听端口是用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。 - 同一个负载均衡实例内，监听端口不可重复。
默认域名	可选择开启或关闭。 - 开启：当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名。 - 如果您的七层监听器已配置默认域名，未匹配其他规则的客户端请求会被转发到默认域名。 - 如果您的七层监听器未配置默认域名，未匹配其他规则的客户端请求则会被转发到 CLB 加载的第一个域名，由于加载顺序与控制台配置顺序可能不一致，因此不一定是控制台配置的第一个。 - 关闭：当客户端请求没有匹配本监听器的任何域名时，请求将无法被转发。

2. 创建转发规则

转发规则基本配置	说明	示例
域名	请求域名。 - 支持精准域名，如 www.example,com 。支持通配域名， 如 *.example.com 或 www.example.* ，单个域名中 * 只能出现一次。 - 非正则的域名支持的字符集如下： a-z``0-9``.``- 。 - 支持正则表达式，正则表达式中不支持的字符集如下： "``{``}``;``\ ``` ~````空格 。 - 域名长度限制为1 - 120。	www.example.com
默认域名	- 当监听器中所有域名均没有匹配成功时，系统会将请求指向默认访问域名，让默认访问可控。 - 一个监听器下仅能配置一个默认域名。	开启
URL 路径	请求路径。 - 默认为 / ，必须以 / 开头，长度限制为1 - 120。 - 非正则的 URL 路径，以 / 开头，支持的字符集如下： a-z``A-Z``0-9``.``-``/``=``? 。 - 支持正则表达式 - = 开头表示精确匹配。 - ^~ 开头表示 uri 以某个常规字符串开头，不是正则匹配。 - ~ 开头表示区分大小写的正则匹配。 - ~* 开头表示不区分大小写的正则匹配。 - / 通用匹配, 如果没有其它匹配,任何请求都会匹配到 - 正则的 URL，不支持的字符集如下： "``{``}``;``\ ``` ~````空格 。	/index
均衡方式	HTTP 监听器中，负载均衡支持按权重轮询（WRR）、加权最小连接数（WLC）和 IP Hash 三种调度算法。 - 按权重轮询算法：根据后端服务器的权重，按依次将请求分发给不同的服务器。按权重轮询算法根据新建连接数来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 - 加权最少连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 - IP Hash：根据请求的源 IP 地址，使用散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器为可用且未超载状态，则请求发送到该服	按权重轮询

转发规则基本配置	说明	示例
	务器，反之则返回空。	
获取客户端 IP	默认启用。	已开启
Gzip 压缩	默认启用。	已开启

选择需要创建转发规则的 HTTP 监听器，单击右侧【+】进行规则创建，基本配置如下图所示。

3. 健康检查

健康检查配置	说明	示例
健康检查	开启或关闭健康检查。HTTP 监听器中，负载均衡实例向指定的服务器端口发 HTTP 请求进行健康检查。	开启
检查域名	请求域名 - 默认为转发域名。 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。 - 暂不支持正则表达式。 - 当用户填写域名为通配域名时，需要指定某一固定域名（非正则）为健康检查域名。	使用默认值（即为 www.example.com ）
检查目录	请求路径 - 默认为 / ，必须以 / 开头。 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。	使用默认值（即为 / ）

健康检查配置	说明	示例
	- 暂不支持正则表达式。 - 建议指定某个固定 URL 路径（静态页面）进行健康检查。	
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒，默认值5秒。	5s
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次，默认值3次。	3次
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次，默认值3次。	3次
HTTP 请求方式	健康检查的 HTTP 请求方式，可选：GET 或 HEAD，默认为 GET。 - 若使用 HEAD 方法，服务器仅返回 HTTP 头部信息，可降低后端开销，提升请求效率，对应的后端服务需支持 HEAD。 - 若使用 GET 方法，则后端服务支持 GET 即可。	GET
HTTP 状态码检测	当状态码为所选状态码时，认为后端服务器存活，即健康检查正常，可选：http_1xx，http_2xx， http_3xx，http_4xx，http_5xx。	多选：http_1xx，http_2xx，http_3xx，http_4xx

健康检查具体配置如下图所示。

4. 会话保持

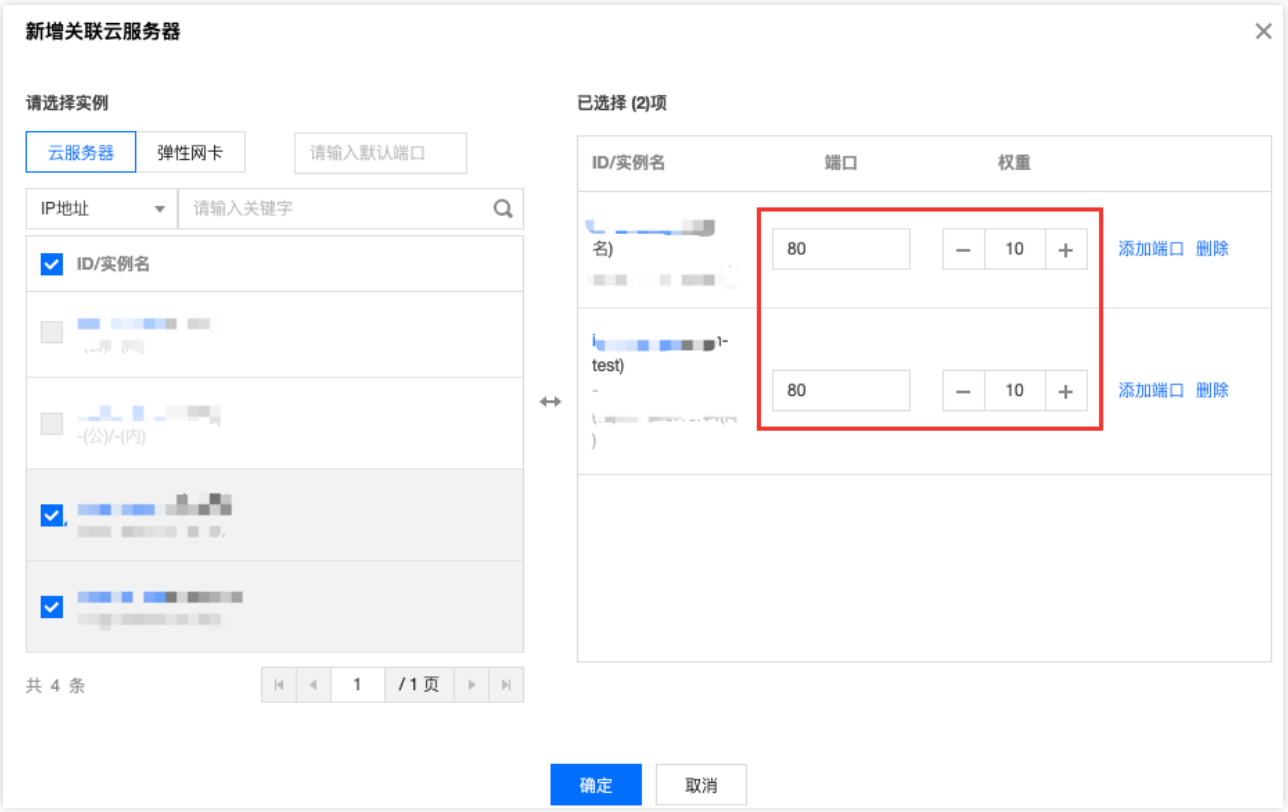
会话保持配置	说明	示例
会话保持状态	开启或关闭会话保持。 - 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端服务器上。 - HTTP 协议是基于 Cookie 的会话保持，由负载均衡器向客户端植入 Cookie。 - 加权轮询调度支持会话保持，加权最小连接数和 IP Hash 调度不支持开启会话保持功能。	开启
会话保持时间	会话保持时间。 - 当超过保持时间，连接内无新的请求，将会自动断开会话保持。 - 可配置范围30 - 3600秒。	30s

会话保持具体配置如下图所示。

步骤3：绑定后端云服务器

1. 在“监听器管理”页面，单击已创建完毕的监听器，如上述 HTTP:80 监听器，单击左侧的三角图标展开域名和 URL 路径，选中具体的 URL 路径，即可在监听器右侧查看该路径上已绑定的后端服务。

2. 单击【绑定】，在弹出框中选择需绑定的后端服务器，并配置服务端口和权重。
   - 添加端口功能：在右侧“已选择”的云服务器框内，单击【添加端口】，即可给同一个云服务器添加多个端口。
   - 默认端口功能：先填写【默认端口】，再选择云服务器，每台云服务器的端口均为默认端口。



步骤4：修改/删除监听器

如果您需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器/域名/URL 路径，选择修改或删除完成操作。

配置HTTPS监听器

HTTPS 监听器简介

您可以在负载均衡实例上添加一个 HTTPS 监听器转发来自客户端的 HTTPS 协议请求。HTTPS 协议适用于需要加密传输的 HTTP 应用。

配置 HTTPS 监听器

步骤1：打开监听器管理页面

1. 登录负载均衡控制台，在左侧导航栏，单击【LB实例列表】。
2. 在 CLB 实例列表页单击目标实例 ID。
3. 在实例详情页单击【监听器管理】标签页。

步骤2：配置监听器

在 HTTP/HTTPS 监听器模块下，单击【新建】，在弹出框中配置 HTTPS 监听器。

1. 创建监听器

监听器基本配置	说明	示例
名称	监听器的名称。	test-https-443
监听协议端口	监听器的协议和监听端口。 - 监听协议：该监听器下CLB 支持的协议包括HTTP、HTTPS，本例选择 HTTPS。 - 监听端口：用来接收请求并向后端服务器转发请求的端口，端口范围为1 - 65535。 - 同一个负载均衡实例内，监听端口不可重复。	HTTPS:443
默认域名	可选择开启或关闭。 - 开启：当客户端请求没有匹配到本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名。 - 如果您的七层监听器已配置默认域名，未匹配到其他规则的客户端请求会被转发到默认域名。 - 如果您的七层监听器未配置默认域名，未匹配到其他规则的客户端请求则会被转发到 CLB 加载的第一个域名，由于加载顺序与控制台配置顺序可能不一致，因此不一定是控制台配置的第一个。 - 关闭：当客户端请求没有匹配到本监听器的任何域名时，请求将无法被转发。	开启
启用 SNI	启用 SNI 表示一个监听器下可为不同的域名配置不同的证书，不启用 SNI 表示该监听器下多个域名使用同一个证书。	开启
SSL 解析方式	支持单向认证和双向认证。	单向认证
服务器证书	选择已有证书。	选择已有证书

创建 HTTPS 监听器具体配置如下图所示。

2. 创建转发规则

转发规则基本配置	说明	示例
域名	请求域名。 - 支持精准域名，如 www.example,com 。支持通配域名， 如 *.example.com 或 www.example.* ，单个域名中 * 只能出现一次。 - 非正则的域名支持的字符集如下： a-z``0-9``.``- 。 - 支持正则表达式，正则表达式中不支持的字符集如下： "``{``}``;``\```````~`````空格 。 - 域名长度限制为1 - 120。	www.example.com
默认域名	- 当监听器中所有域名均没有匹配成功时，系统会将请求指向默认访问域名，让默认访问可控。 - 一个监听器下仅能配置一个默认域名。	开启
URL 路径	请求路径。 - 默认为 / ，必须以 / 开头，长度限制为 1-120 。 - 非正则的 URL 路径，以 / 开头，支持的字符集如下： a-z``A-Z``0-9``.``-``/``=``? 。 - 支持正则表达式 - = 开头表示精确匹配。 - ^~ 开头表示 uri 以某个常规字符串开头，不是正则匹配。 - ~ 开头表示区分大小写的正则匹配。 - ~* 开头表示不区分大小写的正则匹配。 - / 通用匹配，如果没有其它匹配，任何请求都会匹配到。 - 正则的 URL，不支持的字符集如下： "``{``}``;``\ ``` ~`````空格 。	/index

转发规则基本配置	说明	示例
均衡方式	HTTPS 监听器中，负载均衡支持按权重轮询（WRR）、加权最小连接数（WLC）和 IP Hash 三种调度算法。 - 按权重轮询算法：根据后端服务器的权重，依次将请求分发给不同的服务器。按权重轮询算法根据新建连接数来调度，权值高的服务器被轮询到的次数（概率）越高，相同权值的服务器处理相同数目的连接数。 - 加权最小连接数：根据服务器当前活跃的连接数来估计服务器的负载情况，加权最小连接数根据服务器负载和权重来综合调度，当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 - IP Hash：根据请求的源 IP 地址，使用散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器为可用且未超载状态，则请求发送到该服务器，反之则返回空。	按权重轮询
后端协议	后端协议是指 CLB 与后端服务之间的协议： - 后端协议选择 HTTP 时，后端服务需部署 HTTP 服务。 - 后端协议选择 HTTPS 时，后端服务需部署 HTTPS 服务，HTTPS 服务的加解密会让后端服务消耗更多资源。后端服务需要配置相同的 SSL 证书。传统账户的后端转发协议不支持选择 HTTPS。	HTTPS
获取客户端 IP	默认启用。	已开启
Gzip 压缩	默认启用。	已开启

选择需要创建转发规则的 HTTPS 监听器，单击添加规则进行创建，具体基本配置如下图所示。

3. 健康检查

健康检查配置	说明	示例
健康检查	开启或关闭健康检查。HTTPS 监听器中，负载均衡实例向指定的服务器端口发送 HTTPS 请求进行健康检查。	开启
检查域名	请求域名。 - 默认为访问域名。 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。 - 暂不支持正则表达式。 - 当用户填写域名为通配域名时，需指定某一固定域名（非正则）为健康检查域名。	使用默认值（即为 www.example.com ）
检查目录	请求路径 。 - 默认为 / ，必须以 / 开头。 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。 - 暂不支持正则表达式。 - 建议指定某个固定 URL 路径（静态页面）进行健康检查。	使用默认值（即为 / ）

健康检查配置	说明	示例
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒，默认值5秒。	5s
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次，默认值3次。	3次
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次，默认值3次。	3次
HTTP 请求方式	健康检查的 HTTP 请求方式，可选：GET 或 HEAD，默认为 GET。 - 若使用 HEAD 方法，服务器仅返回 HTTP 头部信息，可降低后端开销，提升请求效率，对应的后端服务需支持HEAD。 - 若使用 GET 方法，则后端服务支持 GET 即可。	GET
HTTP 状态码检测	当状态码为所选状态码时，认为后端服务器存活，即健康检查正常，可选：http_1xx，http_2xx， http_3xx，http_4xx，http_5xx。	多选：http_1xx，http_2xx，http_3xx，http_4xx

健康检查具体配置如下图所示。

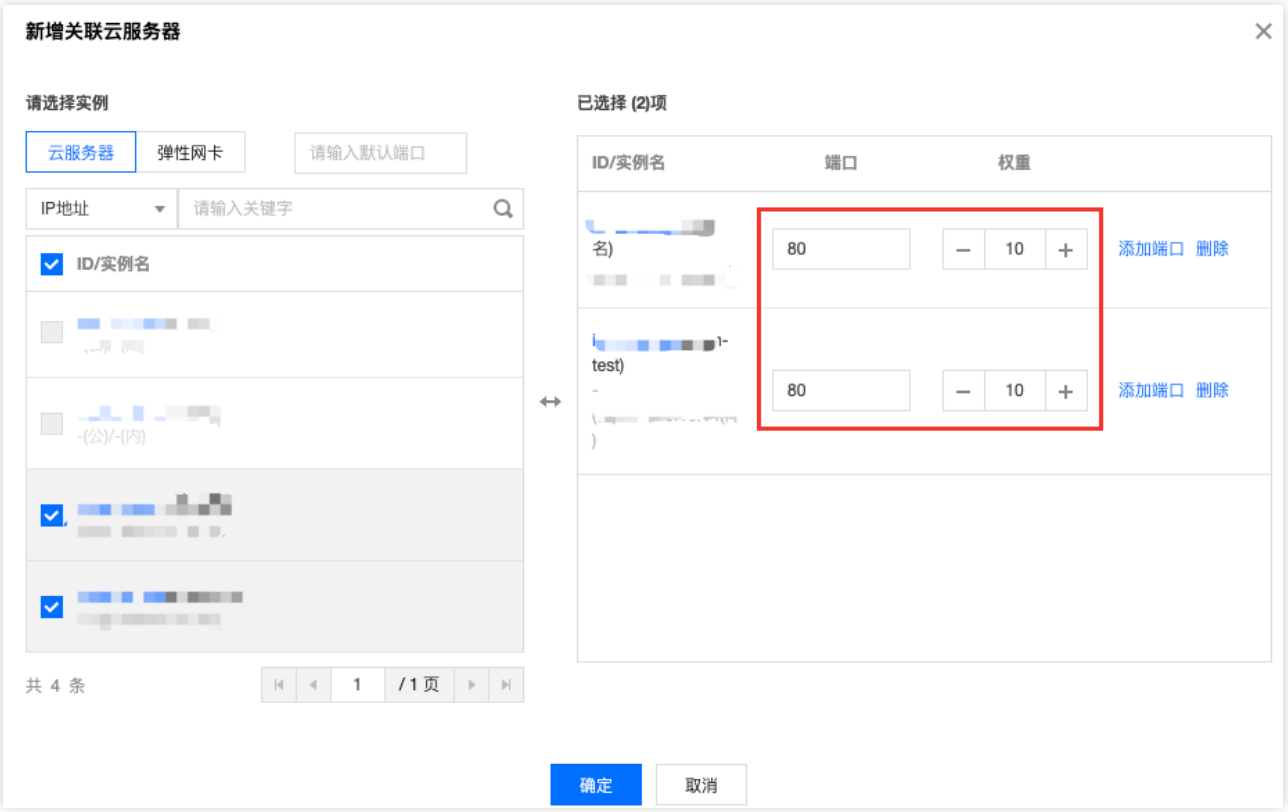
4. 会话保持

会话保持配置	说明	示例
会话保持状态	开启或关闭会话保持。 - 开启会话保持后，负载均衡监听器会把来自同一客户端的访问请求分发到同一台后端服务器上。 - HTTPS 协议是基于 Cookie 的会话保持，由负载均衡器向客户端植入 Cookie。 - 加权轮询调度支持会话保持，加权最小连接数和 IP Hash 调度不支持开启会话保持功能。	开启
会话保持时间	会话保持时间。 - 当超过保持时间，连接内无新的请求，将会自动断开会话保持。 - 可配置范围30 - 3600秒。	30s

会话保持具体配置如下图所示。

步骤3：绑定后端云服务器

1. 在“监听器管理”页面，单击已创建完毕的监听器，单击左侧的三角符号展开域名和 URL 路径，选中具体的 URL 路径，即可在监听器右侧查看该路径上已绑定的后端服务。
2. 单击【绑定】，在弹出框中选择需绑定的后端服务器，并配置服务端口和权重。
    - 添加端口功能：在右侧【已选择】云服务器框内，单击【添加端口】，即可添加同一个云服务器的多个端口。
    - 默认端口功能：先填写【默认端口】，再选择云服务器，每台云服务器的端口均为默认端口。



完成步骤1到步骤3之后，HTTPS 监听器规则已配置完毕。

步骤4：修改/删除监听器（可选）

如果您需要修改或删除已创建的监听器，请在“监听器管理”页面，单击已创建完毕的监听器/域名/URL 路径，选择修改或删除完成操作。

轮询方式

轮询方式是负载均衡向 后端服务器 分配流量的算法，根据不同的轮询方式及后端服务器的权重设置，可以达到不同的效果。

按权重轮询算法

权重轮询算法（Weighted Round-Robin Scheduling）是以轮叫的方式、依次请求调度不同的服务器。权重轮询调度算法可以解决服务器间性能不一的情况，它用相应的权值表示服务器的处理性能，按权值的高低和轮询方式分配请求到各服务器。权重轮询算法根据新建连接数来调度，权值高的服务器先收到连接，权重值越高被轮询到的次数（概率）也越高，相同权值的服务器处理相同数目的连接数。

- 优势：简洁实用，无需记录当前所有连接的状态，是一种无状态调度。
- 劣势：相对简单，在请求服务时间变化较大或每个请求消耗时间不一致的情况下，容易导致服务器间的负载不平衡。
- 适用场景：当每个请求所占用的后端时间基本相同时，负载情况最好。常用于短连接服务，例如 HTTP 等。
- 用户推荐：已知每个请求所占用后端时间基本相同、后端服务器处理的请求类型相同或者相似时，推荐您选择加权轮询的方式。请求时间相差较小时，也推荐您使用加权轮询的方式，因为该实现方式消耗小，无需遍历，效率较高。

加权最小连接数算法

在实际情况中，客户端的请求服务在服务器停留的时间会有较大的差异。随着工作时间的延伸，采用简单的轮询或随机均衡算法，每台服务器上的连接进程数目可能会有极大的不同，导致没有达到真正的负载均衡。
最小连接调度是一种动态调度算法，与轮询调度算法相反，它通过服务器当前所活跃的连接数来估计服务器的负载情况。调度器需要记录各个服务器已建立连接的数目，当一个请求被调度到某台服务器时，其连接数加一; 当连接中止或超时，其连接数减一。
加权最小连接数算法（Weighted Least-Connection Scheduling）是在最小连接数调度算法的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权值，使其能够接受相应权值数的服务请求，是在最小连接数调度算法的基础上的改进。

> 说明：
>
> 假设各台后端服务器的权值依次为 wi，当前连接数依次为 ci，依次计算 ci/wi，值最小的后端服务器实例作为下一个分配的实例。如果存在 ci/wi 相同的后端服务器实例，再使用加权轮询的方式调度。

- 优势：此算法适合长时处理的请求服务，如 FTP 等应用。
- 劣势：由于接口限制，目前最小连接数和会话保持功能不能同时开启。
- 适用场景：每个请求所占用的后端时间相差较大的场景。常用于长连接服务。

- 用户推荐：如果用户需要处理不同的请求，且请求所占用后端时间相差较大，如3ms和3s等数量级差距，推荐使用加权最小连接数算法，实现负载均衡。

源地址散列调度算法

源地址散列调度算法（ip_hash）根据请求的源 IP 地址，使用散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器为可用且未超载状态，则请求发送到该服务器，反之则返回空。

- 优势：可以使某一客户端的请求通过哈希表一直映射在同一台后端服务器上，在不支持会话保持的场景中，可以使用 ip_hash 实现简单的会话保持。
- 用户推荐：将请求的源地址进行哈希运算，并结合后端服务器的权重，派发请求至某匹配的服务器，使得同一客户端 IP 的请求始终被派发至某特定的服务器。该方式适合无 cookie 功能的 TCP 协议。

均衡算法选取及权重配置

为了让用户在不同场景下实现后端服务器集群稳定地承接业务，下文将给出负载均衡选择与权重配置的场景示例，供您参考。

- 场景1：
  i. 假设有3台配置相同（CPU/内存）的后端服务器，由于性能一致，可以将后端服务器权重都设置为10。
  ii. 现在每台后端服务器与客户端建立了100个 TCP 连接，并新增1台后端服务器。
  iii. 在此场景下，推荐使用最小连接数均衡方式，能快速实现第4台后端服务器的负载提升，降低另外3台后端服务器的压力。
- 场景2：
  1.1. 假设您首次接触云服务，且建站时间不长，网站负载较低，建议购买相同配置的后端服务器，此时后端服务器都是无差别的接入层服务器。
  1.2. 在此场景下，可以将后端服务器权重都设为默认值10，采用加权轮询的均衡方式进行流量分发。
- 场景3：
  1.1. 假设您有5台服务器，用于承载简单的静态网站访问，且5台服务器的计算能力的比例为 9：3：3：3：1（按 CPU、内存换算）。
  1.2. 在此场景下，可以依次将后端服务器权重比例设置为 90、30、30、30、和10。静态网站访问大多数是短连接请求，因此，可以采用加权轮询的均衡方式，让负载均衡实例按后端服务器的性能比例分配请求。
- 场景4：
  1.1. 假设您有10台后端服务器，用于承担海量的 Web 访问请求，且不希望多购置后端服务器增加支出，但某台后端服务器经常会因为负载过高，导致服务器重启。
  1.2. 在此场景下，建议根据后端服务器的性能进行相应的权重设置，为负载过高的后端服务器设置较小的权值。此外，可以采用最小连接数的负载均衡方式，将请求分配到活跃连接数较少的后端服务器上，从而解决某台后端服务器负载过高的问题。
- 场景5：

1.1. 假设您有3台后端服务器，用于处理若干长连接请求，且这3台服务器的计算能力比例为 3：1：1（按CPU、内存换算）。

1.2. 此时性能最好的服务器处理请求较多，您不希望过载此服务器，欲将新的请求分配到空闲服务器上。

1.3. 在此场景下，可以采用最小连接数的均衡方式，并适当降低繁忙服务器的权重，便于负载均衡将请求分配到活跃数较少的后端服务器上，实现负载均衡。

- 场景6：

1.1. 假设您希望后续客户端的请求可以分配到同一服务器上。此时，采用加权轮询或加权最小连接数的方式，不能保证相同客户端的请求被分到固定服务器上。

1.2. 为了配合特定应用程序服务器的需求，保证客户端的会话具有“粘性”或“持续性”。在此场景下，可以采用 ip_hash 的均衡方式进行流量分发，可以确保来自同一客户端的请求总被定向分发到同一后端服务器上（服务器数量变化或该服务器不可用时除外）。

健康检查

- TCloudFinanceZone负载均衡实例可以定期向后端服务器发送 Ping、尝试连接或发送请求来测试后端服务器运行的状况，这些测试称为健康检查。
- 当后端服务器实例被判定为不健康时，负载均衡实例将不会把请求转发到该实例上。但健康检查会对所有后端服务器（不管是判定为健康的还是不健康的）进行，当不健康实例恢复正常状态时，负载均衡实例将恢复把新的请求转发给它。
- 弹性伸缩组会定期使用相似的方法确定每个组内实例的运行状况。有关更多信息，请参见 弹性伸缩 。

四层转发健康检查配置

四层转发的健康检查机制：由负载均衡器向配置中指定的服务器端口发起访问请求，若端口访问正常，则视为后端服务器运行正常，否则视为运行异常。
对于 TCP 的业务，使用 SYN 包进行探测；对于 UDP 业务，使用 Ping 进行检查。

健康检查配置	说明	默认值
响应超时	健康检查响应的最大超时时间。 如果后端云服务器在超时时间内没有正确响应，则判定为健康检查异常。 可配置范围：2 - 60秒。	2秒
检测间隔	负载均衡进行健康检查的时间间隔。 可配置范围：5 - 300秒。	5秒
不健康阈值	如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 可配置范围：2 - 10次。	3次
健康阈值	如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 可配置范围：2 - 10次。	3次

七层转发健康检查配置

七层转发的健康检查机制由负载均衡器向后端服务器发送 HTTP 请求来检测后端服务，负载均衡器会根据用户选择的 HTTP 返回值来判断服务是否正常。假定在某场景下，HTTP 返回值为 http_1xx 、 http_2xx 、 http_3xx 、 http_4xx 和 http_5xx 这几种，用户可以根据业务需要编辑 http_1xx 及 http_2xx 为服务正常状态，并设置 http_3xx 至 http_5xx 的返回值代表异常状态。

健康检查配置	说明	默认值

健康检查配置	说明	默认值
检查域名	请求域名 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。 - 暂不支持正则表达式。 - 当用户填写域名为通配域名时，需要指定某一固定域名（非正则）为健康检查域名。	转发域名
检查路径	请求路径 - 必须以 / 开头。 - 支持的字符集包括： a-z``0-9``.``- ，长度限制为1 - 120。 - 暂不支持正则表达式。 - 建议指定某个固定 URL 路径（静态页面）进行健康检查。	/
检测间隔	- 负载均衡进行健康检查的时间间隔。 - 可配置范围：5 - 300秒。	5秒
不健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果失败，则识别为不健康，控制台显示为异常。 - 可配置范围：2 - 10次。	3次
健康阈值	- 如果连续 n 次（n 为填写的数值）收到的健康检查结果为成功，则识别为健康，控制台显示为健康。 - 可配置范围：2 - 10次。	3次
HTTP 请求方式	健康检查的 HTTP 请求方式，可选：GET 或 HEAD。 - 若使用 HEAD 方法，服务器仅返回 HTTP 头部信息，可降低后端开销，提升请求效率，对应的后端服务需支持 HEAD。 - 若使用 GET 方法，则后端服务支持 GET 即可。	GET
HTTP 状态码检测	当状态码为所选状态码时，认为后端服务器存活，即健康检查正常，可选：http_1xx，http_2xx， http_3xx，http_4xx，http_5xx。	http_1xx，http_2xx，http_3xx，http_4xx

健康检查状态

根据健康检查探测情况，后端服务的健康检查状态有如下两种：

状态	说明	是否转发流量
健康	后端服务正常	CLB 向“健康”的后端服务转发流量。
异常	后端服务异常	- CLB 不向“异常”的后端服务转发流量。 - 在一个四层监听器或者七层 URL 规则下，如果 CLB 探测到所有后端服务都不健康，将会激活全死全活逻辑，即请求将会转发给所有后端服务。

健康检查异常排查思路

四层排查

TCP 协议下，负载均衡使用 SYN 包进行探测。UDP 协议下，负载均衡使用 Ping 命令进行探测。
在页面查看后端服务器端口的健康状态，若不健康，排查思路如下：

- 确定后端服务器是否有配置有安全组影响了服务。有关如何控制后端服务器的访问来保证服务正常运行，请参见 后端云服务器安全组配置说明。
- 使用 netstat 命令，确定后端服务器的端口是否有进程在监听，若未发现进程则请重新启动服务。

七层排查

针对七层（HTTP/HTTPS 协议）服务，当某一监听出现健康检查异常时，可以通过如下方面进行排查：

1. 由于负载均衡的七层健康检查服务与后端 CVM 之间通过内网通信，您需要登录服务器检查应用服务器端口是否正常监听在内网地址上，如果没有监听在内网地址，请将应用服务器端口监听到内网上，从而确保负载均衡系统和后端 CVM 之间的通讯正常。
   假设负载均衡前端端口是80，CVM 后端端口也是80，CVM 的内网 IP 是： 1.1.1.10 。

   Windows 系统服务器使用如下命令：

   ```
   netstat -ano | findstr :80
   ```

   Linux 系统服务器使用如下命令：

   ```
   netstat -anp | grep :80
   ```

   如果能看到 1.1.1.10:80 的监听或 0.0.0.0:80 的监听则说明此配置正常。

2. 请确保后端服务器开启了您在负载均衡监听器中配置的后端端口。
   如果是四层负载均衡，只要后端端口 telnet 有响应即可，可以使用 telnet 1.1.1.10 80 来测试。如果是七层负载均衡，需要 HTTP 状态码是200等代表正常的状态码。检验方法如下：

   - Windows 系统可以直接在 CVM 内的浏览器输入内网 IP 测试是否正常，本例使用 http://1.1.1.10 。
   - Linux 系统可以通过 curl -I 命令查看状态是否为 HTTP/1.1 200 OK ，本例使用 curl -I 1.1.1.10 命令。

3. 检查后端 CVM 内部是否有防火墙或其他安全类防护软件，这类软件很容易将负载均衡系统的本地 IP 地址屏蔽，从而导致负载均衡系统无法跟后端服务器进行通讯。
   检查服务器内网防火墙是否放行80端口，可以暂时关闭防火墙进行测试。

- Windows 系统可以运行输入 firewall.cpl 操作关闭
- Linux 系统可以输入 /etc/init.d/iptables stop 关闭

4. 检查负载均衡健康检查参数设置是否正确，建议参照本文档提供的健康检查参数默认值进行设置。
5. 健康检查指定的检测文件，建议是 HTML 形式的简单页面，只用于检查返回结果。不建议用 PHP 等动态脚本语言。
6. 检查后端是否有较高负载导致 CVM 对外提供服务响应慢。
7. 检查 HTTP 请求方式，如果使用 HEAD 方法，则后端服务一定要支持 HEAD。如果是 GET 方法，则后端服务一定要支持 GET。

关于健康检查探测频率过高的说明

健康检查探测包频率过高，控制台设置接受探测包5秒1次，实际后端 RS 发现1秒内收到1次甚至多次健康检查请求的原因是：

- 当前，健康检查频率过高的问题，主要跟负载均衡后端健康探测实现机制有关。假设100万的 client 端请求，会分散在4台CLB 后端物理机上，再转给云服务器。 健康检查探测是在 CLB 的后端物理机上，各自探测的。因此，CLB 实例设置5秒1次的探测请求，实际上 CLB 后端的每台物理机都会每5s发送一次探测。因此在后端云服务器上，会收到多次探测请求。（假设 CLB 实例所在集群有8台物理机，那么每台机器5s发送一次请求，后端主机可能会在5s中收到8次探测）
- 该实现方案的优势是：效率高，探测精准，避免误剔除。例如，CLB 实例集群的8台物理机中，其中1台判断失败，仅那1台机器不再转发流量，另外7台的流量是正常的。
  因此，如果您后端云服务器的探测频率过高，可以通过设置更长的探测间隔时间来解决（ 例如设置为15s探测一次）。

会话保持

会话保持可使得来自同一 IP 的请求被转发到同一台后端服务器上。默认情况下，负载均衡会将每个请求分别路由到不同后端服务器实例负载。但是，您可以使用会话保持功能使特定用户的请求被路由到同一台后端服务器实例上，这样可以使某些需要保持会话的应用程序（如购物车）合理地工作。

四层会话保持

四层协议（TCP/UDP）支持基于源 IP 的会话保持能力，会话保持时间可设为30 - 3600秒中的任意整数值，超过该时间阈值，会话中无新请求则断开连接，会话保持与均衡方式相关：

- 均衡方式为“加权轮询”时，根据后端服务器的权重分发请求，支持基于源 IP 的会话保持。
- 均衡方式为“加权最小连接数”时，根据服务器负载和权重来综合调度，不支持会话保持。

七层会话保持

七层协议（HTTP/HTTPS）支持基于 Cookie 插入的会话保持能力（由负载均衡器向客户端植入 Cookie），会话保持时间设置支持30 - 3600秒，会话保持与均衡方式相关：

- 均衡方式为“加权轮询”时，根据后端服务器的权重分发请求，支持基于 Cookie 插入的会话保持。
- 均衡方式为“加权最小连接数”时，根据服务器负载和权重来综合调度，不支持会话保持。
- 均衡方式为 “IP Hash” 时，支持基于源 IP 的会话保持，不支持基于 Cookie 插入的会话保持。

连接超时时间

当前 HTTP 连接超时时间（keepalive_timeout）默认为75秒。超过该时间阈值，会话中无数据传输则断开连接。
当前 TCP 连接的超时时间暂时不支持调整，默认为900秒。超过该时间阈值，会话中无数据传输则断开连接。

配置会话保持

1. 登录负载均衡控制台，单击需要配置会话保持的负载均衡实例 ID，进入负载均衡详情页。
2. 选择【监听器管理】标签页。
3. 单击需要配置会话保持的负载均衡监听器后的【修改】。
4. 选择是否需要开启会话保持功能，单击按钮开启，输入保持时间，单击【确定】。

长连接和会话保持的关系

场景1：HTTP 七层业务

假设 Client 端访问是 HTTP/1.1 协议，头部信息中设置 Connection:keep-alive。通过 CLB，再访问到后端 CVM，此时不开会话保持，下一次访问，能否访问到同一台 CVM？

答：不能。

首先，HTTP keep-alive 是指 TCP 连接在发送后将仍然保持打开状态，于是，浏览器可以继续通过相同的连接发送请求。保持连接节省了为每个请求建立新连接所需的时间，还节约了带宽。CLB 集群的默认超时时间是75秒（75秒内无新请求刷新，则默认断开 TCP 连接）。

HTTP keep-alive 是由 Client 端跟 CLB 建立的，若此时没有开启 Cookie 会话保持，则下一次访问，CLB 会根据轮询策略，随机挑选后端的一台CVM，此前的长连接等于白费了。

因此建议开启会话保持。

当设置 Cookie 会话保持的时间为1000秒时，Client 端再次发起请求。由于距离上一次请求，已经超过了75秒，TCP 的连接要重新建立。应用层判断 Cookie，找到同一台 CVM，Client 访问的 CVM 还是上一次访问的那一台。

场景2：TCP 四层业务

假设 Client 端发起访问，传输层协议是 TCP，启用长连接。但没有开基于源 IP 的会话保持。下一次访问，同一个 Client，能否访问到同一个机器？

答：不一定。

首先，根据四层的实现机制，当 TCP 启用长连接时，如果该长连接一直没有断开，前后两次访问都是同一条连接，则可以访问到同一台机器。如果第二次访问时，第一条连接由于其他原因（网络重启、连接超时）被释放，这时第二次访问就有可能调度到其他后端云服务器上，且长连接默认全局的超时时间是900秒，即若没有新请求，则释放。

证书配置

常用证书申请流程

- 本地生成私钥：openssl genrsa -out privateKey.pem 2048 ，其中 privateKey.pem 为您的私钥文件，请妥善保管。
- 生成证书请求文件：openssl req -new -key privateKey.pem -out server.csr ，其中 server.csr 是您的证书请求文件，可用其去申请证书。
- 获取请求文件中的内容前往 CA 等机构站点申请证书。

证书格式说明

证书格式要求

- 用户要申请的证书为：Linux 环境下 PEM 格式的证书。负载均衡不支持其他格式的证书，如其它格式的证书请参见下文 “证书转换为 PEM 格式说明“的内容。
- 如果是通过 root CA 机构颁发的证书，您拿到的证书为唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。
- 如果是通过中级 CA 机构颁发的证书，您拿到的证书文件包含多份证书，需要人为的将服务器证书与中间证书合并在一起上传。
- 当您的证书有证书链时，请将证书链内容，转化为 PEM 格式内容，与证书内容合并上传。
- 拼接规则为：服务器证书放第一份，中间证书放第二份，中间不要有空行。

证书格式和证书链格式范例

如下为证书格式和证书链格式范例，请确认格式正确后上传：

1. root CA 机构颁发的证书：证书格式为 Linux 环境下 PEM 格式。样例如下：

证书规则为：

- [———-BEGIN CERTIFICATE———-, ———-END CERTIFICATE———-] 开头和结尾；请将这些内容一并上传。
- 每行64字符，最后一行不超过64字符。

2. 中级机构颁发的证书链：

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

证书链规则为：

- 证书之间不能有空行。
- 每一份证书遵循上文“2.1 证书格式要求”。

RSA 私钥格式要求

样例如下：

RSA 私钥可以包括所有私钥（RSA 和 DSA）、公钥（RSA 和 DSA）和 (x509) 证书。它存储用 Base64 编码的 DER 格式数据，用 ASCII 报头包围，因此适合系统之间的文本模式传输。

RSA 私钥规则：

- [———-BEGIN RSA PRIVATE KEY———-, ———-END RSA PRIVATE KEY———-] 开头结尾，请将这些内容一并上传。
- 每行64字符，最后一行长度可以不足64字符。
  如果您不是按照上述方案生成 [———-BEGIN PRIVATE KEY———-, ———-END PRIVATE KEY———-] 这种格式的可用私钥，您可以按照如下方式转换成可用私钥：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

然后将 new_server_key.pem 的内容与证书一起上传。

证书转换为 PEM 格式说明

目前负载均衡只支持 PEM 格式的证书，其他格式的证书需要转换成 PEM 格式后才能上传到负载均衡中，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为 PEM 格式的方法。

DER 格式证书转换为 PEM 格式

DER 格式一般出现在 Java 平台中。

证书转换： openssl x509 -inform der -in certificate.cer -out certificate.pem

私钥转换： openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem

P7B 格式证书转换为 PEM 格式

P7B 格式一般出现在 Windows Server 和 tomcat 中。

证书转换： openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer

获取 outcertificat.cer 里面 [——-BEGIN CERTIFICATE——-， ——-END CERTIFICATE——-] 的内容作为证书上传。

私钥转换：私钥一般在 IIS 服务器里可导出。

PFX 格式证书转换为 PEM 格式

PFX 格式一般出现在 Windows Server 中。

证书转换： openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

私钥转换： openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes

CER/CRT 格式证书转换为 PEM 格式

对于 CER/CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将 “servertest.crt” 证书文件直接重命名为 “servertest.pem” 即可。

七层重定向配置

负载均衡支持七层重定向，该功能支持用户在七层 HTTP/HTTPS 监听器上配置重定向。

> 说明：
>
> 会话保持：如果客户端访问了 example.com/bbs/test/123.html ，且后端 CVM 开启了会话保持。当启用重定向后，将流量导到 example.com/bbs/test/456.html 时，原会话保持机制将失效。

重定向概述

1. 自动重定向
   - 简介
     系统自动为已存在的 HTTPS:443 监听器创建 HTTP 监听器进行转发，默认使用 80 端口。创建成功后可以通过 HTTP:80 地址自动跳转为 HTTPS:443 地址进行访问。
   - 使用场景
     强制 HTTPS 跳转，即 HTTP 强转 HTTPS。PC、手机浏览器等以 HTTP 请求访问 Web 服务，CLB 会将所有 HTTP:80 的请求重定向至 HTTPS:443 进行转发。
   - 方案优势
     - 仅需1次配置：一个域名，一次配置即可完成强制 HTTPS 跳转。
     - 更新方便：若 HTTPS 服务的 URL 有增减，只需要在控制台，重新使用该功能刷新一遍即可。
2. 手动重定向
   - 简介
     您可以配置一对一重定向，如在某个 CLB 实例中，配置 监听器1 / 域名1 / URL1 重定向至 监听器2 / 域名2 / URL2 。
   - 使用场景
     单路径的重定向。如 Web 业务需要临时下线（如电商售罄、页面维护，更新升级时），此时需将原有页面重定向至新页面。如果不做重定向，用户的收藏和搜索引擎数据库中的旧地址只能让访客得到一个 404/503 错误信息页面，降低了用户体验度，导致访问流量白白丧失。

自动重定向

CLB 支持一键式的 HTTP 强转 HTTPS。
假定开发者需要配置网站 https://www.example.com 。开发者希望用户在浏览器中输入网址时，不论是 HTTP 请求（ http://www.example.com ）还是 HTTPS 请求（ https://www.example.com ），都可通过 HTTPS 协议进行安全访问。

前提条件

已配置 HTTPS:443 监听器。

操作步骤

1. 请在负载均衡控制台完成 CLB 的 HTTPS 监听器的配置，搭建 https://example.com 的 Web 环境。详情请参见 配置 HTTPS 监听器。

2. 完成 HTTPS 监听器配置。

3. 在 CLB 实例详情的“重定向配置”标签页中，单击【新建重定向配置】。

4. 选择【自动重定向配置】，并选择已配置的 HTTPS 监听器和域名，在“域名配置”中选择重定向状态码，单击【下一步：配置路径】。

> 说明：
>
> 状态码301（Moved Permanently）、302（Move Temporarily）、307（Temporary Redirect），详情请参见 HTTP / 1.1标准（RFC 7231）。

5. 单击【提交】即可完成配置。

6. 完成重定向配置后，可以看到已为 HTTPS:443 监听器自动配置了 HTTP:80 监听器，且 HTTP 的流量均会被自动重定向到 HTTPS。

手动重定向

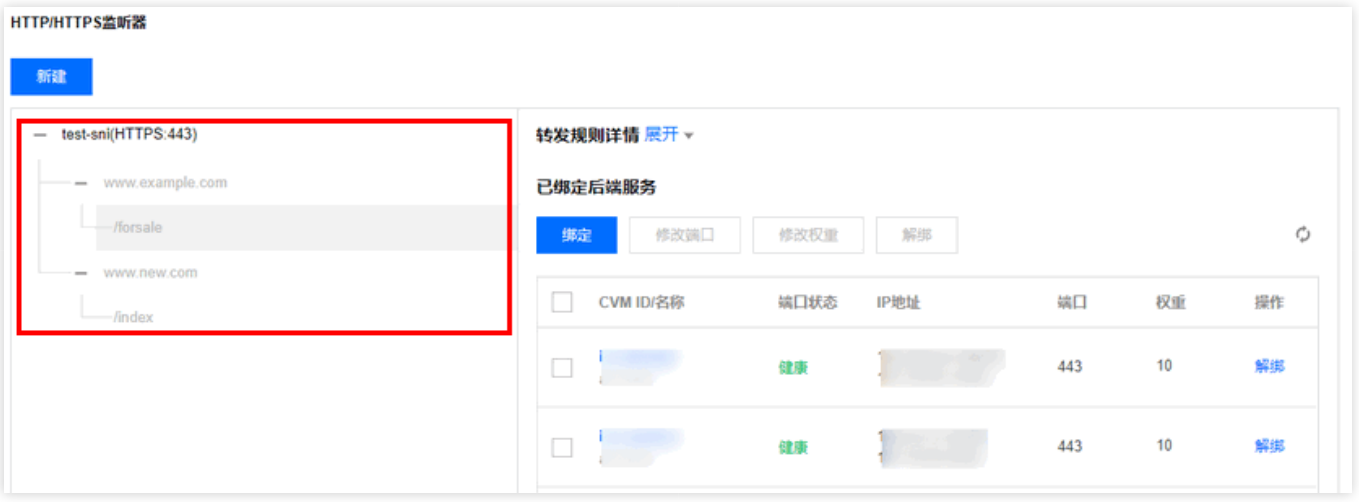
CLB 支持配置一对一的重定向跳转。
例如，业务使用 forsale 页面来做运营活动，现在活动结束需要将活动页面 https://www.example.com/forsale 重定向至新主页 https://www.new.com/index 。

前提条件

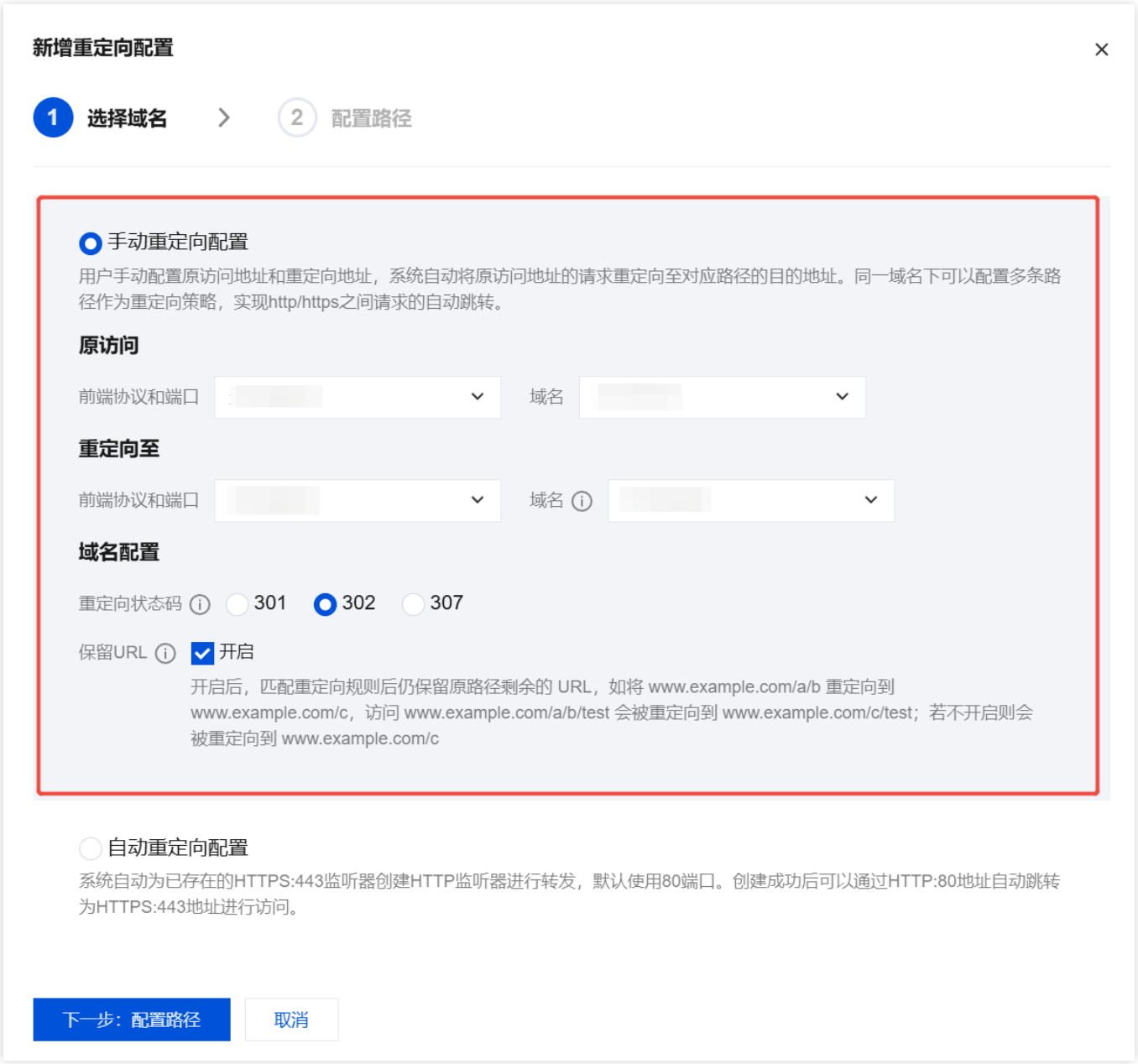
- 已配置 HTTPS 监听器。
- 已配置转发域名 https://www.example.com/forsale 。
- 已配置转发域名和路径 https://www.new.com/index 。

操作步骤

1. 请在负载均衡控制台完成 CLB 的 HTTPS 监听器的配置，搭建 https://example.com 的 Web 环境。详情请参见 配置 HTTPS 监听器。
2. 完成 HTTPS 监听器配置。



3. 在 CLB 实例详情的“重定向配置”标签页中，单击【新建重定向配置】。
4. 选择【手动重定向配置】，选择原访问的前端协议端口 HTTPS:443 和域名 https://www.example.com/forsale ，选择重定向后的前端协议端口 HTTPS:443 和域名 https://www.new.com/index ，在“域名配置”中选择重定向状态码，选择保留 URL 或不保留 URL，单击【下一步：配置路径】。



5. 原访问路径选择 /forsale ，重定向后的访问路径选择 /index ，单击【提交】即可完成配置。
6. 完成重定向配置后的结果，可以看到 HTTP:443 监听器中， https://www.example.com/forsale 已重定向至 https://www.new.com/index 。

七层个性化配置

CLB 支持个性化配置功能，允许设置单 CLB 实例的配置参数，如 client_max_body_size，ssl_protocols 等，满足您的个性化配置需求。

> 说明：
>
> - 个性化配置的个数限制与租户的公网 CLB 配额一致，例如公网 CLB 配额默认为200个，则个性化配置的个数限制为200个。
> - 个性化配置的长度限制为64k。
> - 当前一个实例仅允许绑定一个个性化配置。
> - 个性化配置仅针对负载均衡的七层 HTTP/HTTPS 监听器生效。

CLB 个性化配置参数说明

当前 CLB 的个性化配置支持如下字段：

配置字段	默认值/建议值	参数范围	说明
ssl_protocols	TLSv1 TLSv1.1 TLSv1.2	TLSv1 TLSv1.1 TLSv1.2	使的 TLS 协议版本。
ssl_ciphers	下	下	加密套件。
client_header_timeout	60s	[30-120]s	获取到 Client 请求头部的超时时间, 超时返回408。
client_header_buffer_size	4k	[1-256]k	存放 Client 请求头部的默认 Buffer 。
client_body_timeout	60s	[30-120]s	获取 Client 请求 Body 的超时时间，不是获取整个 Body 的持续 时间，是指空闲段时间没有传输数据的超时时间，超时返回 408。
client_max_body_size	60M	[1-10240]M	- 默认配置范围为1M-256M，直接配置即可。 - 最持10240M，即10G。当client_max_body_size 的配置范围于256M时，必须设置proxy_request_buffering 的值为 off。

配置字段	默认值/建议值	参数范围	说明
keepalive_timeout	75s	[0-3600]s	Client-Server 连接保持时间，设置为0则禁用连接。
add_header	用户定义添加	-	向客户端返回特定的头部字段，格式为 add_header xxx yyy。
more_set_headers	用户定义添加	-	向客户端返回特定的头部字段，格式为 more_set_headers "A:B"。
proxy_connect_timeout	4s	[4-120]s	upstream 后端连接超时时间。
proxy_read_timeout	60s	[30-3600]s	读取 upstream 后端响应超时时间。
proxy_send_timeout	60s	[30-3600]s	向 upstream 后端发送请求的超时时间。
keepalive_requests	100	[1-10000]	Client-Server 连接上最多能发送的请求数量。
proxy_buffer_size	4k	[1-32]k	Server 响应头的缓冲区，默认为 proxy_buffer 中设置的单个缓冲区，使用 proxy_buffer_size 时，必须同时设置 proxy_buffers。
proxy_buffers	8 4k	[3-8] [4-16]k	缓冲区数量和缓冲区。
proxy_request_buffering	on	on， off	- on 表示缓存客户端请求体：CLB 会缓存请求，全部接收完成后再分块转发给后端 CVM。 - off 表示不缓存客户端请求体：CLB 收到请求后，即转发给后端 CVM，此时会导致后端 CVM 有定性能压。
proxy_set_header	X-Real-Port	- X-Real-Port $remote_port - X-clb-stgw-vip $server_addr - Stgw-request-id $stgw_request_id - X-Forwarded-Port $vport - X-Method $request_method	- X-Real-Port $remote_port 表示客户端端。 - X-clb-lbid $lbid 表示 CLB 的 LBID，是 CLB 实例

配置字段	默认值/建议值	参数范围	说明
	$remote_port	- X-Uri $uri	的标识。 - Stgw-request-id $stgw_request_id 表示请求 ID （CLB 内部使）。 - X-Forwarded-Port 表示 CLB 监听器的端。 - X-Method 表示客户端请求法。 - X-Uri 表示客户端请求路径URI。
send_timeout	60s	[1-3600]s	服务端向客户端传输数据的超时时间，是连续两次发送数据的间隔时间，整个请求传输时间。
ssl_verify_depth	1	[1， 10]	设置客户端证书链中的验证深度。
proxy_redirect	http:// https://	http:// https://	当上游服务器返回的响应是重定向或刷新请求（如 HTTP 响码是301或者302）时，proxy_redirect 重设 HTTP 头部的 Location 或 Refresh 字段中的 http 为 https ，实现安全跳转。
http2_max_field_size	4k	[1-256]k	限制 HPACK 压缩的请求头字段的最（Size ）。
error_page	-	error_page code [= [response]] uri	当发特定错误码（Code）的时候，能够显示个预定义的 URI，默认状态码（Response）为 302 。URI 必须是以 / 开头的路径。
proxy_ignore_client_abort	off	on， off	当客户端不等待响应结果主动中断与 CLB 的连接时，配置 CLB 与 后端服务器的连接是否中断。

ssl_ciphers 配置说明

配置 ssl_ciphers 加密套件时，格式需同 OpenSSL 使用的格式保持一致。算法列表是一个或多个 <cipher strings> ，多个算

法间使用":"隔开，ALL 表示全部算法，"!"表示不启用该算法，"+"表示将该算法排到最后一位。
默认强制禁用的加密算法为： !aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE。
默认值：

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-CHACHA20-POLY1305:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128:AES256:AES:HIGH:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE:3DES;

参数范围：

ECDH-ECDSA-AES128-SHA256:ECDH-RSA-AES256-SHA:ECDH-ECDSA-AES256-SHA:SRP-DSS-AES-256-CBC-SHA:SRP-AES-128-CBC-SHA:ECDH-RSA-AES128-SHA256:DH-RSA-AES128-SHA256:DH-RSA-CAMELLIA128-SHA:DH-DSS-AES256-GCM-SHA384:DH-RSA-AES256-SHA256:AES256-SHA256:SEED-SHA:CAMELLIA256-SHA:ECDH-RSA-AES256-SHA384:ECDH-ECDSA-AES128-GCM-SHA256:DH-RSA-AES128-SHA:DH-RSA-AES128-GCM-SHA256:DH-DSS-AES128-SHA:ECDH-RSA-AES128-SHA:DH-DSS-CAMELLIA256-SHA:SRP-AES-256-CBC-SHA:DH-DSS-AES128-SHA256:SRP-RSA-AES-256-CBC-SHA:ECDH-ECDSA-AES256-GCM-SHA384:ECDH-RSA-AES256-GCM-SHA384:DH-DSS-AES256-SHA256:ECDH-ECDSA-AES256-SHA384:AES128-SHA:DH-DSS-AES128-GCM-SHA256:AES128-SHA256:DH-RSA-SEED-SHA:ECDH-ECDSA-AES128-SHA:IDEA-CBC-SHA:AES128-GCM-SHA256:DH-RSA-CAMELLIA256-SHA:CAMELLIA128-SHA:DH-RSA-AES256-GCM-SHA384:SRP-RSA-AES-128-CBC-SHA:SRP-DSS-AES-128-CBC-SHA:ECDH-RSA-AES128-GCM-SHA256:DH-DSS-CAMELLIA128-SHA:DH-DSS-SEED-SHA:AES256-SHA:DH-RSA-AES256-SHA:kEDH+AESGCM:AES256-GCM-SHA384:DH-DSS-AES256-SHA:HIGH:AES128:AES256:AES:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!DHE

CLB 个性化配置示例

1. 登录负载均衡控制台，在左侧导航栏单击【个性化配置】。
2. 在"个性化配置"页面，单击【新建】。
3. 在弹出的"配置信息"对话框，填写配置名和代码配置项，代码配置项以;结尾。配置完成后，单击【完成】。

> 说明：
>
> 默认配置代码示例：
>
> ```
> ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
> client_header_timeout 60s;
> client_header_buffer_size 4k;
> client_body_timeout 60s;
> client_max_body_size 60M;
> keepalive_timeout 75s;
> add_header xxx yyy;
> more_set_headers "A:B";
> proxy_connect_timeout 4s;
> ```

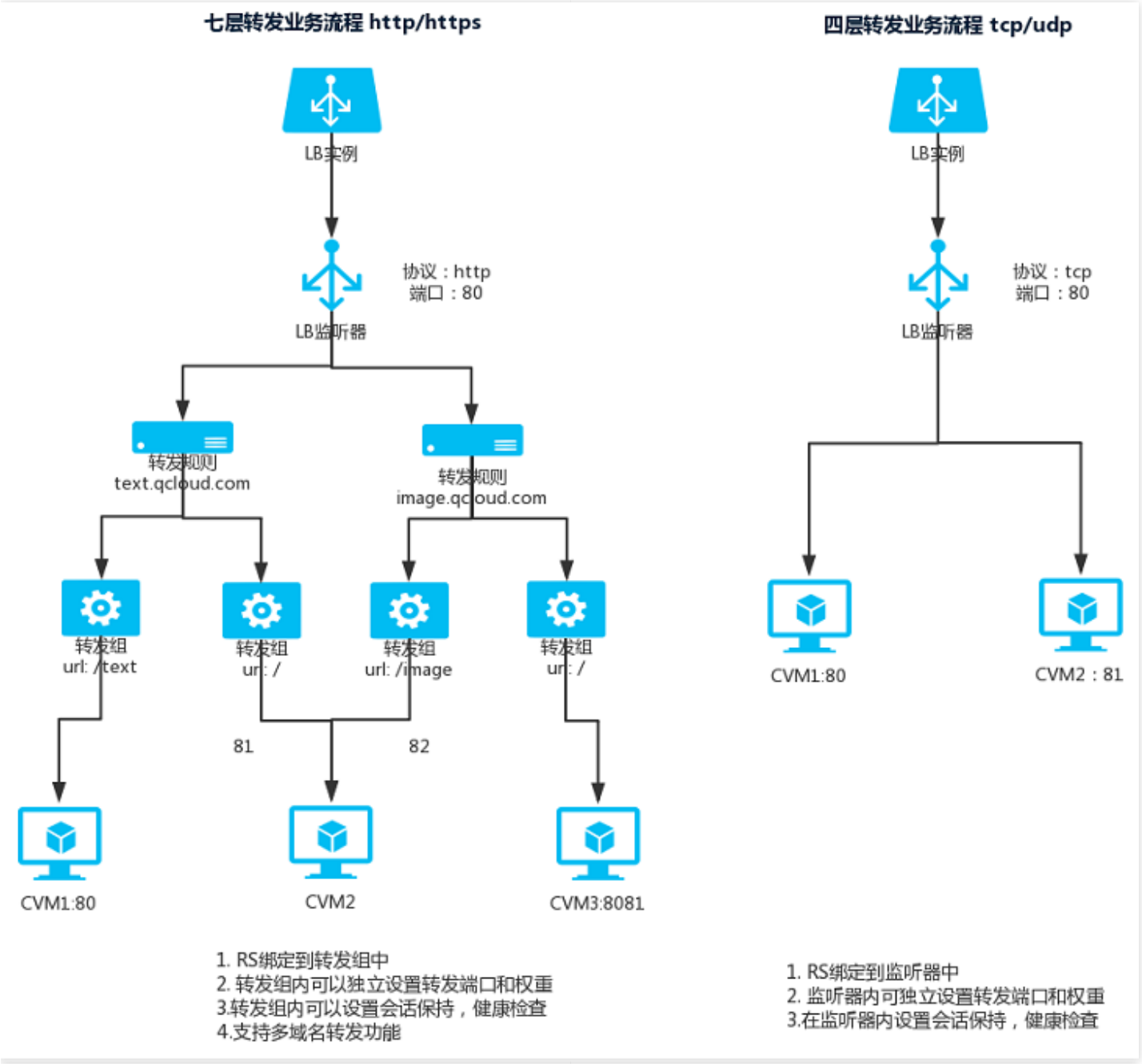
> proxy_read_timeout 60s;
> proxy_send_timeout 60s;

4. 返回“个性化配置”页面，在右侧“操作”栏下单击【绑定至实例】。
5. 在弹出的“绑定至实例”对话框中选择需绑定的负载均衡实例，单击【提交】。
6. 绑定实例后，在“个性化配置”页面单击刚才配置的个性化配置 ID 进入详情页面，单击“绑定实例”页签即可查看到刚才绑定的负载均衡实例。

七层转发域名和URL规则说明

业务流程图

负载均衡的七层业务流程及四层业务流程如下所示：



使用负载均衡的七层转发 HTTP / HTTPS 协议时，在一个 CLB 实例的监听器中新建转发规则，用户可以添加一个对应的域名。

- 当用户仅建立了一条转发规则时，访问 VIP + URL 可以对应相应的转发规则，并正常访问服务。

- 当用户建立了多条转发规则时，此时访问 VIP + URL 不能确保访问到某一个具体的域名 + URL，需要用户直接访问域名 + URL 来确保具体的转发规则生效。即用户配置多条转发规则时，同一个 VIP 对应了多条域名，此时不建议通过 VIP + URL 访问服务，而应该通过具体的域名 + URL 访问服务。

转发规则配置说明

域名配置规则

负载均衡七层监听器的转发规则配置域名时，支持正则表达式，长度限制为1 - 120。

- 非正则的域名支持的字符集如下：
  a-z``0-9``.``-
- 通配的域名，目前仅支持 *.example.com 或者 www.example.* 的形式，且单个域名中仅支持 * 出现一次。
- 域名的正则表达式中不支持的字符集如下：
  "``{``}``;``~`````` 空格`
- 负载均衡支持的正则域名举例如下：
  ~^www\d+\.example\.com$

健康检查配置规则

- 当用户填写的域名为通配域名时，需要指定某一固定域名（非正则）为健康检查域名。该健康检查域名配置支持的字符集如下：
  a-z``0-9``.``-
- 负载均衡七层监听器配置健康检查的路径时，默认 / ，必须以 / 开头，长度限制为1 - 120。暂不支持正则表达，建议指定某个固定 URL 路径（静态页面）进行健康检查。其中，健康检查路径配置支持的字符集如下：
  a-z``A-Z``0-9``.``-``/``=``?

域名匹配规则

1. 转发规则中不配置域名，填写 IP 代替，并在转发组中配置多个 URL，该服务通过 VIP + URL 进行访问。
2. 转发规则中配置完整域名，并在转发组中配置多个 URL，服务通过域名 + URL 进行访问。
3. 转发规则中配置通配符域名，并在转发组中配置多个 URL，通过匹配请求域名 + URL 进行访问。当用户希望不同的域名能够指向相同的 URL 地址时，可以参照这种方式进行配置。以 example.test.com 为例，格式如下所示：

   - example.test.com 精确匹配 example.test.com 域名。
   - *.test.com 匹配所有以 test.com 结尾的域名。
   - example.test.* 匹配所有以 example.test 开头的域名。

4. 转发规则中配置域名，并在转发组中配置模糊匹配的 URL。使用前缀匹配，可在最后加入通配符 $ 进行完整

匹配。
例如，用户通过配置转发组 URL ~* \.(gif|jpg|bmp)$ ，希望匹配任何以 gif、 jpg 或 bmp 结尾的文件。

转发域名中的默认域名策略

您可选择开启或关闭默认域名。

- 开启：当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名。
  - 如果您的七层监听器已配置默认域名，未匹配其他规则的客户端请求会被转发到默认域名。
  - 如果您的七层监听器未配置默认域名，未匹配其他规则的客户端请求则会被转发到 CLB 加载的第一个域名，由于加载顺序与控制台配置顺序可能不一致，因此不一定是控制台配置的第一个。
- 关闭：当客户端请求没有匹配本监听器的任何域名时，请求将无法被转发。

例如，在 CLB1 的 HTTP:80 监听器下配置了2个域名： www.test1.com ， www.test2.com ，其中 www.test1.com 是默认域名。当用户访问 www.example.com 时，由于没有匹配到任何一个域名，CLB会将该请求转发给默认域名 www.test1.com 。

转发组 URL 匹配规则说明

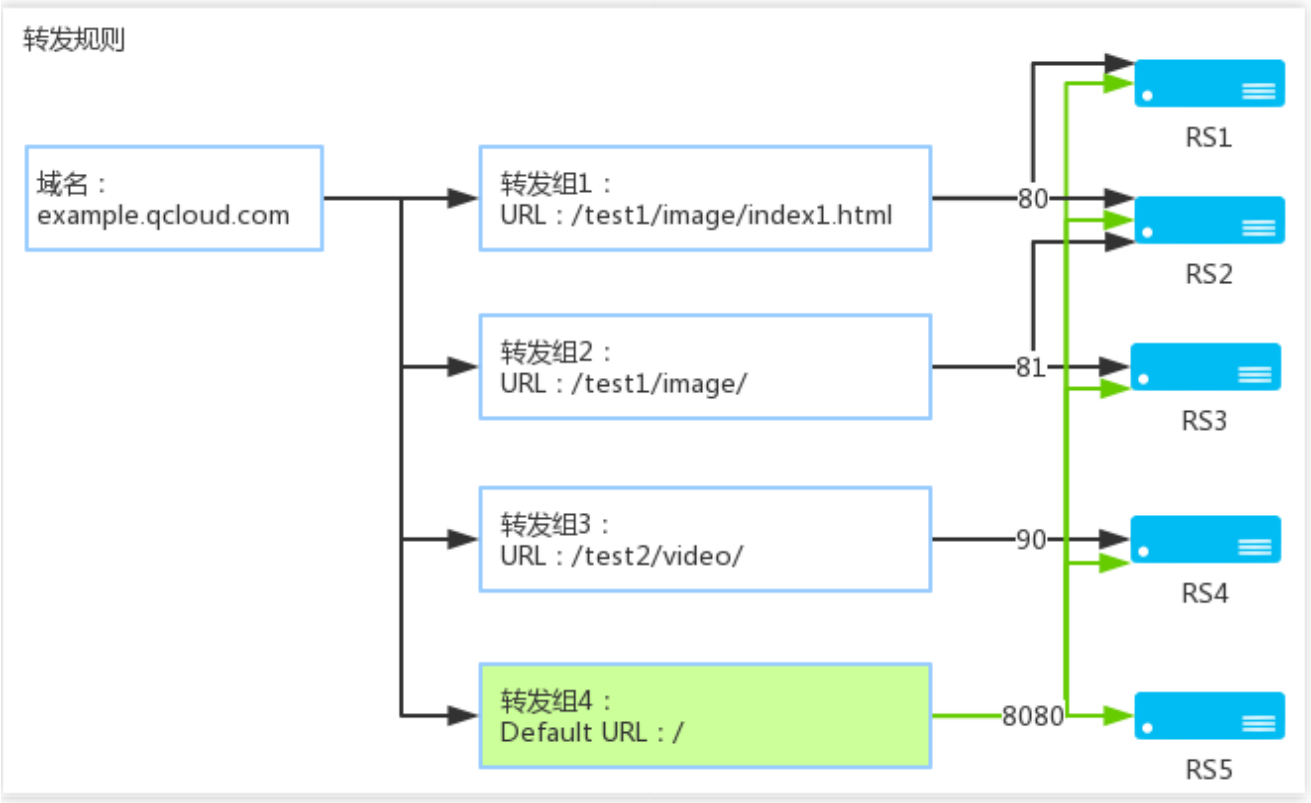
URL 配置规则

负载均衡七层监听器转发路径 URL，默认 / ，必须以 / 开头，长度限制为1 - 120。

- URL 支持正则表达，用如下方法判断：
- = 开头表示精确匹配。
- ^~ 开头表示 URL 以某个常规字符串开头，不是正则匹配。
- ~ 开头表示区分大小写的正则匹配。
- ~* 开头表示不区分大小写的正则匹配。

- / 通用匹配, 如果没有其它匹配，任何请求都会匹配到。
- 非正则的 URL 路径，以 / 开头，支持的字符集如下：
  a-z``A-Z``0-9``.``-``/``=``?
- 正则的 URL，不支持的字符集如下：
  "``{``}``;``\ ``` ~`````空格

URL 匹配规则示例



1. 匹配规则：优先精确匹配，之后依照规则模糊匹配。

例如，依照上图配置转发规则及转发组后，如下请求将依次被匹配到不同的转发组中：

2. example.qloud.com/test1/image/index1.html 由于精确匹配转发组1设置的 URL 规则，则该请求将被转发到转发组1所关联的后端云服务器中，即图中 RS1 和 RS2 的80端口。
3. example.qloud.com/test1/image/hello.html 由于此请求无法精确匹配第一条规则，因此将继续匹配转发组2中的规则，发现模糊匹配成功。因此该请求将被转发到转发组2所关联的后端云服务器中，图中即 RS2 和 RS3 的81端口。
4. example.qloud.com/test2/video/mp4/ 由于此请求无法精确匹配到前两条规则，因此将继续向下匹配，直至发现可以模糊匹配转发组 3 中的规则。因此该请求将被转发到转发组3所关联的后端云服务器中，图中即 RS4 的90端口。
5. example.qloud.com/test3/hello/index.html 由于此请求无法匹配到前三个转发组中的规则，因此将匹配用户配置的最通用规则 Default URL 。这时是 Nginx 转发请求给后端应用服务器，如 FastCGI（php），

tomcat（jsp），Nginx 作为反向代理服务器存在。

6. example.qloud.com/test2/ 由于请求无法精确匹配到前三个转发组中的规则，因此将匹配用户配置的通用规则 default URL 。
7. 如果用户设置的 URL 规则中，服务不能正常运行，则匹配成功后，不会重定向到其他页面。
   例如，客户端请求 example.qloud.com/test1/image/index1.html 匹配了转发组1的 URL 规则，但此时转发组1的后端服务器运行异常，出现404的页面时，用户进行访问时页面则会显示404，不会跳转到其他页面。
8. 建议用户设置 Default URL，将其指向服务稳定的页面（如静态页面、首页等），并绑定所有后端云服务器。
   此时，如果所有规则均没有匹配成功时，系统会将请求指向 Default URL 所在的页面，否则可能会出现404的问题。
9. 如果用户未设置 Default URL，且所有转发规则都不匹配时，此时访问服务，会返回404。

CLB 支持 SNI 多域名证书

服务器名称指示（Server Name Indication，SNI）是用来改善服务器与客户端 SSL/TLS，主要解决一台服务器只能使用一个证书的问题，支持 SNI 表示服务器支持绑定多个证书。客户端使用 SNI，则需在与服务器建立 SSL/TLS 连接之前指定要连接的域名，服务器会根据这个域名返回一个合适的证书。

使用场景

TCloudFinanceZone CLB 的七层 HTTPS 监听器支持 SNI，即支持绑定多个证书，监听规则中的不同域名可使用不同证书。如在同一个 CLB 的 HTTPS:443 监听器中， *.test.com 使用证书1，将来自该域名的请求转发至一组服务器上； *.example.com 使用证书2，将来自该域名的请求转发至另一组服务器上。

前提条件

已 创建负载均衡实例。

操作步骤

1. 登录负载均衡控制台。
2. 参考 配置 HTTPS 监听器 的操作步骤配置监听器，并且在配置 HTTPS 监听器时，开启 SNI。
3. 在该监听器中添加转发规则时，针对不同的域名配置不同的服务器证书，单击【下一步】，继续完成健康检查和会话保持的配置。

后端云服务器
后端云服务器概述

什么是后端云服务器？

后端云服务器是创建负载均衡实例后，绑定在负载均衡上处理相应转发请求的 CVM 实例。在配置 负载均衡监听器 时，需绑定 CVM 实例作为后端服务器，CLB 通过不同的 轮询方式，将请求转发到后端云服务器上，并由 CVM 来做处理，保证应用平稳可靠的运行。您可在负载均衡实例所在的地域内的单个或多个可用区中，绑定 CVM 实例，以增加应用程序的健壮性，屏蔽单点故障。

注意事项

在添加后端服务器时，我们建议您：

- 在要添加到负载均衡上的所有 CVM 实例上，安装 Web 服务器（如 Apache 或 IIS），并保持运行应用程序的一致性。
- 建议您开启 会话保持 功能，使负载均衡维持一个较长时间的 TCP 连接并使多个请求重用它，可减少 Web 服务器上的负载并提高负载均衡的吞吐量。
- 确保后端实例的安全组具有针对负载均衡监听器端口和健康检查端口的入站规则，详情请参见 后端服务器的访问控制。

添加、修改和解绑后端服务器

负载均衡将请求路由至运行正常的后端云服务器实例，首次使用负载均衡或根据业务需求，需要增删后端服务器数量时，可按照下文指引进行操作。

> - 解绑后端服务器会解除负载均衡实例与云服务器实例的关联关系，且负载均衡会立即停止对其的请求转发。
> - 解绑后端服务器不会对云服务器的生命周期产生任何影响，您也可以再次将它添加至后端服务器集群中。
> - 如果负载均衡实例与某个弹性伸缩组关联，则该组中的云服务器会自动添加至负载均衡后端云服务器，从弹性伸缩组移除的云服务器实例会自动从负载均衡后端云服务器中删除。

添加负载均衡后端云服务器

1. 登录负载均衡控制台，在列表中，单击相应的负载均衡实例 ID，进入负载均衡详情页。

2. 在实例对应的监听器中，添加相应的后端云服务器。

   > 说明：
   >
   > IPv4负载均衡支持绑定云服务器和裸金属服务器，绑定方法相同；IPv6仅支持绑定云服务器的弹性网卡。

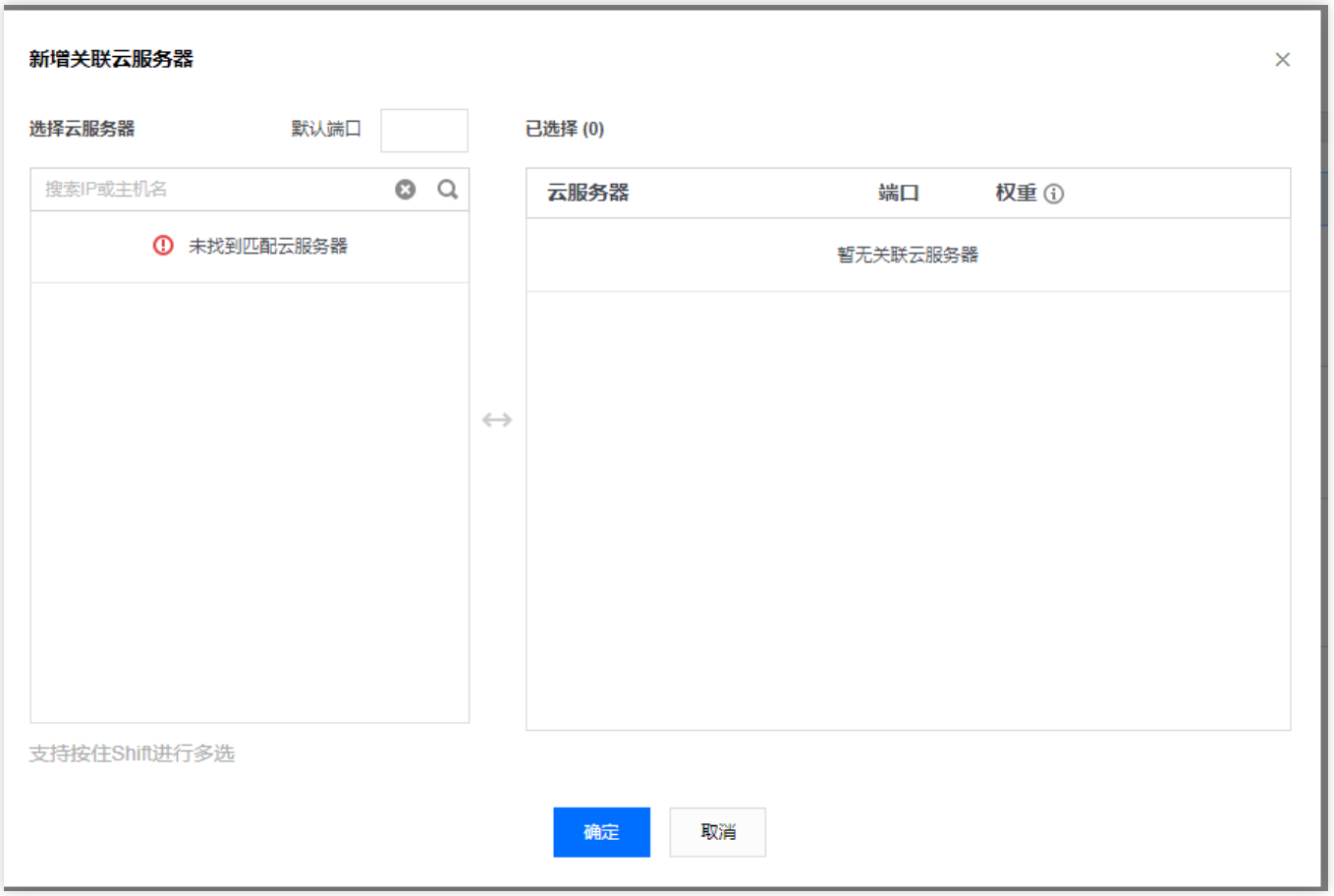
   - TCP/UDP 监听器

选中需要绑定后端云服务器的监听器，单击【绑定】。

- HTTP/HTTPS 监听器
  选中需要绑定后端云服务器的监听器，单击【绑定】。

3. 在弹框中，选择需要关联的云服务器，填写相关云服务器需要被转发的端口与权重，单击【确定】，即可完成云服务器与负载均衡关联操作。

> 说明：
>
> 弹框中仅展示同地域、相同网络环境、未被隔离、未过期、带宽（峰值）不为0的可选云服务器。



4. 如果需要批量绑定服务器且预设端口值一致时，可先在【默认端口】处输入预设端口值、再勾选相关服务器并设定权

重值，单击【确定】，即可完成绑定。

修改负载均衡后端服务器权重

后端服务器权重决定了云服务器被转发的请求相对数量，在绑定后端云服务器时，需要预设权重信息，后续如需修改权重，可请参考下文指引。有关负载均衡后端服务器权重的更多信息，请参见 负载均衡轮询方式。

1. 登录负载均衡控制台，在列表中，单击相应的负载均衡实例 ID，进入负载均衡详情页。
2. 选中实例与监听器规则后，在服务器列表中，选择相关服务器，单击编辑图标，输入修改后的权重值，单击【提交】，即可完成对该台服务器权重的修改。
3. 如需批量修改，选择所有相关服务器后，单击【修改权重】，输入修改后的权重值，单击【提交】，即可完成批量修改。

修改负载均衡后端服务器端口

1. 登录负载均衡控制台，在列表中，单击相应的负载均衡实例 ID，进入负载均衡详情页。
2. 选中实例与监听器规则后，在服务器列表中，选择相关服务器，单击【编辑】，输入修改后的端口值，单击【提交】，即可完成对该台服务器端口的修改。
3. 如需批量修改，选择所有相关服务器后，单击【修改端口】，输入修改后的端口，单击【提交】，即可完成批量修改。

解绑负载均衡后端服务器

1. 登录负载均衡控制台，在列表中，单击相应的负载均衡实例 ID，进入负载均衡详情页。
2. 选中监听器与规则后，在右端云服务器列表中，选择需要解绑的云服务器，单击【解绑】，在弹出框中，单击【提交】即可。
3. 如果需要批量解绑，选中所有需要解绑的云服务器，单击【解绑】，在弹出框中，单击【提交】即可。

绑定弹性网卡

弹性网卡简介

弹性网卡（Elastic Network Interface，ENI）是一种可以绑定私有网络内 CVM 实例上的虚拟网卡。弹性网卡可以自由地在相同私有网络、可用区下的 CVM 间自由迁移，通过弹性网卡可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。
CLB 的后端服务支持 CVM 和 ENI，即 CLB 支持绑定 CVM 和 ENI。CLB 与后端服务之间使用内网通信，当 CLB 绑定多台 CVM 和 ENI 时，访问流量会被转发到 CVM 的内网 IP 和 ENI 的内网 IP上。

前提条件

ENI 必须先绑定在某台云服务器上，CLB 才能绑定该 ENI。CLB 只做负载均衡转发流量，并不实际处理业务逻辑，因此需要计算资源 CVM 实例来处理用户请求。请先前往【私有网络控制台】，将所需的弹性网卡与云主机做绑定。

操作步骤

1. 您需要先配置负载均衡监听器，详情请参见 负载均衡监听器概述。
2. 单击已创建完毕的监听器，展开域名和 URL 路径，选中具体的 URL 路径，在监听器右侧查看已绑定的后端服务。
3. 单击【绑定】，即可在弹出框中选择需绑定的后端服务器，并配置服务端口和权重，绑定后端服务时，可选择【云服务器】或【弹性网卡】。
   - 云服务器：可绑定与 CLB 同私有网络下所有云服务器主网卡的主内网 IP。
   - 弹性网卡：可绑定与 CLB 同私有网络下除云服务器主网卡的主内网 IP 之外的所有弹性网卡 IP，例如主网卡的辅助内网 IP 和辅助网卡的内网 IP。弹性网卡 IP 种类详情请参见 弹性网卡-相关概念 。

     > 说明：
     >
     > IPv4负载均衡支持绑定云服务器或弹性网卡，IPv6负载均衡仅支持绑定弹性网卡。

4. 单击【确定】完成后端弹性网卡的绑定。

后端云服务器安全组配置说明

CVM 安全组简介

负载均衡的后端云服务器实例可以通过 安全组 进行访问控制，起到防火墙的作用。
您可以将一个或多个安全组与后端云服务器关联，并对每个安全组添加一条或多条规则控制不同服务器的流量访问权限。您可以随时修改某个安全组的规则，新规则会自动应用于与该安全组关联的所有实例。在 私有网络 环境中，您还可以使用 网络ACL 进行访问控制。

CVM 安全组配置说明

在 CVM 的安全组上，需放通 Client IP 和服务端口。
若您使用 CLB 转发业务流量到 CVM 上，为保障健康检查功能，在 CVM 的安全组上需做如下配置：

1. 公网负载均衡：您需要在后端 CVM 的安全组上放通 CLB 的 VIP，CLB 使用 VIP 来探测后端 CVM 的健康状态。
2. 内网负载均衡：CLB 属于 VPC 网络，您需要在后端 CVM 的安全组上放通 CLB 的 VIP（用作健康检查）。

CVM 安全组配置示例

如下示例为通过 CLB 访问 CVM 时，CVM 安全组的配置示例。

- 应用场景 1：
  公网负载均衡，监听器配置为 TCP:80 监听器，后端服务端口为8080，希望只允许 Client IP（ClientA IP 和 ClientB IP）访问负载均衡，则后端服务器安全组入站规则配置如下：

  ```
  ClientA IP + 8080 allow
  ClientB IP + 8080 allow
  CLB VIP    + 8080 allow
  0.0.0.0/130618222416261120  + 8080 drop
  ```

- 应用场景 2：
  公网负载均衡，监听器配置为 HTTP:80 监听器，后端服务端口为8080，希望开放所有 Client IP 的正常访问，则后端服务器安全组入站规则配置如下：

  ```
  0.0.0.0/130618222416261120 + 8080 allow
  ```

- 应用场景 3：
  应用型内网负载均衡，网络类型为 VPC 网络，在 CVM 的安全组上需放通 CLB 的 VIP 来做健康检查。为该 CLB 配置 TCP:80 监听器，后端服务端口为8080，希望只允许 Client IP（ClientA IP 和ClientB IP）访问负载均衡的 VIP，并且希望限制 Client IP 只能访问该 CLB 下绑定的后端主机。

  i. 后端服务器安全组入站规则配置如下：

  ClientA IP + 8080 allow
  ClientB IP + 8080 allow
  CLB VIP + 8080 allow
  0.0.0.0/130618222416261120 + 8080 drop

  ii. 用作 Client 的服务器安全组出站规则配置如下：

  CLB VIP + 8080 allow
  0.0.0.0/130618222416261120 + 8080 drop

- 应用场景 4：黑名单
  如用户需要给某些 Client IP 设置黑名单，拒绝其访问，可以通过配置云服务关联的安全组实现。安全组的规则需要按照如下步骤进行配置：
  1.1. 将需要拒绝访问的 Client IP + 端口添加至安全组中，并在策略栏中选取拒绝该 IP 的访问。
  1.2. 设置完毕后，再添加一条安全组规则，默认开放该端口全部 IP 的访问。
  配置完成后，安全组规则如下：

  clientA IP + port drop
  clientB IP + port drop
  0.0.0.0/130618222416261120 + port accept

  > 注意：

  > - 上述配置步骤有顺序要求，顺序相反会导致黑名单配置失效。
  > - 安全组是有状态的，因此上述配置均为入站规则的配置，出站规则无需特殊配置。

CVM 安全组操作指引

使用控制台管理后端服务器安全组

1. 登录负载均衡控制台，单击相应的负载均衡实例 ID 进入负载均衡详情页。
2. 在 CLB 绑定的云服务器页面中，单击相应的后端服务器 ID 进入云服务器详情页。
3. 单击【安全组】选项卡，即可绑定/解绑安全组。

监控与告警
获取监控数据

云监控为负载均衡和后端实例提供数据收集和数据展示功能。使用云监控，您可以查看负载均衡的统计数据，验证系统是否正常运行并创建相应告警。有关云监控的更多信息，请参见 云监控 产品文档。

TCloudFinanceZone默认为所有用户提供云监控功能，您无需手动开通，只要您使用了负载均衡，云监控即可帮助您收集相关监控数据。您可以通过以下几种方式查看负载均衡的监控数据：

负载均衡控制台

1. 登录负载均衡控制台，单击负载均衡实例 ID 旁的监控图标，即可通过监控浮窗，快速浏览各个实例的性能数据。

2. 单击负载均衡实例 ID，进入负载均衡详情页，单击【监控】选项卡，即可查看当前负载均衡实例的监控数据。

云监控控制台

登录 云监控控制台，单击左侧导航栏中“云产品监控”模块下的负载均衡，单击负载均衡实例 ID 进入监控详情页，即可查看该负载均衡实例的监控数据，展开实例即可查看监听器、后端服务器等的监控信息。

监控指标说明

云监控从运行状态下的负载均衡实例中收集原始数据，并将数据展示为易读的图标形式。统计数据默认保存一个月，您可以观察实例一个月的运行情况，从而更好地了解应用服务的运行情况。

建议您通过云监控控制台查看负载均衡的监控，单击【云产品监控】>【负载均衡】，单击负载均衡实例 ID，进入监控详情页，查看该负载均衡实例的监控数据，展开实例即可查看监听器、后端服务器等的监控信息。

负载均衡实例维度

指标	单位	说明
入带宽	bps	在统计周期内，客户端通过外网访问负载均衡所用的带宽。
出带宽	bps	在统计周期内，负载均衡访问外网所用的带宽。
入包数	个/s	在统计周期内，负载均衡每秒接到的请求数据包数量。
出包数	个/s	在统计周期内，负载均衡每秒发出的数据包数量。

四层监听器（TCP/UDP）维度

四层监听器支持您在如下三个维度查看下表中的各个监控指标：

- 监听器维度。
- 后端云服务器维度。
- 后端云服务的端口维度。

指标	单位	说明
连接数	个	在统计周期内，该监听器上的连接数。
新建连接数	个	在统计周期内，该监听器上新建连接数。
入带宽	bps	在统计周期内，客户端通过外网访问负载均衡所用的带宽。
出带宽	bps	在统计周期内，负载均衡访问外网所用的带宽。
入包数	个/s	在统计周期内，负载均衡每秒接到的请求数据包数量。
出包数	个/s	在统计周期内，负载均衡每秒发出的数据包数量。

七层监听器（HTTP/HTTPS）维度

七层监听器支持您在如下五个维度查看下表中的各个监控指标：

- 监听器维度。
- 域名维度。
- URL 转发路径维度。
- 后端云服务器维度。
- 后端云服务的端口维度。

指标	单位	说明
连接数	个	在统计周期内，该监听器上的连接数。
新建连接数	个	在统计周期内，该监听器上新建连接数。
入带宽	bps	在统计周期内，客户端通过外网访问负载均衡所用的带宽。
出带宽	bps	在统计周期内，负载均衡访问外网所用的带宽。
入包数	个/s	在统计周期内，负载均衡每秒接到的请求数据包数量。
出包数	个/s	在统计周期内，负载均衡每秒发出的数据包数量。
平均响应时间	ms	在统计周期内 CLB 的平均响应时间。
最大响应时间	ms	在统计周期内 CLB 的最大响应时间。
响应超时个数	个	在统计周期内 CLB 响应超时的个数。
每秒钟请求数	个	在统计周期内 CLB 每秒钟的请求数，即为 QPS。
2xx 状态码	个	在统计周期，后端服务器返回 2xx 状态码的个数。
3xx 状态码	个	在统计周期，后端服务器返回 3xx 状态码的个数。
4xx 状态码	个	在统计周期，后端服务器返回 4xx 状态码的个数。
5xx 状态码	个	在统计周期，后端服务器返回 5xx 状态码的个数。
404 状态码	个	在统计周期，后端服务器返回 404 状态码的个数。
502 状态码	个	在统计周期，后端服务器返回 502 状态码的个数。
clb 返回的 3xx 状态码	个	在统计周期，负载均衡 CLB 返回 3xx 状态码的个数。
clb 返回的 4xx 状态码	个	在统计周期，负载均衡 CLB 返回 4xx 状态码的个数。

指标	单位	说明
clb 返回的 5xx 状态码	个	在统计周期，负载均衡 CLB 返回 5xx 状态码的个数。
clb 返回的 404 状态码	个	在统计周期，负载均衡 CLB 返回 404 状态码的个数。
clb 返回的 502 状态码	个	在统计周期，负载均衡 CLB 返回 502 状态码的个数。

> 说明：
>
> 如果您需要查看某监听器下某台云服务器的监控数据，请登录负载均衡控制台，单击负载均衡实例 ID 旁的监控图标，即可通过监控浮窗快速浏览各个实例的性能数据。

配置告警策略

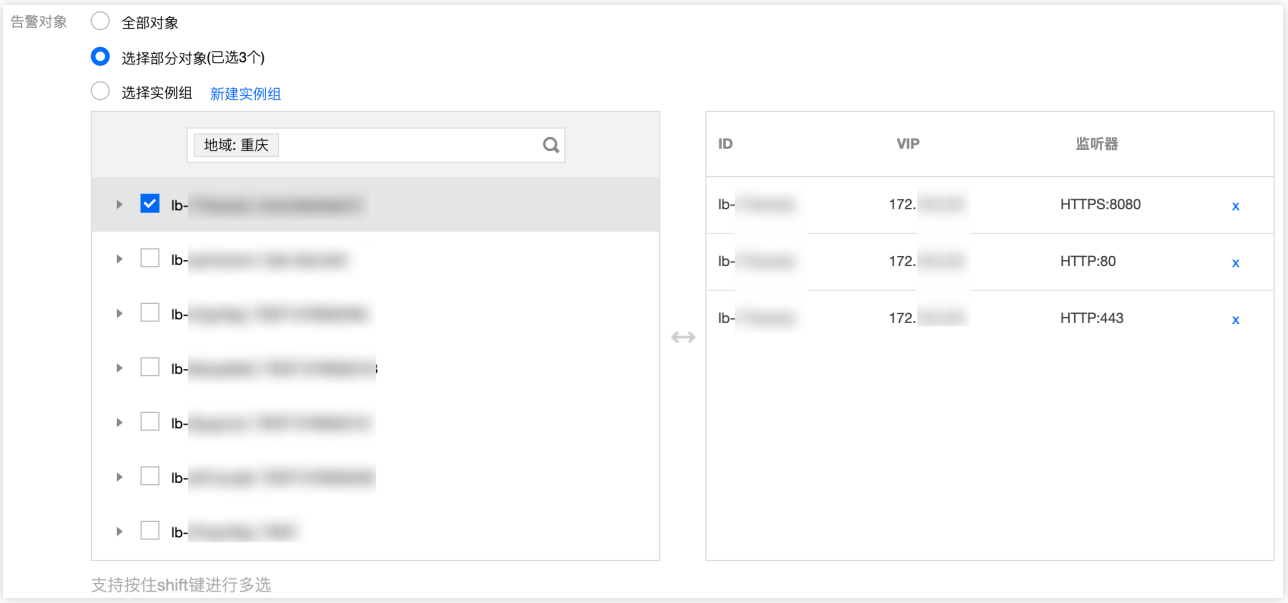
您可以创建告警，使云产品状态达到设定条件时触发警报，并发送相关消息给指定用户群体。创建的告警会依据每隔一段时间监控的指标相对于给定阈值的情况，来判断是否需要触发相关通知。

云产品状态改变导致告警触发后，指定用户可以及时进行相应的预防或补救措施。因此，合理地创建告警能帮助您提高应用程序的健壮性和可靠性。有关告警的更多信息，请参见 创建告警策略。

创建告警策略的详细步骤如下：

1. 登录云控制台，单击【云监控】进入云监控控制台。
2. 在左侧菜单选择【告警配置】>【告警策略】，进入告警策略配置页面。
3. 单击【新增】，配置告警策略。
4. 配置基础选项，配置说明如下。
   - 策略名称：填写策略名称。
   - 备注：填写策略备注。
   - 策略类型：选择监控项。

5. 配置告警对象。
   - 选中全部对象，则该告警策略绑定当前账号的全部实例。
   - 选中选择部分对象，则该告警策略绑定用户选中的实例。
   - 选中选择实例组，则该告警策略绑定用户选中的实例分组。



6. 设置告警触发条件。有两种方式，触发条件模板和配置触发条件，您可选择其中一种触发条件。

   - 触发条件模板

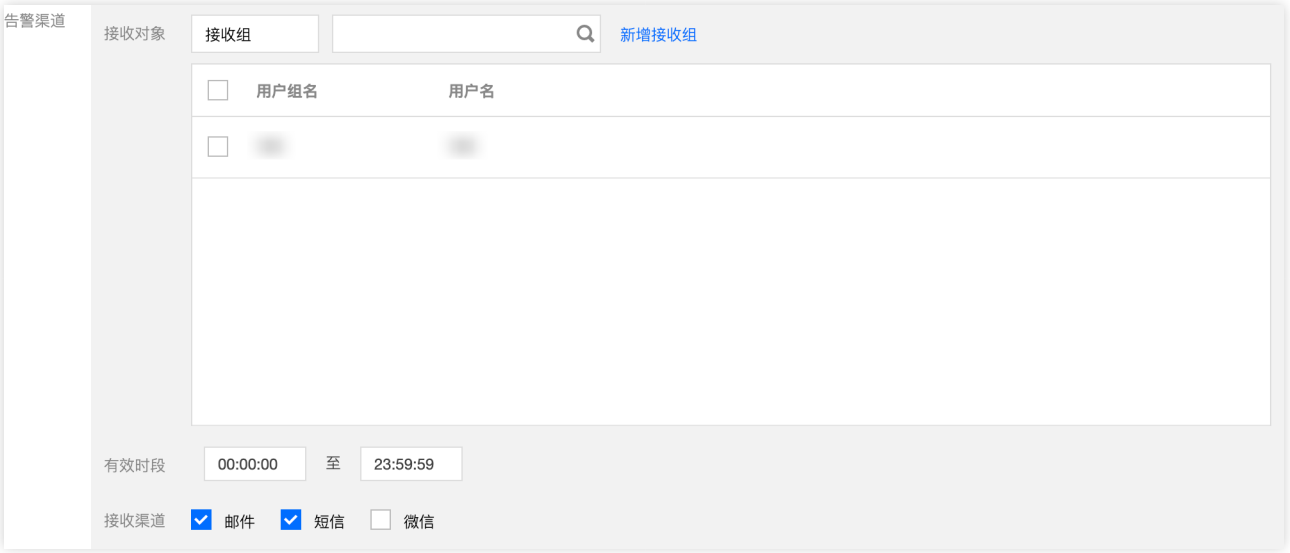
     开启触发条件模板，并在下拉列表选择已配置的模板，具体配置请参阅云监控文档。若新建的模板没有显示，则单击右侧的【刷新】，即可刷新触发告警模版选择列表。
   - 配置触发条件

     告警触发条件是指标、统计周期、比较关系、阈值、持续周期和重复通知组成的一个有语义的条件。

     例如指定指标为 入包量 、统计周期为 1分钟 、比较关系为 > 、阈值为 100个/秒 、持续周期为 持续2个周期 ，重复通知为 每1天警告一次 表示：每1分钟收集一次入包量数据，若某个负载均衡实例监听器的入包量连续两次大于100个/秒，则触发告警，且每天警告一次。

7. 配置告警渠道。

   根据需求，配置告警接收组、有效时段、接收渠道（邮件、对象、微信）。



8. 您可以将已有的策略设为默认告警策略，新购买的负载均衡会自动关联默认策略。
   - 每种策略类型每个项目仅有一个默认策略。
   - 设置为默认的告警策略不可删除。

告警指标说明

告警说明

您可以为您关注的实例指标创建告警，使负载均衡实例在运行状态达到某一条件时，及时发送告警信息至关心的用户群体。这样能确保您及时发现异常状况从而采取相应措施，保持系统的稳定性和可靠性。更多内容请参考 告警概述。负载均衡的告警策略包括如下类型：

- 外网监听器
- 内网监听器
- 服务器端口
- 服务器端口维度

外网监听器/内网监听器

目前公网负载均衡和内网负载均衡均支持监听器维度的告警，具体指标如下：

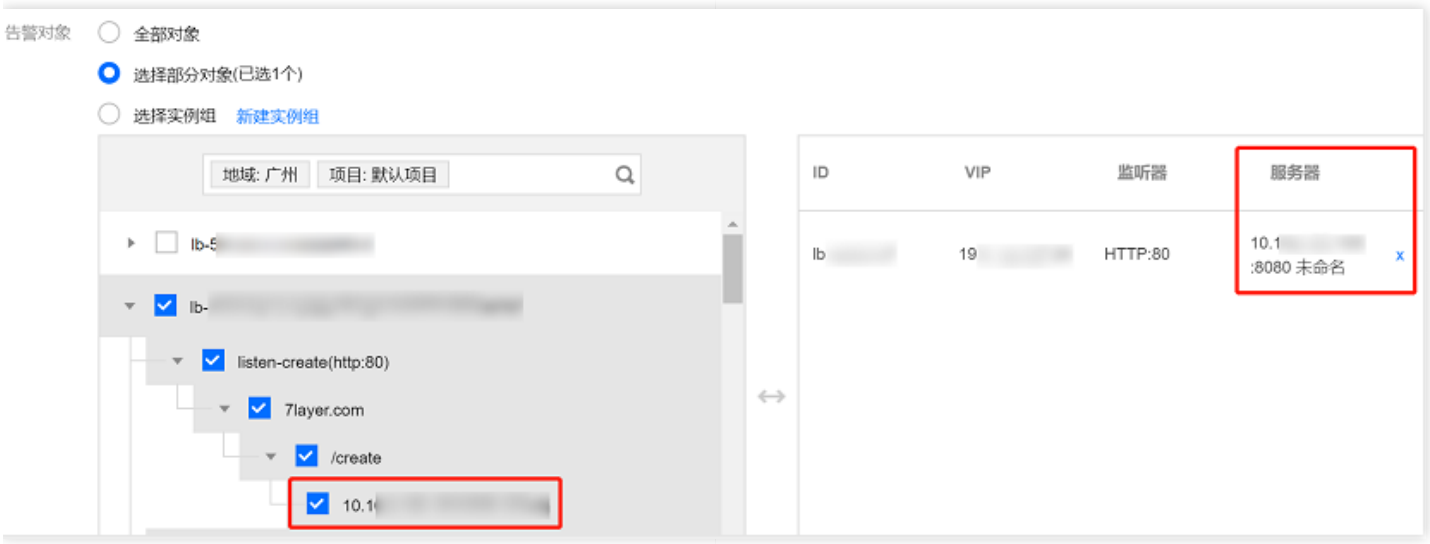
指标	单位	说明
入带宽	bps	在统计周期内，客户端通过外网访问负载均衡所用的带宽。
出带宽	bps	在统计周期内，负载均衡访问外网所用的带宽。
入包数	个/s	在统计周期，内负载均衡每秒接到的请求数据包数量。
出包数	个/s	在统计周期内，负载均衡每秒发出的数据包数量。

服务器端口

负载均衡支持服务器端口维度的告警：

可配置某个监听器绑定的某后端云服务器的某端口的异常告警，只要该端口异常就发送告警。

告警对象配置：



触发条件配置：

> 说明：
>
> 后端服务器端口异常表示：负载均衡探测到后端服务器的该端口不可用，少数网络抖动的情况也会触发端口异常。

证书管理
管理证书

在配置负载均衡的 HTTPS 监听器时，您可以直接使用 SSL 证书服务中的证书或者将所需的第三方签发的服务器证书和SSL证书上传到负载均衡。

证书要求

负载均衡只支持 PEM 格式的证书。在上传证书前，确保您的证书、证书链和私钥符合格式要求。证书要求请参考 证书要求及转换证书格式。

配置证书

为 HTTPS 监听器配置证书分为以下两种类型：

- 不启用 SNI，则在监听器维度配置证书，该监听器下所有域名都使用同一个证书。详情请参考 在监听器维度配置证书。
- 启用 SNI，则在域名维度配置证书，该监听器下可为不同的域名配置不同的证书。详情请参考 在域名维度配置证书。

批量更新证书

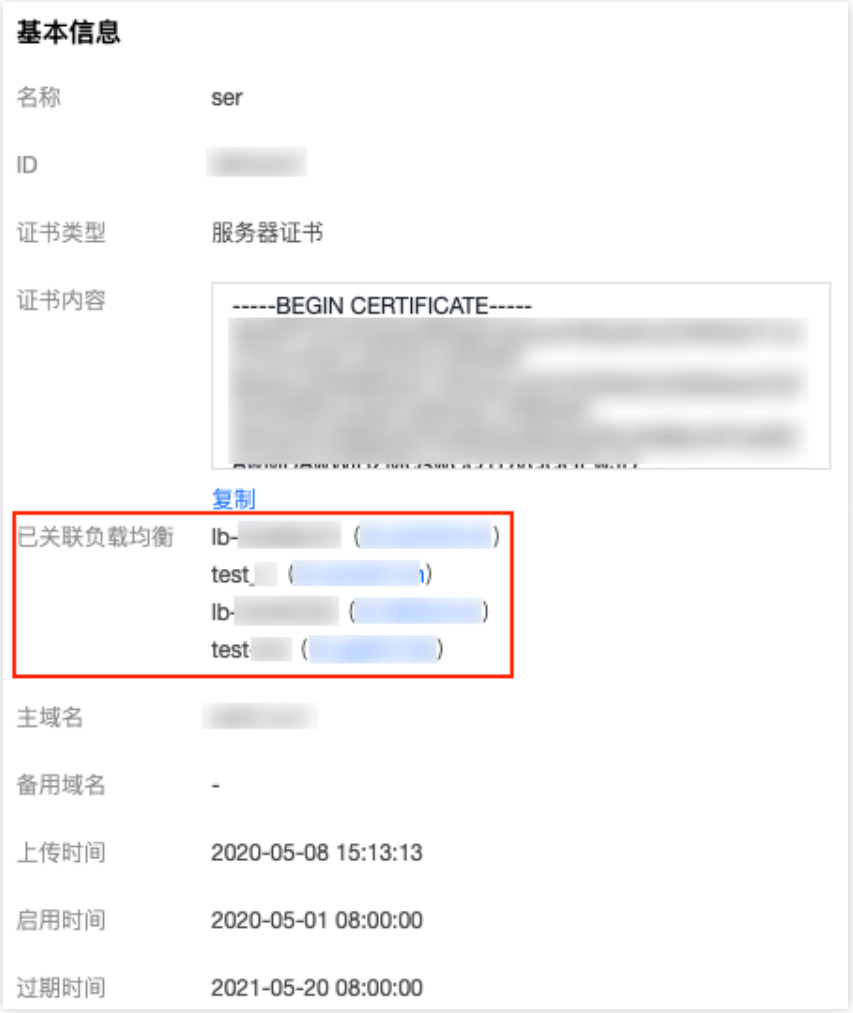
为避免证书过期对您的服务产生影响，请在证书过期前更新证书。

> 说明：
>
> 证书更新后，系统不会删除旧证书，但会生成新证书，所有使用该证书的负载均衡实例将会自动更新证书。

1. 登录负载均衡控制台。
2. 在左侧导航栏单击【证书管理】。
3. 在“证书管理”页面的证书列表中，单击目标证书右侧“操作”列的【更新】。
4. 在弹出的“新建证书”对话框中，填写新证书的证书内容和密钥内容，并单击【提交】。

查看证书关联的负载均衡

1. 登录负载均衡控制台。
2. 在左侧导航栏单击【证书管理】。
3. 在“证书管理”页面的证书列表中，单击目标证书 ID。
4. 在“基本信息”页面，查看证书已关联的负载均衡实例。


基本信息
名称
ser
ID
证书类型
服务器证书
证书内容
-----BEGIN CERTIFICATE-----
复制
已关联负载均衡
lb-
test
lb-
test
主域名
备用域名
-
上传时间
2020-05-08 15:13:13
启用时间
2020-05-01 08:00:00
过期时间
2021-05-20 08:00:00

证书要求及转换证书格式

常用证书申请流程

- 本地生成私钥：openssl genrsa -out privateKey.pem 2048 ，其中 privateKey.pem 为您的私钥文件，请妥善保管。
- 生成证书请求文件：openssl req -new -key privateKey.pem -out server.csr ，其中 server.csr 是您的证书请求文件，可用其去申请证书。
- 获取请求文件中的内容前往 CA 等机构站点申请证书。

证书格式说明

证书格式要求

- 用户要申请的证书为：Linux 环境下 PEM 格式的证书。负载均衡不支持其他格式的证书，如其它格式的证书请参见下文“证书转换为 PEM 格式说明”的内容。
- 如果是通过 root CA 机构颁发的证书，您拿到的证书为唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。
- 如果是通过中级 CA 机构颁发的证书，您拿到的证书文件包含多份证书，需要人为的将服务器证书与中间证书合并在一起上传。
- 当您的证书有证书链时，请将证书链内容，转化为 PEM 格式内容，与证书内容合并上传。
- 拼接规则为：服务器证书放第一份，中间证书放第二份，中间不要有空行。

  > 一般情况下，机构在颁发证书的时候会有对应说明，请注意查阅。

证书格式和证书链格式范例

如下为证书格式和证书链格式范例，请确认格式正确后上传：

1. root CA 机构颁发的证书：证书格式为 Linux 环境下 PEM 格式。样例如下：

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626gg0oJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

证书规则为：

- [———-BEGIN CERTIFICATE———-, ———-END CERTIFICATE———-] 开头和结尾；请将这些内容一并上传。
- 每行64字符，最后一行不超过64字符。

2. 中级机构颁发的证书链：

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

证书链规则为：

- 证书之间不能有空行。
- 每一份证书遵循上文“2.1 证书格式要求”。

RSA 私钥格式要求

样例如下：

RSA 私钥可以包括所有私钥（RSA 和 DSA）、公钥（RSA 和 DSA）和 (x509) 证书。它存储用 Base64 编码的 DER 格式数据，用 ASCII 报头包围，因此适合系统之间的文本模式传输。

RSA 私钥规则：

- [———-BEGIN RSA PRIVATE KEY———-, ———-END RSA PRIVATE KEY———-] 开头结尾，请将这些内容一并上传。
- 每行64字符，最后一行长度可以不足64字符。
  如果您不是按照上述方案生成 [———-BEGIN PRIVATE KEY———-, ———-END PRIVATE KEY———-] 这种格式的可用私钥，您可以按照如下方式转换成可用私钥：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

然后将 new_server_key.pem 的内容与证书一起上传。

证书转换为 PEM 格式说明

目前负载均衡只支持 PEM 格式的证书，其他格式的证书需要转换成 PEM 格式后才能上传到负载均衡中，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为 PEM 格式的方法。

DER 格式证书转换为 PEM 格式

DER 格式一般出现在 Java 平台中。

证书转换： openssl x509 -inform der -in certificate.cer -out certificate.pem

私钥转换： openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem

P7B 格式证书转换为 PEM 格式

P7B 格式一般出现在 Windows Server 和 tomcat 中。

证书转换： openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer

获取 outcertificat.cer 里面 [——-BEGIN CERTIFICATE——-， ——-END CERTIFICATE——-] 的内容作为证书上传。

私钥转换：私钥一般在 IIS 服务器里可导出。

PFX 格式证书转换为 PEM 格式

PFX 格式一般出现在 Windows Server 中。

证书转换： openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

私钥转换： openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes

CER/CRT 格式证书转换为 PEM 格式

对于 CER/CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将 “servertest.crt” 证书文件直接重命名为 “servertest.pem” 即可。

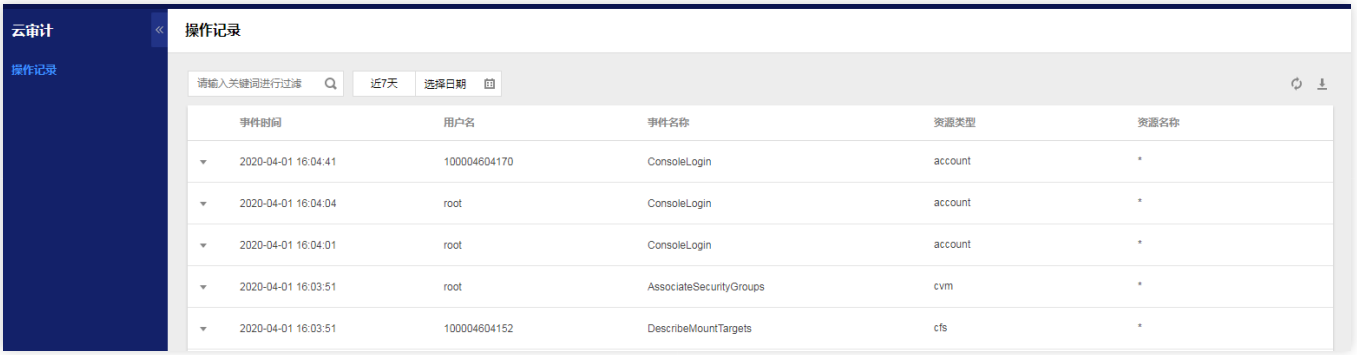
日志管理
查看操作日志

您可以在 云审计控制台 查询、下载负载均衡的操作记录。

云审计（CloudAudit）是一项支持对您的TCloudFinanceZone账号进行监管、合规性检查、操作审核和风险审核的服务。CloudAudit 提供TCloudFinanceZone账号活动的事件历史记录，这些活动包括通过TCloudFinanceZone管理控制台、API服务、命令行工具和其他云服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和问题排查工作。

操作步骤

1. 登录 云审计控制台。
2. 在操作记录页面中，您可以根据用户名、资源类型、资源名称、事件源、事件 ID 等查询操作记录，默认情况下仅展示部分数据，可在页面下方单击【点击加载更多】来获取更多记录。



3. 您如果想更进一步了解单个操作记录，单击该操作记录左侧的 ，即可查看操作记录的详情，包括访问密钥、错误码、事件 ID 等。同时，可以单击【查看事件】，进行了解事件的相关信息。

4.

配置访问日志

负载均衡的访问日志收集了每个客户端请求的详细信息，日志中记录了请求时间、请求路径、客户端 IP 和端口、返回码、响应时间等信息。访问日志可以帮助您了解客户端请求、辅助排查问题、分析梳理用户行为等。当前访问日志支持存储到 CLS 中，支持分钟粒度的日志上报，在线多规则检索。
负载均衡的访问日志主要用于故障排查，帮助业务快速定位问题。访问日志功能包括日志上报、日志存储和查询。

> 说明：
>
> - 仅 IPv4 版本的负载均衡支持配置访问日志，IPv6 和 IPv6 NAT64 版本不支持。
> - 仅七层负载均衡支持配置访问日志，四层负载均衡不支持。
> - 公网和内网网络类型的负载均衡均支持配置访问日志。

步骤一：开启访问日志存入 CLS

1. 登录负载均衡控制台，单击左侧导航栏的【LB 实例列表】。

2. 在“LB 实例列表”页面，单击目标负载均衡 ID。

3. 在“基本信息”页面的“访问日志（七层）”模块，单击铅笔图标开启日志服务 CLS。

4. 在弹出的“授权”对话框中，单击【前往访问管理】，然后单击【同意授权】。

5. 授权成功后，返回实例详情页面，单击铅笔图标，在弹出的“修改 CLS 日志存放位置”对话框，开启“启用日志”，并选择存储访问日志的日志集和日志主题，单击【提交】。若您没有创建日志集或日志主题，请新建相关资源后，再选取具体的存储位置。

> 说明：
>
> 建议选择 clb_logset 日志集下带“CLB”标识的日志主题。带“CLB”标识的日志主题和普通日志主题的差异在于：
>
> - 带“CLB”标识的日志主题默认自动创建索引；普通日志主题需手动创建索引，否则不支持检索。
> - 带“CLB”标识的日志主题默认支持仪表盘；普通日志主题需手动配置仪表盘。

6. 配置完成后单击日志集或日志主题即可跳转到 CLS 控制台的检索分析页面。

7. （可选）若想关闭访问日志，可再次单击铅笔图标，在弹出的“修改 CLS 日志存放位置”对话框中进行关闭并提交即可。

步骤二：配置日志主题的索引

> 说明：
>
> 为单实例配置的访问日志的日志主题必须配置索引，否则检索不到日志。

建议配置的索引如下：

键值索引	字段类型	分词符
server_addr	text	无需配置分词符
server_name	text	无需配置分词符
http_host	text	无需配置分词符
status	long	-
vip_vpcid	long	-

1. 登录日志服务控制台，在左侧导航栏单击日志主题。
2. 在“日志主题”页面，单击目标日志主题 ID。
3. 在日志主题详情页，单击索引配置页签，单击右上角的编辑，即可添加索引。配置完成后，单击【确定】。

步骤三：查看访问日志

1. 登录日志服务控制台，单击左侧导航栏的【检索分析】。
2. 在“检索分析 ”页面中，选择日志集、日志主题和时间范围，单击检索分析，即可检索 CLB 上报到 CLS 的访问日志。

访问管理

概述

如果您使用到了负载均衡 CLB、云服务器、数据库等服务，这些服务由不同的人管理，但都共享您的云账号密钥，将存在如下问题：

- 您的密钥由多人共享，泄密风险高。
- 您无法限制其它人的访问权限，易产生误操作造成安全风险。
  访问管理（CAM）用于管理云账户下资源访问权限，通过 CAM，您可以通过身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的账户下有多个负载均衡实例部署在不同项目中，为了加强权限控制，对资源进行授权，您可以给项目 A 的管理员绑定一个授权策略，该策略规定：只有该管理员可操作项目 A 下的负载均衡资源。

如果您不需要对子账户进行 CLB 相关资源的访问管理，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用.

CAM 基本概念

根账户通过给子账户绑定策略实现授权，策略设置可精确到 [API，资源，用户/用户组，允许/拒绝，条件] 维度。

1. 账户
   - 根账号：云资源归属、资源使用计量计费的基本主体，可登录TCloudFinanceZone服务。
   - 子账号：由根账号创建账号，有确定的身份ID和身份凭证，且能登录到TCloudFinanceZone控制台。根账号可以创建多个子账号(用户)。子账号默认不拥有资源，必须由所属根账号进行授权。
   - 身份凭证
     包括登录凭证和访问证书两种，登录凭证是指用户登录名和密码，访问证书是指云API密钥（SecretId 和 SecretKey）。
2. 资源与权限
   - 资源：资源是云服务中被操作的对象，如一个云服务器实例，COS 存储桶，VPC 实例等。
   - 权限：权限是指允许或拒绝某些用户执行某些操作。默认情况下，根账号拥有其名下所有资源的访问权限，而子账号没有根账号下任何资源的访问权限。
   - 策略：策略是定义和描述一条或多条权限的语法规范。根账号通过将策略关联到用户/用户组完成授权。

更多相关信息，请参见 CAM 概述。

相关文档

目标	链接
了解策略和用户之间关系	策略管理
了解策略的基本结构	策略语法

授权定义

CAM 中可授权的负载均衡资源类型

资源类型	授权策略中的资源描述方法
负载均衡实例	qcs::clb:$region::clb/$loadbalancerid
负载均衡监听器	qcs::clb:$region::listener/$loadbalancerlistenerid
负载均衡后端服务器	qcs::cvm:$region:$account:instance/$cvminstanceid

其中：

- 所有 $region 应为某个 region 的 ID，可以为空。
- 所有 $account 应为资源拥有者的 AccountId，或者“*”。
- 所有 $loadbalancerid 应为某个 loadbalancer 的 ID，或者“*”。
  以此类推。

CAM 中可对负载均衡进行授权的接口

在 CAM 中，可以对一个负载均衡资源进行以下 Action 的授权。

实例相关

API 操作	资源描述	接口说明
DescribeLoadBalancers	查询负载均衡实例列表	* 只对接口进行鉴权
CreateLoadBalancer	购买负载均衡	qcs:$projectid:clb:$region:$account:clb/*
DeleteLoadBalancers	删除负载均衡	qcs::clb:$region:$account:clb/$loadbalancerid
ModifyLoadBalancerAttributes	修改负载均衡属性信息	qcs::clb:$region:$account:clb/$loadbalancerid
ModifyForwardLBName	修改负载均衡的名字	qcs::clb:$region:$account:clb/$loadbalancerid

监听器相关

API 操作	资源描述	接口说明
DeleteLoadBalancerListeners	删除负载均衡监听器	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
DescribeLoadBalancerListeners	获取负载均衡监听器列表	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/*
ModifyLoadBalancerListener	修改负载均衡监听器属性	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
CreateLoadBalancerListeners	创建负载均衡监听器	qcs::clb:$region:$account:clb/$loadbalancerid
DeleteForwardLBListener	删除负载均衡监听器（四层和七层）	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
ModifyForwardLBSeventhListener	修改负载均衡七层监听的属性	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
ModifyForwardLBFourthListener	修改负载均衡四层监听器属性	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
DescribeForwardLBListeners	查询负载均衡监听器列表	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/*
CreateForwardLBSeventhLayerListeners	创建七层负载均衡监听器	qcs::clb:$region:$account:clb/$loadbalancerid
CreateForwardLBFourthLayerListeners	创建四层负载均衡监听器	qcs::clb:$region:$account:clb/$loadbalancerid

负载均衡域名 + URL 相关

API 操作	资源描述	接口说明
ModifyForwardLBRulesDomain	修改负载均衡监听器转发规则的域名	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid

API 操作	资源描述	接口说明
CreateForwardLBListenerRules	创建负载均衡监听器转发规则	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
DeleteForwardLBListenerRules	删除七层负载均衡监听器规则	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid
DeleteRewrite	删除负载均衡转发规则之间的重定向关系	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$sourceloadbalancerlistenerid``qcs::clb:$region:$account:listener/$targetloadbalancerlistenerid
ManualRewrite	手动添加负载均衡转发规则的重定向关系	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$sourceloadbalancerlistenerid``qcs::clb:$region:$account:listener/$targetloadbalancerlistenerid
AutoRewrite	自动生成负载均衡转发规则的重定向关系	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid

后端服务器相关

API 操作	资源描述	接口说明
ModifyLoadBalancerBackends	修改负载均衡器后端服务器权重	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::cvm:$region:$account:instance/$loadbalancerlistenerid
DescribeLoadBalancerBackends	获取负载均衡绑定的后端服务器列表	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/*
DeregisterInstancesFromLoadBalancer	解绑后端服务器	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::cvm:$region:$account:instance/$cvminstanceid
RegisterInstancesWithLoadBalancer	绑定后端服务器到负载均衡	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::cvm:$region:$account:instance/$cvminstanceid

API 操作	资源描述	接口说明
DescribeLBHealthStatus	查询负载均衡健康状态	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/*
ModifyForwardFourthBackendsPort	修改四层监听器转发规则上云服务器的端口	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
ModifyForwardFourthBackendsWeight	修改四层监听器转发规则上云服务器的权重	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
RegisterInstancesWithForwardLBSeventhListener	绑定云服务器到负载均衡七层监听器的转发规则上	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
RegisterInstancesWithForwardLBFourthListener	绑定云服务器到负载均衡四层监听器的转发规则上	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
DeregisterInstancesFromForwardLBFourthListener	解绑负载均衡四层监听器转发规则上的云服务器	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
DeregisterInstancesFromForwardLB	解绑负载均衡七层监听器转发规则上的云服务器	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid

API 操作	资源描述	接口说明
ModifyForwardSeventhBackends	修改七层监听器转发规则上云服务器的权重	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::cvm:$region:$account:instance/$cvminstanceid
ModifyForwardSeventhBackendsPort	修改七层监听器转发规则上云服务器的端口	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid``qcs::cvm:$region:$account:instance/$cvminstanceid
DescribeForwardLBBackends	查询负载均衡云服务器列表	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::cvm:$region:$account:instance/*
DescribeForwardLBHealthStatus	查询负载均衡健康检查状态	qcs::clb:$region:$account:clb/*
ModifyLoadBalancerRulesProbe	修改负载均衡监听器转发规则的健康检查及转发路径	qcs::clb:$region:$account:clb/$loadbalancerid``qcs::clb:$region:$account:listener/$loadbalancerlistenerid

策略示例

CLB 的全读写策略

- 授权一个子账户以 CLB 服务的完全管理权限（创建、管理等全部操作）。
- 策略名称：CLBResourceFullAccess

```
{
  "version": "2.0",
  "statement": [{
      "action": [
          "name/clb:*"
      ],
      "resource": "*",
      "effect": "allow"
  }]
}
```

CLB 的只读策略

- 授权一个子账户只读访问 CLB 的权限（即可以查看所有 CLB 下面所有资源的权限），但子账户无法创建、更新或删除它们。 在控制台，操作一个资源的前提是可以查看该资源，所以建议您为子账户开通 CLB 全读权限。
- 策略名称： CLBResourceReadOnlyAccess

```
{
  "version": "2.0",
  "statement": [{
      "action": [
          "name/clb:Describe*"
      ],
      "resource": "*",
      "effect": "allow"
  }]
}
```

配额管理

负载均衡支持主账号管理子账号配额，可对子账号配额进行调整。子账号仅可查看配额。

查看子账号配额

1. 登录云平台负载均衡。
2. 在左侧导航栏单击【配额管理】，查看子账号的配额。

管理子账号配额

1. 使用主账号登录云平台负载均衡。
2. 在左侧导航栏单击【配额管理】。
3. 在“配额管理”页面，单击右侧“操作”栏的【设置子账号配额】。
4. 在弹出的“设置子账号配额”对话框中，设置子账号的配额，单击【确定】。

设置子账号配额
主账号总配额：700，主账号已使用配额：1
子账号
设置配额
已使用配额
100004607607（hikeeli）
10
0
100004603443（bingya...
10
0
总计
20
确定
取消

常见问题
健康检查异常排查思路

四层排查

TCP 协议下，负载均衡使用 SYN 包进行探测；UDP 协议下，负载均衡使用 ping 命令进行探测。

在页面查看 CLB 后端服务器端口的健康状态，若不健康，排查思路如下：

- 确定 CLB 后端服务器是否有配置有防火墙影响了服务，如果有请关闭。
- 使用 netstat 命令，确定后端服务器的端口是否有进程在监听，若未启动，则重新启动服务。

七层排查

针对七层（HTTP 协议）服务，当某一监听出现健康检查"异常"时，可以通过如下方面进行排查：

- 由于负载均衡的七层健康检查服务与后端 CVM 之间的通讯是走内网的，您需要登录服务器检查应用服务器端口是否正常监听在内网地址上，如果没有监听在内网地址，请将应用服务器端口监听到内网上，从而确保负载均衡系统和后端 CVM 之间的通讯正常。
  假设负载均衡前端端口是80，CVM 后端端口也是80，CVM 内网 IP 是： 1.1.1.10
  - Windows 系统服务器使用如下命令：

```
netstat -ano | findstr :80
```

- Linux 系统服务器使用如下命令：

```
netstat -anp | grep :80
```

如果能看到 1.1.1.10:80 的监听或 0.0.0.0:80 的监听则说明这部分正常。

- 请确保后端服务器开启了相应的端口，该端口必须与您在负载均衡监听配置中配置的后端端口保持一致。
  - 如果是四层负载均衡，只要后端端口telnet有响应即可，可以使用 telnet 1.1.1.10 80 来测试。
  - 如果是七层负载均衡，需要 HTTP 状态码是200 等代表正常的状态码。检验方法如下：
    - Windows 系统可以直接在 CVM 内的浏览器输入内网IP测试是否正常，本例为： http://1.1.1.10 。
    - Linux 系统可以通过 curl -I 命令查看状态是否为 HTTP/1.1 200 OK，本例是： curl -I 1.1.1.10 。
- 检查后端 CVM 内部是否有防火墙或其他安全类防护软件，这类软件很容易将负载均衡系统的本地 IP 地址屏

蔽，从而导致负载均衡系统无法跟后端服务器进行通讯。

检查服务器内网防火墙是否放行80端口，可以暂时关闭防火墙进行测试。

  - Windows 系统可以运行输入 firewall.cpl 操作关闭。
  - Linux 系统可以输入 /etc/init.d/iptables stop 关闭。

- 检查负载均衡健康检查参数设置是否正确，建议参见 健康检查 提供的健康检查参数默认值进行设置。
- 健康检查指定的检测文件，建议是以 html 形式的简单页面，只用于检查返回结果，不建议用 PHP 等动态脚本语言。
- 检查后端是否有较高负载导致 CVM 对外提供服务响应慢。

客户端timewait过多解决方案

本文背景

客户压测 CLB 时，常会遇到一些客户端 timewait 过多，端口被快速占满，导致 connect 失败的问题，下面会说明原因和解决方案。

Linux 参数介绍

tcp_timestamps ： 是否开启 tcp timestamps 选项，timestamps 是在 tcp 三次握手过程中协商的，任意一方不支持，该连接就不会使用 timestamps 选项。
tcp_tw_recycle ： 是否开启 tcp time_wait 状态回收。
tcp_tw_resuse ： 开启后，可直接回收超过1s的 time_wait 状态的连接。

原因分析

客户端timewait太多，是因为客户端主动断开连接，客户端每断开一个连接，该连接都会进入timewait状态，默认60s超时回收。一般情况下，遇到这种场景时，客户会选择打开 tcp_tw_recycle 和 tcp_tw_resuse 两个参数，便于回收timewait状态连接。
然而当前 CLB 没有打开 tcp_timestamps 选项，导致客户端打开的 tcp_tw_recycle 和 tcp_tw_resuse 都不会生效，不能快速回收 timewait 状态连接。下面会解释几个 Linux 参数的含义和 CLB 不能开启 tcp_timestamps 的原因。

1. tcp_tw_recycle 和 tcp_tw_resuse只有在 tcp_timestamps 打开时才会生效。
2. tcp_timestamps和tcp_tw_recycle是不能同时打开的，因为公网客户端经过 NAT 网关访问服务器，会存在问题，原因如下：

tcp_tw_recycle/tcp_timestamps 都开启的条件下，60s内同一源 IP 主机的 socket connect 请求中的 timestamp 必须是递增的。以2.6.32内核为例，具体实现如下：

```
if (tmp_opt.saw_tstamp &&
    tcp_death_row.sysctl_tw_recycle &&
    (dst = inet_csk_route_req(sk, req)) ! = NULL &&
    (peer = rt_get_peer((struct rtable *)dst)) ! = NULL &&
    peer- >v4daddr == saddr) {
        if (get_seconds() < peer- >tcp_ts_stamp + TCP_PAWS_MSL &&
            (s32)(peer- >tcp_ts -  req- >ts_recent) >
                                TCP_PAWS_WINDOW) {
                NET_INC_STATS_BH(sock_net(sk), LINUX_MIB_PAWSPASSIVEREJECTED);
                goto ↓drop_and_release;
        }
}
```

> 说明：
>
> - tmp_opt.saw_tstamp：该 socket 支持 tcp_timestamp。

- sysctl_tw_recycle：本机系统开启 tcp_tw_recycle 选项。
- TCP_PAWS_MSL：60s，该条件判断表示该源 IP 的上次 tcp 通讯发生在60s内。
- TCP_PAWS_WINDOW：1，该条件判断表示该源 IP 的上次 tcp 通讯的 timestamp 大于本次 tcp。

3. CLB（7层）关闭了 tcp_timestamps 原因，因为公网客户端经过 NAT 网关访问服务器，可能会存在问题，如下例：

4. 某五元组还是 time_wait 状态。NAT网关对端口的分配策略，2MSL内复用了同个五元组，发来syn包。

5. 在开启 tcp_timestamps 情况下，同时满足如下两个条件，会丢弃该 syn 包（因为开启了时间戳选项，认为是老包）。
   i. 上次时间戳 > 本次时间戳。
   ii. 24天内收过包（时间戳字段是32位，Linux 默认1ms更新一次时间戳，24天会发生时间戳回绕）。

备注：在移动端该问题更为明显，因为客户端都是在运营商NAT网关下面共享有限的公网 IP，五元组还可能在2MSL内被复用，不同客户端传来的时间戳不能保证是递增的。
以2.6.32内核为例，具体实现如下：

```
static inline int tcp_paws_check(const struct tcp_options_received *rx_opt,
                        int paws_win)
{
      if ((s32)(rx_opt- >ts_recent -  rx_opt- >rcv_tsval) <= paws_win)
            return 1;
      if (unlikely(get_seconds() >= rx_opt- >ts_recent_stamp + TCP_PAWS_24DAYS))
            return 1;

      return 0;
}
```

> 说明：
>
> - rx_opt->ts_recent：上次的时间戳

- rx_opt->rcv_tsval：本次收到的时间戳
- get_seconds（）： 当前时间
- rx_opt->ts_recent_stamp： 上次收到包的时间

解决方案

客户端 Timewait 过多问题，有如下解决方案：

1. HTTP 使用短连接（Connection: close），这时由 CLB 主动关闭连接，客户端不会产生 timewait。

2. 如果场景需要使用长连接，可以打开 socket 的 SO_LINGER 选项，使用 rst 关闭连接，避免进入 timewait 状态，达到快速回收端口的目的。

负载均衡HTTPS服务性能测试

CLB 负载均衡器 HTTPS 能力说明

TCloudFinanceZone CLB 负载均衡器通过对协议栈及服务端的深度优化，实现了 HTTPS 性能的巨大提升。同时，我们也通过证书的国际合作，极大降低了证书的成本。TCloudFinanceZone CLB 在如下几个方面能够为业务带来非常显著的收益：

1. 使用 HTTPS 并不会降低 Client 端的访问速度。
2. 集群内单台服务器 SSL 加解密性能，高达6.5W cps的完全握手。相比高性能 CPU 提升了至少3.5倍，节省了服务端成本，极大提升了业务运营及流量突涨时的服务能力，增强了计算型防攻击的能力。
3. 支持多种协议卸载及转换。减少业务适配客户端各种协议的压力，业务后端只需要支持 HTTP1.1 就能使用 HTTP2，SPDY，SSL3.0，TLS1.2 等各版本协议。
4. 一站式 SSL 证书申请、监控、替换。我们和国际证书厂商 comodo，symantec 展开对话，探讨合作，大幅缩减证书申请流程及成本。
5. 防 CC 及 WAF 功能。能够有效杜绝慢连接、高频定点攻击、SQL 注入、网页挂马等应用层攻击。

测试目的

HTTPS 服务拥有身份验证，信息加密及完整性校验等优势，但通过新增 SSL 协议实现安全通信，必然会产生一定的性能损耗，主要包括延时的增加及加解密消耗 CPU 资源等方面。本文测试了TCloudFinanceZone HTTPS 服务在 SSL 加解密情况下的极限性能数据，供用户与 HTTPS 传统性能数据进行比对和参考。

测试环境

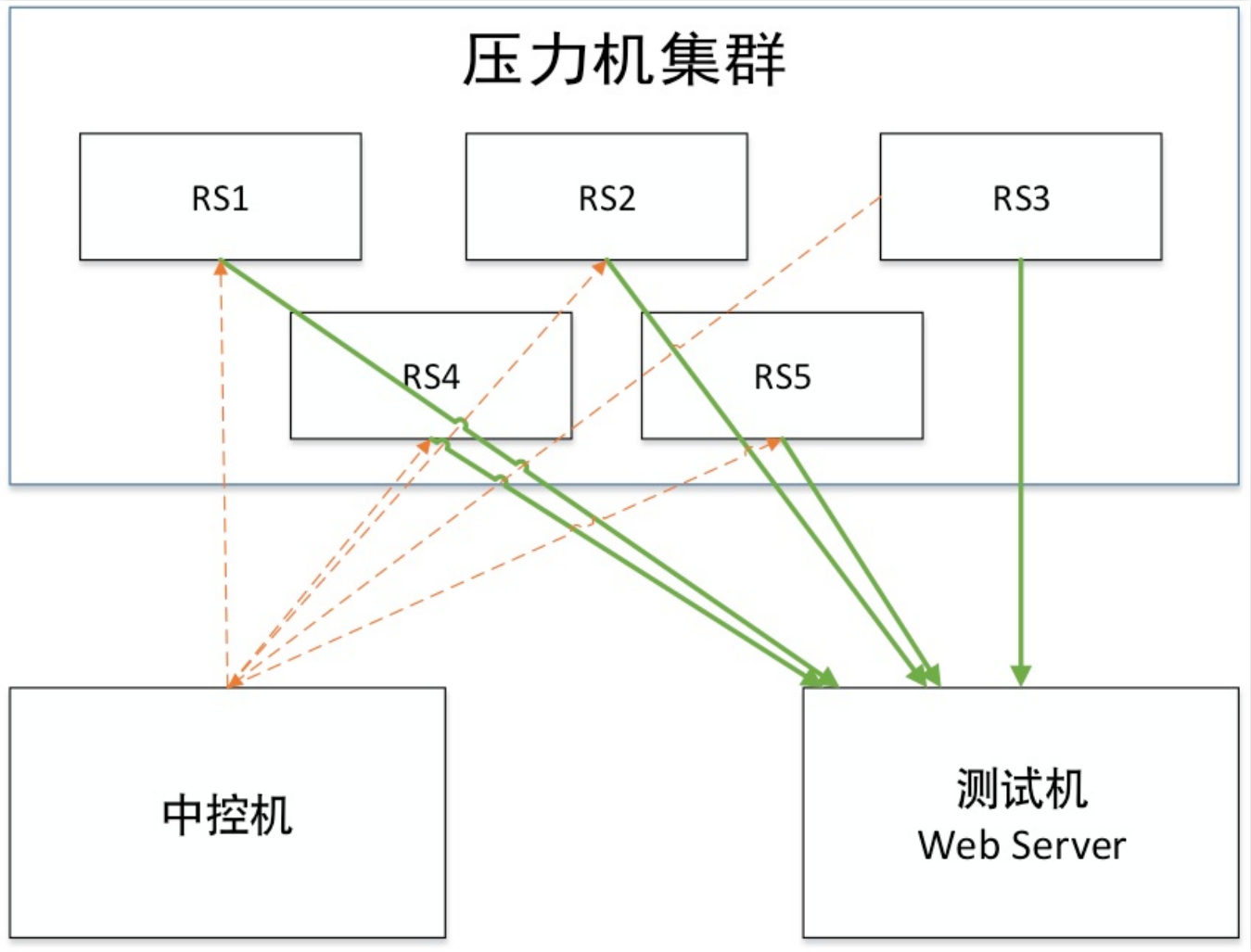
- 压力工具：wrk 4.0.2
- TCloudFinanceZone底层服务环境：Nginx 1.1.6_1.9.9 + Openssl 1.0.2h
- 安装Nginx机器操作系统信息：Linux TENCENT64.site 3.10.94-1-tlinux2-0036.tl2 #1 SMP Thu Jan 21 03:40:59 CST 2016 x86_64 x86_64 x86_64 GNU/Linux
- 其他压力机器操作系统：Linux TENCENT64.site 2.6.32.43-tlinux-1.0.17-default #1 SMP Tue Nov 17 18:03:12 CST 2015 x86_64 x86_64 x86_64 GNU/Linux

WebServer 集群测试方案

由于单台压力机无法发送足够大的压力测试TCloudFinanceZonehttps服务的极限性能，需要采用多台压力机来发送压力，整个测试包含三部分：

1. 压力机集群。用来发送 http/https 压力，并输出单台机器的压力测试结果 。
2. 中控机，同步控制压力机集群的启动和结束，获取各台机器的压力数据并汇总输出。

3. 测试机，即承载TCloudFinanceZone HTTPS 服务的云机器，测试 WebServer 性能，直接返回页面，不需要连接 upstream。
   连接关系如下表示：



HTTPS WebServer 测试性能数据

连接类型	Session cache	包体(bytes)	加密套件	性能(qps)
长	打开	230	ECDHE-RSA-AES128-GCM-SHA256	296241
短	关闭	230	ECDHE-RSA-AES128-GCM-SHA256	65630

CLB HTTPS 能力测试结论

由上表可知，TCloudFinanceZone HTTPS 支持 SSL 加解密，其后端拥有多个服务器集群，单集群的单台云服务器完全握手性能可达到65000 qps，长连接时性能可以达到约300000qps。

普通情况下，HTTPS 协议由于使用 SSL 协议，增加了至少一次完整握手的过程，因此增加延时为2 × RTT。此外，SSL 对称/非对称加密将消耗大量 CPU 资源，RSA 的解密能力是困扰 HTTPS 接入的主要难题。

使用TCloudFinanceZone负载均衡的 HTTPS 服务，用户无需为SSL加解密单独部署服务，且TCloudFinanceZone不收取任何额外费用，让用户轻松拥有极强的业务承载能力和防攻击能力。

压力测试常见问题

压力测试常见问题

后端主机未开启公网流量

购买云服务器时，如果不开启公网流量，则该主机挂载公网负载均衡时会导致转发不通的情况。

后端主机带宽设置不够

如果后端主机设置带宽过低，则带宽超过设定阈值后，后端服务器不会回包给 CLB，这样 CLB 处理时会返回504、502给客户端。

客户端端口不足

客户端个数过少，或客户端的端口范围设置过小时，客户端端口不足，会导致建立连接失败。此外，长连接建立时如果 keep_alive 字段大于0，此时连接会一直占用端口，导致客户端端口不足。

后端服务器依赖的应用成为性能瓶颈

请求经过负载均衡达到后端服务器后，后端服务器本身负载正常，但由于所有的后端服务器上的应用又依赖数据库等其他应用，此时如数据库出现性能瓶颈，也会影响压测性能。

后端服务器的健康状态异常

压测时容易忽略后端服务器的健康状态，如果有后端服务器健康检查失败或者健康检查状态反复（时好时坏，反复变化）时，也会导致压测性能低的现象。

负载均衡开启会话保持，后端主机流量分配不均

负载均衡开启会话保持后，容易造成请求落在固定的几台后端服务器上，导致流量分配不均衡，压测性能受到影响。建议压测时关闭会话保持。

压测建议

> 说明：以下设置仅用于压测负载均衡能力，并不表示用户生产环境也需要如此设置。

- 压测负载均衡转发能力时，建议使用短连接。
  一般除了验证会话保持等功能外，压测主要是希望验证负载均衡的转发能力，因此可以使用短连接来测试 CLB 和后端服务器的处理能力。
- 压测负载均衡吞吐量时建议使用长连接，用来测试带宽上限、或长连接业务等。
  此时建议将压测工具的超时时间调整为较小的阈值，超时时间过长时，会导致平均响应时间加长，从而不利于快速判断是否到达压测水位。

- 建议后端服务器提供一个静态网页用于压测，避免应用本身逻辑带来的损耗，如 I/O、DB 等。
- 监听不开启会话保持功能，否则压力会集中在个别的后端服务器，此外，压力性能不达标时，可以通过查看负载均衡下后端主机的监控数据判断是否流量分配均匀。
- 监听关闭健康检查功能，减少健康检查请求对后端服务器的访问请求。
- 使用多个 client(>5) 进行压测，源 IP 分散，能够更好的模拟线上实际情况。

最佳实践
负载均衡开启Gzip配置及检测方法说明

在公网负载均衡实例中，HTTP/HTTPS 协议默认支持用户开启 gzip 压缩功能。开启 gzip 功能对网页进行压缩，可以有效降低网络传输的数据量，提升客户端浏览器的访问速度。在使用过程中，需要注意如下事项：

注意事项

- 需要后端 CVM 同步开启 GZIP 支持
  对于常见的 Nginx 服务容器，必须在其配置文件（默认为 nginx.conf）中，开启 GZIP 并重启服务

  ```
  gzip on;
  ```

- 当前负载均衡支持的文件类型如下，您可以在 gzip_types 配置项中指定文件类型进行压缩

  ```
  application/atom+xml application/javascript application/json application/rss+xml application/vnd.ms-fontobject application/x-font-ttf application/x-web-app-manifest+json application/xhtml+xml application/xml font/opentype image/svg+xml image/x-icon text/css text/plain text/x-component;
  ```

> 说明：
>
> 负载均衡后端 CVM 业务软件中必须同步开启对上述文件类型的 GZIP 支持。

- 客户端请求中必须带有压缩请求标记
  需要启用压缩，还要求客户端请求时必须携带如下标记：

  ```
  Accept-Encoding: gzip,deflate,sdch
  ```

后端 CVM 开启 GZIP 流程支持示例

示例云服务器运行环境：Debian 6

1. 使用 vim 依据用户路径打开 Nginx 配置文件：

   ```
   vim /etc/nginx/nginx.conf
   ```

2. 找到如下代码：

```
gzip on;
gzip_min_length 1k;
gzip_buffers 4 16k;
gzip_http_version 1.1;
gzip_comp_level 2;
gzip_types text/html application/json;
```

上述代码的语法详解：

- gzip：开启或关闭 gzip 模块。
  语法： gzip on/off
  作用域：http，server，location
- gzip_min_length：设置允许压缩的页面最小字节数，页面字节数从 header 头中的 Content-Length 中进行获取。默认值是1k。
  语法： gzip_min_length length
  作用域：http，server，location
- gzip_buffers：设置系统获取几个单位的缓存用于存储 gzip 的压缩结果数据流。16k代表以16k为单位，按照原始数据大小以16k为单位的4倍申请内存。
  语法： gzip_buffers number size
  作用域：http，server，location
- gzip_http_version ：代表可以使用 gzip 功能的 HTTP 最低版本，设置 HTTP/1.0 代表了需要使用 gzip 功能的 HTTP 最低版本，因此可以向上兼容 HTTP/1.1。由于TCloudFinanceZone现已全网支持 HTTP/1.1，因此无需进行更改。
  语法: gzip_http_version 1.0 | 1.1;
  作用域: http，server，location
- gzip_comp_level：gzip 压缩比，范围为1 - 9。1压缩比最小处理速度最快，9压缩比最大但处理最慢（传输快但比较消耗 cpu）。
  语法: gzip_comp_level 1..9
  作用域: http，server，location
- gzip_types：匹配 MIME 类型进行压缩，默认"text/html" 类型是会被压缩的。 此外，Nginx 下的 gzip 默认不压缩 javascript、图片等静态资源文件，可以通过gzip_types 指定需要压缩的 MIME 类型，非设置值则不进行压缩。 例如，如果需要对 json 格式数据进行压缩，则需要在此语句中添加 application/json 类型数据
  支持的类型如下：

```
text/html text/plain text/css application/x-javascript text/javascript application/xml
```

语法： gzip_types mime-type [mime-type ...]
作用域: http, server, location

如对配置有修改，则首先将文件保存退出，进入到 Nginx bin 文件目录，执行如下命令重新加载 Nginx：

```
./nginx -s reload
```

使用 curl 命令测试 gzip 是否成功开启：

```
curl -I -H "Accept-Encoding: gzip, deflate" "http://finance.cloud.tencent.com/example/"
```

HTTPS转发配置入门指南

负载均衡能力说明

CLB 负载均衡器通过对协议栈及服务端的深度优化，实现了 HTTPS 性能的巨大提升。同时，我们也通过证书的国际合作，极大降低了证书的成本。CLB 在如下几个方面能够为业务带来非常显著的收益：

1. 使用 HTTPS 并不会降低 Client 端的访问速度。
2. 集群内单台服务器 SSL 加解密性能，高达 6.5W cps 的完全握手。相比高性能 CPU 提升了至少3.5倍，节省了服务端成本，极大提升了业务运营及流量突涨时的服务能力，增强了计算型的防攻击能力。
3. 支持多种协议卸载及转换。减少业务适配客户端各种协议的压力，业务后端只需要支持 HTTP1.1 就能使用 HTTP2、SPDY、SSL3.0 及 TLS1.2等各版本协议。
4. 一站式 SSL 证书申请、监控、替换。我们和国际证书厂商 comodo，symantec 展开对话，探讨合作，大幅缩减证书申请流程及成本。
5. 防 CC 及 WAF 功能。能够有效杜绝慢连接、高频定点攻击、SQL 注入、网页挂马等应用层攻击。

HTTP、HTTPS 头部标识

CLB 对 HTTPS 进行代理，无论是 HTTP 还是 HTTPS 请求，到了 CLB 转发给后端 CVM 时，都是 HTTP 请求。这时开发者无法分辨前端的请求是 HTTP 还是 HTTPS。

CLB 在将请求转发给后端 CVM 时，头部 header 会植入 X-Client-Proto：

X-Client-Proto: http（前端为 HTTP 请求）
X-Client-Proto: https（前端为 HTTPS 请求）

入门配置

假定用户需要配置网站 https://example.com 。开发者希望用户在浏览器中输入网址时，直接键入 www.example.com 即可通过 HTTPS 协议安全访问。

此时用户输入的 www.example.com 请求转发流程如下：

1. 该请求以 HTTP 协议传输，通过 VIP 访问负载均衡监听器的80端口，并被转发到后端云服务器的8080端口。
2. 通过在后端服务器的 Nginx 上配置 rewrite 操作，该请求经过8080端口，并被重写到 https://example.com 页面。
3. 此时浏览器再次发送 https://example.com 请求到相应的 HTTPS 站点，该请求通过 VIP 访问负载均衡监听器的443端口，并被转发到后端云服务器的80端口。
   至此，请求转发完成。

该操作在浏览器用户未感知的情况下，将用户的 HTTP 请求重写为更加安全的 HTTPS 请求。为实现以上请求转发操作，用户可以对后端服务器做如下配置：

```
server {

    listen 8080;
    server_name www.example.com;

    location / {

        #! customized_conf_begin;
        client_max_body_size 200m;
        rewrite ^/.(.*) https://$host/$1 redirect;

}
}
```

或者在 Nginx 新版本中，采用推荐的301重定向配置方法，将 Nginx HTTP 页面重定向到 HTTPS 页面：

```
server {
     listen      80;
     server_name    www.example.com;
     return      301 https://$server_name$request_uri;
}

server {
     listen      443 ssl;
    server_name    www.example.com;
    [....]
}
```

如何获取客户端真实IP

CLB 的四层（TCP/UDP）和七层（HTTP/HTTPS）服务均支持直接在后端 CVM 上获取客户端真实 IP，无需进行额外配置。

- 四层负载均衡，在后端 CVM 上获取的源 IP 即为客户端 IP。
- 七层负载均衡，您可以通过 X-Forwarded-For 或 remote_addr 字段来直接获取客户端 IP。

> 说明：
> 对于 CLB 来说，无需在后端 CVM 上做额外配置即可获取客户端 IP。
> 对于其他做了 SNAT 的七层负载均衡服务，您需要在后端 CVM 上配置，然后使用 X-Forwarded-For 的方式获取客户端的真实 IP。

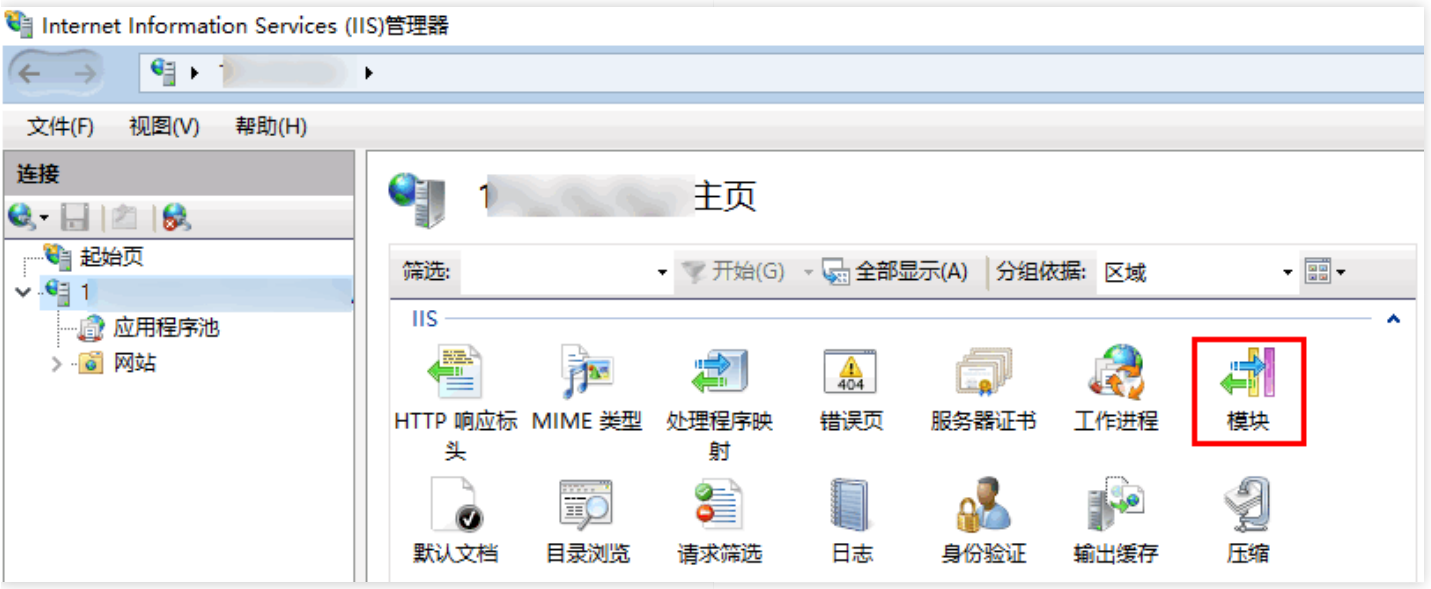
下文将对常见的应用服务器配置方案进行介绍。

IIS 6 配置方案

1. 下载与安装插件 F5XForwardedFor 模块，根据自己的服务器操作系统版本将 x86\Release 或者 x64\Release 目录下的 F5XForwardedFor.dll 拷贝到某个目录，这里假设为 C:\ISAPIFilters ，同时确保对 IIS 进程对该目录有读取权限。
2. 打开 IIS 管理器，找到当前开启的网站，在该网站上右键选择【属性】，打开属性页。
3. 在属性页切换至【ISAPI 筛选器】，单击【添加】，弹出添加窗口。
4. 在添加窗口“筛选器名称”中填写“F5XForwardedFor”，“可执行文件”填写 F5XForwardedFor.dll 的完整路径，单击【确定】。
5. 重启 IIS 服务器，等待配置生效。

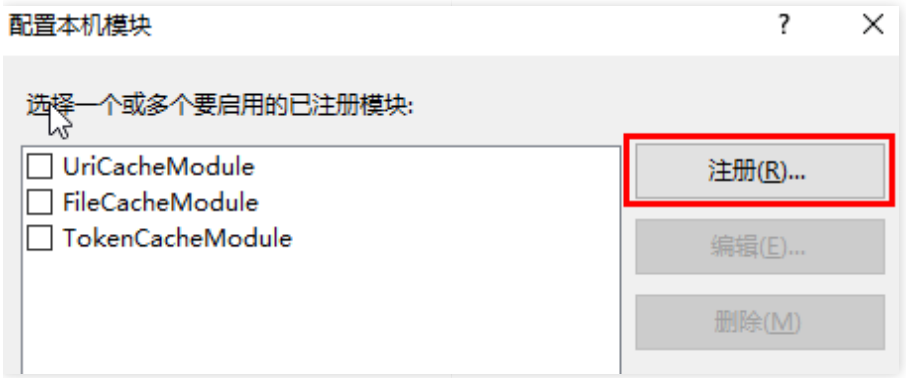
IIS 7 配置方案

1. 下载与安装插件 F5XForwardedFor 模块，根据自己的服务器操作系统版本将 x86\Release 或者 x64\Release 目录下的 F5XFFHttpModule.dll 和 F5XFFHttpModule.ini 拷贝到某个目录，这里假设为 C:\F5XForwardedFor ，确保对 IIS 进程对该目录有读取权限。
2. 选择【IIS服务器】，双击【模块】功能。

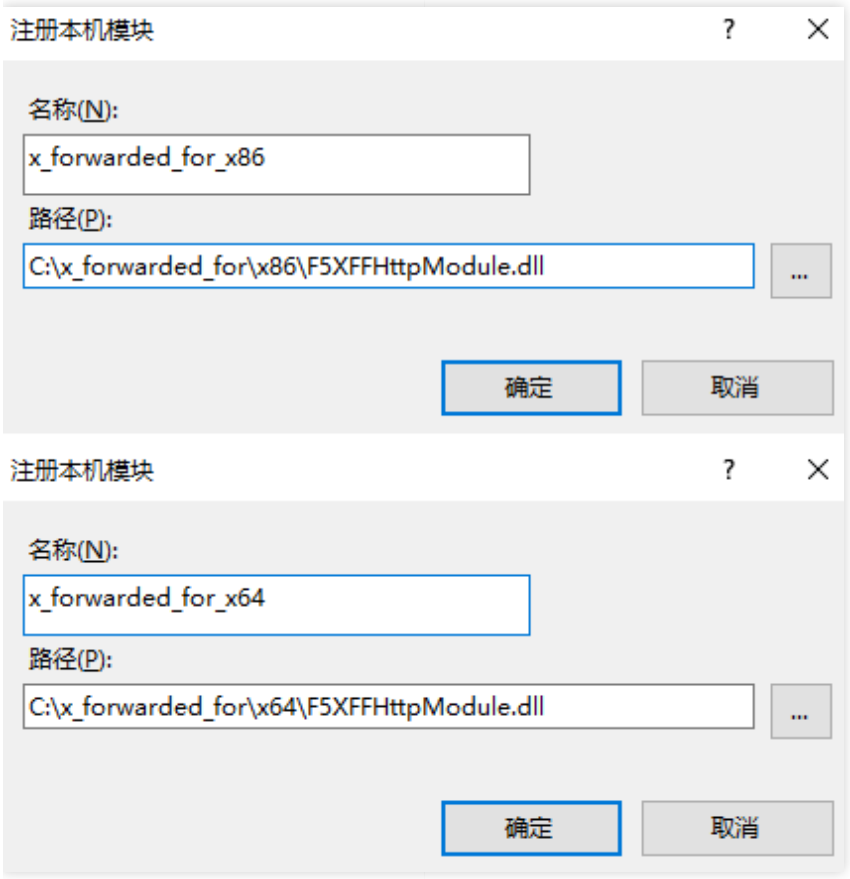


3. 单击【配置本机模块】。

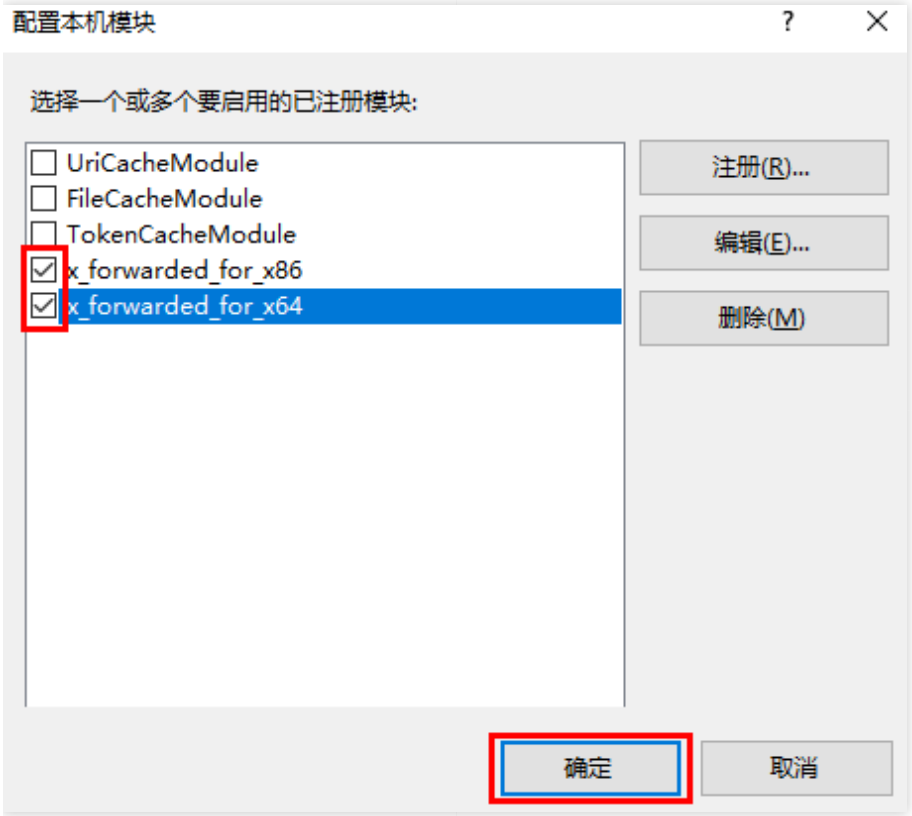
4. 在弹出框中单击【注册】。



5. 添加下载的 DLL 文件，如下图所示：



6. 添加完成后，勾选并单击【确定】。



7. 在 “ISAPI 和 CGI 限制”添加如上两个 DLL ，并将限制设置为允许。

8. 重启 IIS 服务器，等待配置生效。

Apache 配置方案

1. 安装 Apache 第三方模块“mod_rpaf” 。

```
wget http://stderr.net/apache/rpaf/download/mod_rpaf-0.6.tar.gz
tar zxvf mod_rpaf-0.6.tar.gz
cd mod_rpaf-0.6
/usr/bin/apxs -i -c -n mod_rpaf-2.0.so mod_rpaf-2.0.c
```

2. 修改 Apache 配置 /etc/httpd/conf/httpd.conf ，在最末尾添加：

```
LoadModule rpaf_module modules/mod_rpaf-2.0.so
RPAFenable On
RPAFsethostname On
RPAFproxy_ips IP地址（这个IP地址首先不是负载均衡提供的公网IP，具体IP多少可以查看Apache日志，通常会有2个 都要写上）
RPAFheader X-Forwarded-For
```

3. 添加完成后，重启 Apache。

```
/usr/sbin/apachectl restart
```

Nginx 配置方案

1. Nginx 作为服务器时，获取客户端真实 IP 使用 http_realip_module，默认安装的 Nginx 是没有安装这个模块

的，需要重新编译 Nginx 增加 --with-http_realip_module。

```
wget  http://nginx.org/download/nginx-1.14.0.tar.gz
tar  zxvf nginx-1.14.0.tar.gz
cd nginx-1.14.0
./configure --user=www --group=www --with-http_stub_status_module --without-http-cache --with-http_ssl_module --with-http_realip_module
make
make install
```

2. 修改 nginx.conf。

```
vi /etc/nginx/nginx.conf
```

修改如下部分：

```
fastcgi connect_timeout 300;
fastcgi send_timeout 300;
fastcgi read_timeout 300;
fastcgi buffer_size 64k;
fastcgi buffers 4 64k;
fastcgi busy_buffers_size 128k;
fastcgi temp_file_write_size 128k;

set_real_ip_from IP地址;（这个IP地址首先不是负载均衡提供的公网IP，具体IP多少可以查看之前nginx日志，如
real_ip_header X-Forwarded-For;
```

3. 重启 Nginx。

```
service nginx restart
```

多可用区高可用配置说明

负载均衡器多可用区高可用

CLB 负载均衡器支持 IPv4 内外网和 EIP 的多可用区容灾的能力，如在SZ一区、二区金融两个可用区（同一个地域），会分别部署多套集群，以实现同 Region 下的跨可用区容灾。通过该特性可实现当整个可用区故障时，负载均衡10s内，将前端访问流量切换到同一地域下的其它可用区，以恢复服务能力。

具体场景与疑问解答

疑问1：SZ金融区 A、B，有负载均衡器 test1，Client 端公网入流量的策略是？

在SZ一区、二区机房，有一对 IP 资源池，可理解为对等的 IP 资源。开发者无需理解，一区，二区哪个是主集群，哪个是备集群，两个集群拥有同等的负载能力。当开发者购买负载均衡器，并绑定 CVM 时，会生成两套规则写入两套集群，此时就已经获得了高可用能力。

疑问2：SZ金融区 A、B，有负载均衡器 test1，后端在 A、B 可用区各绑定了100台服务器。业务运行中，各建立100万 HTTP 长连接（TCP 连接不关闭）。此时当金融区A的负载均衡器集群整体瘫痪，不可用时，业务的感受是？

当金融区 A 的负载均衡器失去服务能力后，当前的所有长连接会断开，短连接不受影响。容灾架构会在10s内，将 A/B 区的各100台服务器，会立刻自动绑定到金融区 B 的负载均衡器上，业务能力立即恢复，无需人工介入。

疑问3：多可用区容灾的能力，支持哪种类型的负载均衡器？

IPv4 内外网 CLB 和 EIP 支持跨AZ容灾，目前 IPv6 CLB 和 NAT64 暂不支持。

SSL证书格式要求及格式转换说明

证书格式说明

证书格式要求

- 用户要申请的证书为：Linux 环境下 PEM 格式的证书。负载均衡不支持其他格式的证书，如其它格式的证书请参见下文“证书转换为 PEM 格式说明”的内容。
- 如果是通过 root CA 机构颁发的证书，您拿到的证书为唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。
- 如果是通过中级 CA 机构颁发的证书，您拿到的证书文件包含多份证书，需要人为的将服务器证书与中间证书合并在一起上传。
- 当您的证书有证书链时，请将证书链内容，转化为 PEM 格式内容，与证书内容合并上传。
- 拼接规则为：服务器证书放第一份，中间证书放第二份，中间不要有空行。 > 说明：一般情况下，机构在颁发证书的时候会有对应说明，请注意查阅。

证书格式和证书链格式范例

如下为证书格式和证书链格式范例，请确认格式正确后上传：

1. root CA 机构颁发的证书：证书格式为 Linux 环境下 PEM 格式。样例如下：

证书规则为：

- [———-BEGIN CERTIFICATE———-, ———-END CERTIFICATE———-] 开头和结尾；请将这些内容一并上传。
- 每行64字符，最后一行不超过64字符。

2. 中级机构颁发的证书链：

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

———-BEGIN CERTIFICATE———-

———-END CERTIFICATE———-

证书链规则为：

- 证书之间不能有空行。
- 每一份证书遵循上文 “1.1 证书格式要求”。

2. RSA 私钥格式要求

样例如下：

RSA 私钥可以包括所有私钥（RSA 和 DSA）、公钥（RSA 和 DSA）和 (x509) 证书。它存储用 Base64 编码的 DER 格式数据，用 ASCII 报头包围，因此适合系统之间的文本模式传输。

RSA 私钥规则：

- [——-BEGIN RSA PRIVATE KEY——-, ——-END RSA PRIVATE KEY——-] 开头结尾，请将这些内容一并上传。
- 每行64字符，最后一行长度可以不足64字符。
  如果您不是按照上述方案生成 [——-BEGIN PRIVATE KEY——-, ——-END PRIVATE KEY——-] 这种格式的可用私钥，您可以按照如下方式转换成可用私钥：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

然后将 new_server_key.pem 的内容与证书一起上传。

证书转换为 PEM 格式说明

目前负载均衡仅支持 PEM 格式的证书，其他格式的证书需要转换成 PEM 格式后才能上传到负载均衡中，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为 PEM 格式的方法。

DER 格式证书转换为 PEM 格式

DER 格式一般出现在 Java 平台中。

证书转换： openssl x509 -inform der -in certificate.cer -out certificate.pem

私钥转换： openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem

P7B 格式证书转换为 PEM 格式

P7B 格式一般出现在 Windows Server 和 tomcat 中。

证书转换： openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer

获取 outcertificat.cer 里面 [——-BEGIN CERTIFICATE——-， ——-END CERTIFICATE——-] 的内容作为证书上传。

私钥转换：私钥一般在 IIS 服务器里可导出。

PFX 格式证书转换为 PEM 格式

PFX 格式一般出现在 Windows Server 中。

证书转换： openssl pkcs12 -in certname.pfx -nokeys -out cert.pem

私钥转换： openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes

CER/CRT 格式证书转换为 PEM 格式

对于 CER/CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将 “servertest.crt” 证书文件

直接重命名为“servertest.pem”即可。

均衡算法选择与权重配置实例

负载均衡算法比较分析

加权轮询算法 Weighted Round-Robin Scheduling

- 原理
  轮叫调度算法就是以轮叫的方式依次将请求调度不同的服务器，即每次调度执行i = (i + 1) mod n，选出第i台服务器。加权轮叫调度算法可以解决服务器间性能不一的情况，它用相应的权值表示服务器的处理性能，按权值的高低和轮叫方式分配请求到各服务器。权值高的服务器先收到的连接，权值高的服务器比权值低的服务器处理更多的连接，相同权值的服务器处理相同数目的连接数。
- 优势
  算法的优点是其简洁性，和实用性。它无需记录当前所有连接的状态，所以它是一种无状态调度。
- 劣势
  加权轮叫调度算法相对简单，但不适用于请求服务时间变化比较大，或者每个请求所消耗的时间不一致的情况，此时轮叫调度算法容易导致服务器间的负载不平衡。
- 适用场景
  每个请求所占用的后端时间基本相同，负载情况最好。常用于短连接服务，例如 HTTP 等服务。
- 用户推荐
  用户可知每个请求所占用后端时间基本相同时，如已知rs处理的都是同类型或者相似类型的请求时，推荐选择加权轮询的方式。当请求时间相差较小时也推荐使用加权轮询的方式，因为该实现方式消耗小，无需遍历，效率较高。

加权最小连接数 Weighted Least-Connection Scheduling

- 原理
- 在实际情况中，客户端的每一次请求服务在服务器停留的时间可能会有较大的差异，随着工作时间的延伸，如果采用简单的轮询或随机均衡算法，每一台服务器上的连接进程数目可能会产生极大的不同，这样实际上并没有达到真正的负载均衡。最小连接调度是一种动态调度算法，它通过服务器当前所活跃的连接数来估计服务器的负载情况。与轮询调度算法相反，调度器需要记录各个服务器已建立连接的数目，当一个请求被调度到某台服务器，其连接数加1；当连接中止或超时，其连接数减一。权重最少连接数调度算法是在做少连接数调度算法的基础上，根据服务器的不同处理能力，给每个服务器分配不同的权值，使其能够接受相应权值数的服务请求，是在最少连接数调度算法的基础上的改进。

1. 假设各台 rs 的权值依次为 wi,当前连接数依次为 ci，依次计算 ci/wi，值最小的 rs 作为下一个分配的 rs。
2. 如果存在 ci/wi 相同的 rs，这些 rs 再使用加权轮询的方式调度

- 优势
  此种均衡算法适合长时处理的请求服务，如FTP等应用。

- 劣势
  由于接口限制，目前最小连接数和会话保持功能不能同时开启。
- 适用场景
  每个请求所占用的后端时间相差较大的场景。常用于长连接服务。
- 用户推荐
  如果用户需要处理不同的请求，且请求所占用后端时间相差较大，如3ms和3s这种数量级的差距时，推荐使用加权最小连接数算法实现负载均衡。

源地址散列调度算法 ip_hash

- 原理
  根据请求的源IP地址，作为散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器是可用的且未超载，将请求发送到该服务器，否则返回空。
- 优势
  ip_hash 可以实现部分会话保持的效果，能够记住源 IP，使某一 client 请求通过 hash 表一直映射在同一台 rs 上。因此在不支持会话保持的场景可以使用 ip_hash 进行调度。
- 用户推荐
  将请求的源地址进行hash运算，并结合后端的服务器的权重派发请求至某匹配的服务器，这可以使得同一个客户端 IP的请求始终被派发至某特定的服务器。该方式适合负载均衡无 cookie 功能的 TCP 协议。

均衡算法选取及权重配置实例

在负载均衡即将发布的新功能中，七层转发将支持最小连接数的均衡方式，为了让用户在不同场景下，能够让 RS 集群稳定的承接业务，因此我们给出几个负载均衡选择与权重配置的实例供用户进行参考。

- 场景1
  设有3台配置相同（CPU / 内存）的 RS，由于性能一致，用户可以将RS权重都设置为10。设现在每台 RS 与 client 端建立了100个 TCP 链接，此时新增1台 RS。在此场景下，推荐用户使用最小连接数的均衡方式，这种配置能快速的让第四台 RS 的负载提升，降低另外3台 RS 的压力。
- 场景2
  设用户首次接触云服务，且建站时间不长，网站负载较低，则建议购买相同配置的 RS，因此 RS 都是无差别的接入层服务器。在此场景下，用户可以将 RS 权重都设为10，采用加权轮询的均衡方式进行流量分发。
- 场景3
  用户有5台服务器，用与承载简单的静态网站访问，且5台服务器的计算能力的比例为 9：3：3：3：1（按 CPU、内存换算）。在此场景下，用户可以依次将 RS 权重比例设置为90，30，30，30，10，由于静态网站访问大多数是短连接请求，因此可以采用加权轮询的均衡方式，让 CLB 按 RS 的性能比例分配请求。
- 场景4
  某用户有10台 RS 用于承担海量的 Web 访问请求，且不希望多购置 RS 增加支出。 某台 RS 经常会因为负载过高，导致服务器重启。在此场景下，建议用户根据 RS 的性能进行相应的权重设置，给负载过高的 RS 设置较

小的权值。除此之外，可以采用最小连接数的负载均衡方式，将请求分配到活跃连接数较少的 RS 上，从而解决某台 RS 负载过高的问题。

- 场景5

  某用户有3台 RS 用于处理若干长连接请求，且这3太服务器的计算能力比例为3：1：1（按 CPU、内存换算）。 此时性能最好的服务器处理请求较多，用户不希望过载此服务器，希望能够将新的请求分配到空闲服务器上。在此场景下，可以采用最小连接数的均衡方式，并适当降低繁忙服务器的权重，便于 CLB 将请求分配到活跃数较少的 RS 上，实现负载均衡。

- 场景6

  某用户希望后续客户端的请求可以分配到同一服务器上。而采用加权轮询或加权最小连接数的方式，不能保证相同客户端的请求被分到固定某台服务器上去。为了配合客户特定应用程序服务器的需求，保证客户端的会话具有“粘性”或是“持续性”，在此场景下，我们可以采用 ip_hash 的均衡方式进行流量分发。此方法可以确保来自同一客户端的请求总被定向分发到同一 RS 上去。（服务器数量变化或是该服务器不可用时除外）

API文档
负载均衡（clb）
版本（2018-03-17）
API 概览

API版本

V3

其他接口

接口名称	接口功能
DescribeLoadBalancerListByCertId	根据证书ID查询负载均衡
SetLoadBalancerSecurityGroups	设置负载均衡实例的安全组
SetSecurityGroupForLoadbalancers	绑定或解绑一个安全组到多个负载均衡实例

负载均衡相关接口

接口名称	接口功能
AutoRewrite	自动生成负载均衡转发规则的重定向关系
BatchDeregisterTargets	批量解绑四七层后端服务
BatchModifyTargetWeight	批量修改监听器绑定的后端机器的转发权重
BatchRegisterTargets	批量绑定虚拟主机或弹性网卡
CreateListener	创建负载均衡监听器
CreateLoadBalancer	购买负载均衡实例
CreateRule	创建负载均衡七层监听器转发规则
DeleteCert	删除证书

接口名称	接口功能
DeleteListener	删除负载均衡监听器
DeleteLoadBalancer	删除负载均衡实例
DeleteRewrite	删除负载均衡转发规则之间的重定向关系
DeleteRule	删除负载均衡七层监听器的转发规则
DeregisterTargets	从负载均衡监听器上解绑后端服务
DescribeAppIdLabel	查询用户和绑定的集群标签
DescribeCerts	查询证书列表
DescribeCustomizedConfigAssociateList	拉取配置绑定的server或location。
DescribeCustomizedConfigList	拉取配置列表
DescribeIspInfo	查询运营商信息
DescribeListenerListByCertId	根据证书id获取绑定的监听器
DescribeListeners	查询负载均衡的监听器列表
DescribeLoadBalancers	查询负载均衡实例列表
DescribeRewrite	查询负载均衡转发规则的重定向关系
DescribeSubUinQuotas	查询子账号配额
DescribeTargetHealth	获取负载均衡后端服务的健康检查状态
DescribeTargets	查询负载均衡绑定的后端服务列表
DescribeTaskStatus	查询异步任务状态
InquiryPriceModifyLoadBalancer	修改负载均衡配置询价
ManualRewrite	手动添加负载均衡转发规则的重定向关系
ModifyCertAlias	修改证书备注
ModifyDomainAttributes	修改负载均衡七层监听器转发规则的域名级别属性
ModifyListener	修改负载均衡监听器属性
ModifyLoadBalancerAttributes	修改负载均衡实例的属性
ModifyRule	修改负载均衡七层监听器的转发规则

接口名称	接口功能
ModifyTargetPort	修改监听器绑定的后端机器的端口
ModifyTargetWeight	修改监听器绑定的后端机器的转发权重
RegisterTargets	绑定后端机器到监听器上
ReplaceCert	替换证书
SetCustomizedConfigForLoadBalancer	负载均衡维度的个性化配置相关操作
SetSubUinQuotas	设置子账号配额
UpLoadCert	上传证书

调用方式
接口签名v1

TCloudFinanceZone 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TCloudFinanceZone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，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐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。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

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

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	shjr
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

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' : 'shjr',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    '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=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&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.finance.cloud.tencent.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.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&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 = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

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 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%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 http 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
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TCloudFinanceZone 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。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java

- PHP
- Go
- Node

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.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%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，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，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 CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.finance.cloud.tencent.com/?");
```

```
        // 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.finance.cloud.tencent.com/?");
        // 实际请求的url中对参数顺序没有要求
        for (String k : params.keySet()) {
            // 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
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
        // 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Intege
r.MAX_VALUE));
        params.put("Nonce", 11886); // 公共参数
        // 实际调用时应当使用系统当前时间，例如：  params.put("Timestamp", System.currentTimeMillis() /
1000);
        params.put("Timestamp", 1465185768); // 公共参数
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
        params.put("Action", "DescribeInstances"); // 公共参数
        params.put("Version", "2017-03-12"); // 公共参数
        params.put("Region", "shjr"); // 公共参数
        params.put("Limit", 20); // 业务参数
        params.put("Offset", 0); // 业务参数
        params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // 公共参数
        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 time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

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.finance.cloud.tencent.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'shjr',
        '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)
```

接口签名v3

TCloudFinanceZone 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TCloudFinanceZone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，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：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 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，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。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
    HTTPRequestMethod + '\n' +
    CanonicalURI + '\n' +
    CanonicalQueryString + '\n' +
    CanonicalHeaders + '\n' +
    SignedHeaders + '\n' +
    HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；
- 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 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。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 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为： content-type:application/x-www-form-urlencoded\nhost:cvm.finance.cloud.tencent.com\n
- 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。content-type 和 host 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）按照字典排序进行拼接，并且以分号（;）分隔。此例中为： content-type;host
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.finance.cloud.tencent.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 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
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。Date 为 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 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

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，可能导致运行一段时间后，请求必定失败（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（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.finance.cloud.tencent.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.finance.cloud.tencent.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: shjr
```

3. 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
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）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.finance.cloud.tencent.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
```

```
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.finance.cloud.tencent.com";
        String region = "shjr";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // 注意时区，否则容易出错
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* 步骤 1：拼接规范请求串 *************
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* 步骤 2：拼接待签名字符串 *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* 步骤 3：计算签名 *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
```

```
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* 步骤 4：拼接 Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

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

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.finance.cloud.tencent.com"
endpoint = "https://" + host
region = "shjr"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
```

```
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
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)

# 公共参数添加到请求头部
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
```

```
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

请求结构

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

2. 通信协议

TCloudFinanceZone 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 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

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，可以联系我们，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 cor
rect."
        },
        "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，可以联系我们，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，下表列出了公共错误码。

错误码	错误描述
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。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
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。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。

错误码	错误描述
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
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。

公共参数

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口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。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	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。
X-TC-Timestamp	Integer	是	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。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 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=AKIDEXAMPLE/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，AKIDEXAMPLE 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为产品名，必须与调用的产品域名一致，例如cvm； - 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。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

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	是	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。

参数名称	类型	必选	描述
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。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 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	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

其他接口
根据证书ID查询负载均衡

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

根据证书ID查询其在一个地域中所关联到负载均衡实例列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:20:28。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLoadBalancerListByCertId
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
CertIds	是	否	Array of String	服务端证书的ID，或客户端证书的ID 示例值： ["RwFAfr8Y"]

3. 输出参数

参数名称	类型	描述
CertSet	Array of CertIdRelatedWithLoadBalancers	证书ID，以及与该证书ID关联的负载均衡实例列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

设置负载均衡实例的安全组

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

SetLoadBalancerSecurityGroups 接口支持对一个公网负载均衡实例执行设置（绑定、解绑）安全组操作。查询一个负载均衡实例目前已绑定的安全组，可使用 DescribeLoadBalancers 接口。本接口是set语义，
绑定操作时，入参需要传入负载均衡实例要绑定的所有安全组（已绑定的+新增绑定的）。
解绑操作时，入参需要传入负载均衡实例执行解绑后所绑定的所有安全组；如果要解绑所有安全组，可不传此参数，或传入空数组。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:30:50。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetLoadBalancerSecurityGroups
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxw2r00
SecurityGroups	否	否	Array of String	安全组ID构成的数组，一个负载均衡实例最多可绑定50个安全组，如果要解绑所有安全组，可不传此参数，或传入空数组。 示例值： ["sg-0936o7sd","sg-dfsv32sx"]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

绑定或解绑一个安全组到多个负载均衡实例

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

绑定或解绑一个安全组到多个公网负载均衡实例。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:30:27。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetSecurityGroupForLoadbalancers
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
SecurityGroup	是	否	String	安全组ID，如 sg-j9x73ko1 示例值： sg-j9x73ko1
OperationType	是	否	String	ADD 绑定安全组； DEL 解绑安全组 示例值： ADD
LoadBalancerIds	是	否	Array of String	负载均衡实例ID数组 示例值： ["lb-0936o712","lb-tttt5555"]

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

负载均衡相关接口
自动生成负载均衡转发规则的重定向关系

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

用户需要先创建出一个HTTPS:443监听器，并在其下创建转发规则。通过调用本接口，系统会自动创建出一个HTTP:80监听器（如果之前不存在），并在其下创建转发规则，与HTTPS:443监听器下的Domains（在入参中指定）对应。创建成功后可以通过HTTP:80地址自动跳转为HTTPS:443地址进行访问。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2024-02-18 17:59:55。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AutoRewrite
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-r6nx1iby
ListenerId	是	否	String	HTTPS:443监听器的ID 示例值： lbl-lmeeyb1q
Domains	否	否	Array of String	HTTPS:443监听器下需要重定向的域名 示例值： ["www.domain1.com"]
TakeUrls	否	否	Array of Bool	重定向是否携带匹配的URL 示例值： [true]

参数名称	必选	允许NULL	类型	描述
RewriteCodes	否	否	Array of Int64	重定向状态码，可取值301,302,307。 示例值： [301]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

批量解绑四七层后端服务

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

批量解绑四七层后端服务。批量解绑的资源数量上限为500。只支持VPC网络负载均衡。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-28 10:26:30。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：BatchDeregisterTargets
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡ID。 示例值： lb-j3ix99s2
Targets	是	否	Array of BatchTarget	解绑目标。 示例值：查看

3. 输出参数

参数名称	类型	描述
FailListenerIdSet	Array of String	解绑失败的监听器ID。 示例值： ["lbl-4ibsji93"]

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。
InvalidParameter.ProtocolCheckFailed	监听器协议检查失败，比如相关协议不支持对应操作。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
InvalidParameterValue.Duplicate	参数值有重复。
InvalidParameter.RegionNotFound	地域无效。
MissingParameter	缺少参数错误。
InvalidParameterValue.Range	参数取值范围错误。
InvalidParameterValue	参数取值错误

批量修改监听器绑定的后端机器的转发权重

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

本接口(BatchModifyTargetWeight)用于批量修改负载均衡监听器绑定的后端机器的转发权重，支持负载均衡的4层和7层监听器；不支持传统型负载均衡。
本接口为异步接口，本接口返回成功后需以返回的 RequestID 为入参，调用 DescribeTaskStatus 接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-27 20:46:14。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：BatchModifyTargetWeight
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-dx98lwo0
ModifyList	是	否	Array of RsWeightRule	要批量修改权重的列表，例如"ModifyList": [{"ListenerId": "lbl-di3kx902", "LocationId":"", "Domain": "", "Url": "", "Targets": [{"Type":"CVM", "InstanceId": "ins-xxxxxxx", "Port": "443", "Weight": 10, "EniIp":""}], "Weight": 10}] 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

批量绑定虚拟主机或弹性网卡

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

批量绑定虚拟主机或弹性网卡，支持跨域绑定，支持四层、七层（TCP、UDP、HTTP、HTTPS）协议绑定。批量绑定的资源数量上限为500。只支持VPC网络负载均衡。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-07-28 10:21:19。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：BatchRegisterTargets
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡ID。 示例值： lb-j3ix99s2
Targets	是	否	Array of BatchTarget	绑定目标。 示例值：查看

3. 输出参数

参数名称	类型	描述
FailListenerIdSet	Array of String	绑定失败的监听器ID，如为空表示全部绑定成功。 示例值： ["lbl-4ibsji93"]

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。
InvalidParameter.ProtocolCheckFailed	监听器协议检查失败，比如相关协议不支持对应操作。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
InvalidParameter.RegionNotFound	地域无效。
MissingParameter	缺少参数错误。

创建负载均衡监听器

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

在一个负载均衡实例下创建监听器。
本接口为异步接口，接口返回成功后，需以返回的 RequestId 为入参，调用 DescribeTaskStatus 接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-08-22 15:35:31。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateListener
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
Ports	是	否	Array of Int64	要将监听器创建到哪些端口，每个端口对应一个新的监听器 示例值： ["7569","7570"]
Protocol	是	否	String	监听器协议： TCP
ListenerNames	否	否	Array of String	要创建的监听器名称列表，名称与Ports数组按序一一对应，如不需立即命名，则无需提供此参数 示例值： ["lis0","lis1"]

参数名称	必选	允许NULL	类型	描述
HealthCheck	否	否	HealthCheck	健康检查相关参数，此参数仅适用于TCP/UDP/TCP_SSL监听器 示例值：查看
Certificate	否	否	CertificateInput	证书相关信息，此参数仅适用于TCP_SSL监听器和未开启SNI特性的HTTPS监听器。 示例值：查看
SessionExpireTime	否	否	Int64	会话保持时间，单位：秒。可选值：30~3600，默认 0，表示不开启。此参数仅适用于TCP/UDP监听器。 示例值： 60
Scheduler	否	否	String	监听器转发的方式。可选值：WRR、LEAST_CONN 分别表示按权重轮询、最小连接数， 默认为 WRR。此参数仅适用于TCP/UDP/TCP_SSL监听器。 示例值： WRR
SniSwitch	否	否	Int64	是否开启SNI特性，此参数仅适用于HTTPS监听器。0表示未开启，1表示开启。 示例值： 1
TargetType	否	否	String	后端目标类型，NODE表示绑定普通节点，TARGETGROUP表示绑定目标组。 示例值： NODE
DefaultSerSwitch	否	否	Bool	监听器是否支持设置默认域名，默认为true 示例值： true

3. 输出参数

参数名称	类型	描述
ListenerIds	Array of String	创建的监听器的唯一标识数组 示例值： ["lbl-d1ubsydq","lbl-4udz130k"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。

购买负载均衡实例

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

本接口(CreateLoadBalancer)用来创建负载均衡实例（本接口只支持购买按量计费的负载均衡，包年包月的负载均衡请通过控制台购买）。为了使用负载均衡服务，您必须购买一个或多个负载均衡实例。成功调用该接口后，会返回负载均衡实例的唯一 ID。负载均衡实例的类型分为：公网、内网。详情可参考产品说明中的产品类型。
注意：(1)指定可用区申请负载均衡、跨zone容灾；(2)一个账号在每个地域的默认购买配额为：公网100个，内网100个。
本接口为异步接口，接口成功返回后，可使用 DescribeLoadBalancers 接口查询负载均衡实例的状态（如创建中、正常），以确定是否创建成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2024-02-22 11:26:37。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateLoadBalancer
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerType	是	否	String	负载均衡实例的网络类型：OPEN：公网属性， INTERNAL：内网属性。 示例值： OPEN
Forward	否	否	Int64	负载均衡实例的类型。1：通用的负载均衡实例，目前只支持传入1 示例值： 1

参数名称	必选	允许NULL	类型	描述
LoadBalancerName	否	否	String	负载均衡实例的名称，只在创建一个实例的时候才会生效。规则：1-50 个英文、汉字、数字、连接线“-”或下划线“_”。 注意：如果名称与系统中已有负载均衡实例的名称相同，则系统将会自动生成此次创建的负载均衡实例的名称。 示例值： lb-1
VpcId	否	否	String	负载均衡后端目标设备所属的网络 ID，如vpc-j9x73ko1，可以通过 DescribeVpcEx 接口获取。 不传此参数则默认为基础网络（"0"）。 示例值： vpc-30xqji93
SubnetId	否	否	String	在私有网络内购买内网负载均衡实例的情况下，必须指定子网 ID，内网负载均衡实例的 VIP 将从这个子网中产生。 示例值： subnet-dva8ji93
ProjectId	否	否	Int64	负载均衡实例所属的项目 ID，可以通过 DescribeProject 接口获取。不传此参数则视为默认项目。 示例值： 0
AddressIPVersion	否	否	String	仅适用于公网负载均衡。IP版本，可取值：IPV4、IPV6、IPv6FullChain，默认值 IPV4。 示例值： IPV4
Number	否	否	Uint64	创建负载均衡的个数，默认值 1。 示例值： 1
MasterZoneId	否	否	String	设置跨可用区容灾时的主可用区ID，例如 100001 或 ap-region1-1 注：主可用区是需要承载流量的可用区，备可用区默认不承载流量，主可用区不可用时才使用备可用区。可通过 DescribeMasterZones 接口查询一个地域的主可用区的列表。 示例值： ap-region1-1
ZoneId	否	否	String	仅适用于公网负载均衡。可用区ID，指定可用区以创建负载均衡实例。

参数名称	必选	允许NULL	类型	描述
				如：ap-region1-1。私有云暂不使用 示例值： ap-region1-1
AnycastZone	否	否	String	仅适用于公网负载均衡。Anycast的发布域，可 取 ZONE_A 或 ZONE_B。仅带宽非上移用户支持此参数。（已下线） 示例值： ZONE_A
InternetAccessible	否	否	InternetAccessible	仅适用于公网负载均衡。负载均衡的网络计费模式。 示例值：查看
VipIsp	否	否	String	仅适用于公网负载均衡。CMCC
Tags	否	否	Array of TagInfo	购买负载均衡同时，给负载均衡打上标签 示例值：查看
ZhiTong	否	否	Bool	是否支持直通。私有云不支持 示例值： true
Vip	否	否	String	指定Vip申请负载均衡，必须同时指定 TgwGroupName 参数 示例值： 139.X.X.X
TgwGroupName	否	否	String	Tgw独占集群的名称 示例值： tg-1
IsDDos	否	否	Bool	是否可绑定高防包。私有云不支持 示例值： true
BandwidthPackageId	否	否	String	带宽包ID，网络计费方式选择带宽包时必须指定带宽包ID 示例值： bwp-pnbeji93
ExclusiveCluster	否	否	ExclusiveCluster	独占集群信息 示例值：查看
SlaveZoneId	否	否	String	设置跨可用区容灾时的备可用区ID，例如 100001 或 ap-region1-1 注：主可用区是需要承载流量的可用区，备可用区默认不承载流量，主可用区不可用时才使用备可用区，自动切换至备可用区。可通 过 DescribeMasterZones 接口查询一个地域的主备可用区的列表。

参数名称	必选	允许NULL	类型	描述
				示例值： ap-region1-1
TgwSetLabels	否	否	Array of String	私有云专用参数，申请内网clb时，可传入四层集群标签，指定四层独占集群 示例值： ["l4-label1"]
StgwSetLabels	否	否	Array of String	私有云专用参数，申请内网clb时，可传入七层集群标签，指定七层独占集群 示例值： ["l7-label1"]
EipAddressId	否	否	String	EIP 的唯一 ID，形如：eip-11112222，仅适用于内网负载均衡绑定EIP。 示例值： eip-1111ji93
ClusterIds	否	否	Array of String	本地专用集群ID 示例值： ["cluster-gbo2ji93"]
IPv6DecoupleVpc	否	否	Int64	是否从vpc侧申请v6地址，1表示跟vpc解耦，不从vpc侧申请地址，0表示不跟vpc解耦，从vpc侧申请地址 示例值： 0

3. 输出参数

参数名称	类型	描述
LoadBalancerIds	Array of String	由负载均衡实例唯一 ID 组成的数组。 示例值： ["lb-6efswuxa"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。

错误码	描述
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。
InvalidParameterValue.Range	参数取值范围错误。

创建负载均衡七层监听器转发规则

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

CreateRule 接口用于在一个已存在的负载均衡七层监听器下创建转发规则，七层监听器中，后端服务必须绑定到规则上而非监听器上。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:35:19。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateRule
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	监听器 ID 示例值： lbl-4fbxji93*
Rules	是	否	Array of RuleInput	新建转发规则的信息 示例值：查看

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
LocationIds	Array of String	创建的转发规则的唯一标识数组 示例值：["loc-ho6lvh8m"]
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

删除证书

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

租户端CLB删除证书

默认接口请求频率限制：20次/秒。

接口更新时间：2021-08-05 17:43:25。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteCert
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
CertIds	是	否	Array of String	证书ID 列表 示例值： ["GpW7fKkH"]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InternalError	内部错误

删除负载均衡监听器

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

本接口用来删除负载均衡实例下的监听器（四层和七层）。
本接口为异步接口，接口返回成功后，需以得到的 RequestID 为入参，调用 DescribeTaskStatus 接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:37:25。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteListener
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	要删除的监听器 ID 示例值： lbl-4udzji93

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

删除负载均衡实例

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DeleteLoadBalancer 接口用以删除指定的一个或多个负载均衡实例。
本接口为异步接口，接口返回成功后，需以返回的 RequestId 为入参，调用 DescribeTaskStatus 接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:37:48。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteLoadBalancer
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerIds	是	否	Array of String	要删除的负载均衡实例 ID数组，数组大小最大支持20 示例值： ["lb-hsb93u5o"]

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

删除负载均衡转发规则之间的重定向关系

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DeleteRewrite 接口支持删除指定转发规则之间的重定向关系。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:29:51。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteRewrite
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-51jjji93
SourceListenerId	是	否	String	源监听器ID 示例值： lbl-r4iaji93
TargetListenerId	是	否	String	目标监听器ID 示例值： lbl-0nonji93
RewriteInfos	是	否	Array of RewriteLocationMap	转发规则之间的重定向关系 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.SomeRewriteNotFound	一些重定向规则不存在。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

删除负载均衡七层监听器的转发规则

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DeleteRule 接口用来删除负载均衡实例七层监听器下的转发规则。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-06 21:37:30。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteRule
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxw2rm0
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-4fbxq45k
LocationIds	否	否	Array of String	要删除的转发规则的ID组成的数组 示例值： ["loc-5lc6ji93"]
Domain	否	否	String	要删除的转发规则的域名，已提供LocationIds参数时本参数不生效 示例值： foo.net

参数名称	必选	允许NULL	类型	描述
Url	否	否	String	要删除的转发规则的转发路径，已提供LocationIds参数时本参数不生效 示例值： /bar2
NewDefaultServerDomain	否	否	String	监听器下必须配置一个默认域名，当需要删除默认域名时，可以指定另一个域名作为新的默认域名。 示例值： www.default.example.com

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue	参数取值错误
UnauthorizedOperation	未授权操作
InvalidParameterValue.Length	参数长度错误。
FailedOperation	操作失败
InternalError	内部错误

从负载均衡监听器上解绑后端服务

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DeregisterTargets 接口用来将一台或多台后端服务从负载均衡的监听器或转发规则上解绑，对于四层监听器，只需指定监听器ID即可，对于七层监听器，还需通过LocationId或Domain+Url指定转发规则。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:36:52。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeregisterTargets
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID，格式如 lb-j9x73ko1 示例值： lb-cuxwji93
ListenerId	是	否	String	监听器 ID，格式如 lbl-j9x73ko1 示例值： lbl-d1ubji93
LocationId	否	否	String	转发规则的ID，格式如 loc-j9x73ko1，当从七层转发规则解绑机器时，必须提供此参数或Domain+Url两者之一 示例值： loc-j9x7ji93
Domain	否	否	String	目标规则的域名，提供LocationId参数时本参数不生效 示例值： www.aaa.com

参数名称	必选	允许NULL	类型	描述
Url	否	否	String	目标规则的URL，提供LocationId参数时本参数不生效 示例值： /home
Targets	是	否	Array of Target	要解绑的后端服务列表，数组长度最大支持20 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

查询用户和绑定的集群标签

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

查询用户和绑定的集群标签

默认接口请求频率限制：20次/秒。

接口更新时间：2021-03-31 15:26:57。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeAppIdLabel
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表

3. 输出参数

参数名称	类型	描述
OwnerLabelSet	Array of OwnerLabel	用户和标签对应关系 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
FailedOperation	操作失败
MissingParameter	缺少参数错误。
UnauthorizedOperation	未授权操作
InternalError	内部错误
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误

查询证书列表

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

查询可用证书列表

默认接口请求频率限制：20次/秒。

接口更新时间：2021-12-17 15:08:53。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCerts
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
Offset	否	否	Uint64	数据偏移量，默认为 0。 示例值： 0
Limit	否	否	Uint64	返回证书的数量，默认为20 示例值： 20
SearchKey	否	否	String	搜索关键字 示例值： lbname
CertType	否	否	String	证书类型（目前支持:CA=客户端证书,SVR=服务器证书） 示例值： SVR
CertIdList	否	否	Array of String	证书id 列表 示例值： ["GpW7fKkH"]
WithCert	否	否	Bool	是否同时获取证书内容 示例值： true

3. 输出参数

参数名称	类型	描述
CertList	Array of CertList	证书列表 示例值：查看
TotalCount	Uint64	证书总数 示例值： 200
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InternalError	内部错误
InvalidParameterValue	参数取值错误
InvalidParameterValue.Duplicate	参数值有重复。
InvalidParameter	参数错误。
MissingParameter	缺少参数错误。
InvalidParameterValue.Length	参数长度错误。

拉取配置绑定的server或location。

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

拉取配置绑定的 server 或 location，如果 domain 存在，结果将根据 domain 过滤。或拉取配置绑定的 loadbalancer。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-03-16 09:51:04。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCustomizedConfigAssociateList
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
UconfigId	否	否	String	配置ID 示例值： pz-fi018waq
Offset	否	否	Int64	拉取绑定关系列表开始位置，默认值 0 示例值： 0
Limit	否	否	Int64	拉取绑定关系列表数目，默认值 20 示例值： 3
Domain	否	否	String	搜索域名 示例值： a.cc
UconfigIds	否	否	Array of String	CLB维度的配置ID列表，不支持根据 Domain 过滤 示例值： [pz-n651fsue]

3. 输出参数

参数名称	类型	描述
BindList	Array of BindDetailItem	绑定关系列表 示例值：查看
TotalCount	Int64	绑定关系总数目 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

拉取配置列表

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

拉取个性化配置列表，返回用户 AppId 下指定类型的配置。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-27 20:50:03。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCustomizedConfigList
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
ConfigType	是	否	String	配置类型:CLB 负载均衡维度。 SERVER 域名维度。 LOCATION 规则维度。 示例值： CLB
Offset	否	否	Int64	拉取页偏移，默认值0 示例值： 0
Limit	否	否	Int64	拉取数目，默认值20 示例值： 20
ConfigName	否	否	String	拉取指定配置名字，模糊匹配。 示例值： custom
UconfigIds	否	否	Array of String	配置ID 示例值： ["pz-j9x73ko1"]

3. 输出参数

参数名称	类型	描述
ConfigList	Array of ConfigListItem	配置列表 示例值：查看
TotalCount	Int64	配置数目 示例值： 1
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.SomeRewriteNotFound	一些重定向规则不存在。
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。
InvalidParameter.RewriteAlreadyExist	转发规则已绑定重定向关系。
InvalidParameter.ProtocolCheckFailed	监听器协议检查失败，比如相关协议不支持对应操作。

错误码	描述
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
InvalidParameterValue.Duplicate	参数值有重复。
InvalidParameter.RegionNotFound	地域无效。
MissingParameter	缺少参数错误。

查询运营商信息

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

查询当前地域所支持的运营商信息

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-16 11:23:56。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeIspInfo
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表

3. 输出参数

参数名称	类型	描述
IspSet	Array of IspSet	运营商信息列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
UnauthorizedOperation	未授权操作
InvalidParameter.RegionNotFound	地域无效。
InternalError	内部错误

根据证书id获取绑定的监听器

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

根据证书id获取绑定的监听器

默认接口请求频率限制：20次/秒。

接口更新时间：2024-11-22 10:35:55。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeListenerListByCertId
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
CertIds	是	否	Array of String	证书id数组 示例值： ["ke93l2xn","84jbxme2"]

3. 输出参数

参数名称	类型	描述
CertSet	Array of CertIdRelatedWithListener	结果集 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InternalError	内部错误
InvalidParameterValue	参数取值错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

查询负载均衡的监听器列表

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DescribeListeners 接口可根据负载均衡器 ID，监听器的协议或端口作为过滤条件获取监听器列表。如果不指定任何过滤条件，则返回该负载均衡实例下的所有监听器。

默认接口请求频率限制：20次/秒。

接口更新时间：2024-07-22 15:10:58。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeListeners
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-aniqji93
ListenerIds	否	否	Array of String	要查询的负载均衡监听器 ID数组 示例值： ["lbl-8cnlji93","lbl-we2d"]
Protocol	否	否	String	要查询的监听器协议类型，取值 TCP
Port	否	否	Int64	要查询的监听器的端口 示例值： 23
Offset	否	否	Int64	显示的偏移起始量。默认0 示例值： 10
Limit	否	否	Int64	显示的条数限制，不传则获取所有。 示例值： 10

参数名称	必选	允许NULL	类型	描述
Filters	否	否	Array of Filter	过滤器数组 示例值：查看
SearchKey	否	否	String	名称模糊搜索 示例值： jfhadsihfgiegs0dfhje2

3. 输出参数

参数名称	类型	描述
Listeners	Array of Listener	监听器列表 示例值：查看
TotalCount	Uint64	总的监听器个数 示例值： 3
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
FailedOperation	操作失败
InvalidParameter	参数错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
UnauthorizedOperation	未授权操作
InternalError	内部错误
InvalidParameterValue	参数取值错误
InvalidParameterValue.Length	参数长度错误。
InvalidParameterValue.InvalidFilter	Filter参数输入错误。

查询负载均衡实例列表

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

查询一个地域的负载均衡实例列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 19:40:46。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeLoadBalancers
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerIds	否	否	Array of String	负载均衡实例ID。实例ID数量上限为20个。 示例值： ["lb-rbw5ji93"]
LoadBalancerType	否	否	String	负载均衡实例的网络类型： OPEN：公网属性， INTERNAL：内网属性。 示例值： OPEN
Forward	否	否	Int64	负载均衡实例的类型。1：通用的负载均衡实例。如果不传此参数，则查询所有类型的负载均衡实例。 示例值： 1
LoadBalancerName	否	否	String	负载均衡实例的名称。 示例值： lb_internal
Domain	否	否	String	云平台为负载均衡实例分配的域名。 示例值： lb-6m46rm32-seji93o0q2g.clb.ap-region1.com
LoadBalancerVips	否	否	Array of String	负载均衡实例的 VIP 地址，支持多个。 示例值： ["44.23.32.32"]
BackendPublicIps	否	否	Array of String	负载均衡绑定的后端服务的外网 IP。 示例值： ["102.23.32.43"]
BackendPrivateIps	否	否	Array of String	负载均衡绑定的后端服务的内网 IP。 示例值： ["172.16.76.87"]
Offset	否	否	Int64	数据偏移量，默认为 0。 示例值： 0
Limit	否	否	Int64	返回负载均衡实例的数量，默认为20，最大值为100。 示例值： 20
OrderBy	否	否	String	排序参数，支持以下字段：LoadBalancerName，CreateTime，Domain，LoadBalancerType。LoadBalancerName表示lb实例名称，CreateTime表示创建时间，Domain表示域名，LoadBalancerType表示实例类型。 示例值： LoadBalancerName
OrderType	否	否	Int64	1：倒序，0：顺序，默认按照创建时间倒序。 示例值： 0
SearchKey	否	否	String	搜索字段，模糊匹配名称、域名、VIP。 示例值： lb-name
ProjectId	否	否	Int64	负载均衡实例所属的项目 ID，可以通过 DescribeProject 接口获取。 示例值： 1
WithRs	否	否	Int64	负载均衡是否绑定后端服务，0：没有绑定后端服务，1：绑定后端服务，-1：查询全部。 示例值： -1
VpcId	否	否	String	负载均衡实例所属私有网络唯一ID，如 vpc-bhqkbhdx。 示例值： vpc-bhqkji93

参数名称	必选	允许NULL	类型	描述
SecurityGroup	否	否	String	安全组ID，如 sg-m1cc9123 示例值： sg-m1ccji93
MasterZone	否	否	String	主可用区ID，如 ："100001" 示例值： 100001
Filters	否	否	Array of Filter	每次请求的 Filters 的上限为10， Filter.Values 的上限为100。详细的过滤条件如下： • internet-charge-type - String - 是否必填：否 -（过滤条件）按照 CLB 的网络计费模式过滤，包括"BANDWIDTH_PREPAID","TRAFFIC_POSTPAID_BY_HOUR","BANDWIDTH_POSTPAID_BY_HOUR","BANDWIDTH_PACKAGE"。 • master-zone-id - String - 是否必填：否 -（过滤条件）按照 CLB 的主可用区ID过滤，如 ："100001"。 • tag-key - String - 是否必填：否 -（过滤条件）按照 CLB 标签的键过滤。 示例值：查看

3. 输出参数

参数名称	类型	描述
TotalCount	Uint64	满足过滤条件的负载均衡实例总数。此数值与入参中的Limit无关。 示例值： 0
LoadBalancerSet	Array of LoadBalancer	返回的负载均衡实例数组。 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
InvalidParameterValue.InvalidFilter	Filter参数输入错误。

查询负载均衡转发规则的重定向关系

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DescribeRewrite 接口可根据负载均衡实例ID，查询一个负载均衡实例下转发规则的重定向关系。如果不指定监听器ID或转发规则ID，则返回该负载均衡实例下的所有重定向关系。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:29:39。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRewrite
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-qc2iji93
SourceListenerIds	否	否	Array of String	负载均衡监听器ID数组 示例值： ["lbl-j36caqde"]
SourceLocationIds	否	否	Array of String	负载均衡转发规则的ID数组 示例值： ["loc-5t7526km"]

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
RewriteSet	Array of RuleOutput	重定向转发规则构成的数组，若无重定向规则，则返回空数组 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。

查询子账号配额

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

主租户查询子账号配额,若无子账号返回主账号配额

默认接口请求频率限制：20次/秒。

接口更新时间：2021-03-01 19:34:53。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeSubUinQuotas
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
SubUin	否	否	Array of String	子账号UIN列表 示例值： ["110000004918"]

3. 输出参数

参数名称	类型	描述
QuotaData	Array of QuotaData	主账号下各类型及其子账号配额列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
FailedOperation	操作失败
InvalidParameter	参数错误。
InternalError	内部错误

获取负载均衡后端服务的健康检查状态

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DescribeTargetHealth 接口用来获取负载均衡后端服务的健康检查结果，不支持传统型负载均衡。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:44:19。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTargetHealth
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerIds	是	否	Array of String	要查询的负载均衡实例 ID列表 示例值： ["lb-qc2iq5yc"]

3. 输出参数

参数名称	类型	描述
LoadBalancers	Array of LoadBalancerHealth	负载均衡实例列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

查询负载均衡绑定的后端服务列表

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

DescribeTargets 接口用来查询负载均衡实例的某些监听器绑定的后端服务列表。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:37:15。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTargets
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-10iq9lou
ListenerIds	否	否	Array of String	监听器 ID列表 示例值： ["lbl-4fo6k8na"]
Protocol	否	否	String	监听器协议类型。支持传：TCP | UDP | HTTP | HTTPS | TCP_SSL 示例值： HTTP
Port	否	否	Int64	监听器端口 示例值： 80

3. 输出参数

参数名称	类型	描述
Listeners	Array of ListenerBackend	监听器后端绑定的机器信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

查询异步任务状态

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

本接口用于查询异步任务的执行状态，对于非查询类的接口（创建/删除负载均衡实例、监听器、规则以及绑定或解绑后端服务等），在接口调用成功后，都需要使用本接口查询任务最终是否执行成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 19:42:49。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeTaskStatus
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
TaskId	否	否	String	请求ID，即接口返回的 RequestId 参数 示例值： 55c85074-3e7f-4c6d-864f-673660d4f8de
DealName	否	否	String	订单id 示例值： 20220828391256

3. 输出参数

参数名称	类型	描述
Status	Int64	任务的当前状态。 0：成功，1：失败，2：进行中。 示例值： 0
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InternalError	内部错误
FailedOperation	操作失败

修改负载均衡配置询价

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

InquiryPriceModifyLoadBalancer接口修改负载均衡配置询价。

默认接口请求频率限制：20次/秒。

接口更新时间：2022-03-22 10:48:08。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：InquiryPriceModifyLoadBalancer
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-dr0mo6w4
InternetAccessible	是	否	InternetAccessible	修改后的网络带宽信息 示例值：查看
SlaType	否	否	String	性能独享型规格型号（私有云不支持） 示例值： clb.c3.small

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
Price	Price	描述价格信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
InternalError	内部错误
InvalidParameter.FormatError	参数格式错误。
FailedOperation	操作失败
InvalidParameter	参数错误。
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
UnauthorizedOperation	未授权操作
InvalidParameterValue	参数取值错误

手动添加负载均衡转发规则的重定向关系

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

用户手动配置原访问地址和重定向地址，系统自动将原访问地址的请求重定向至对应路径的目的地址。同一域名下可以配置多条路径作为重定向策略，实现http/https之间请求的自动跳转。设置重定向时，需满足如下约束条件：若A已经重定向至B，则A不能再重定向至C（除非先删除老的重定向关系，再建立新的重定向关系），B不能重定向至任何其它地址。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:30:03。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ManualRewrite
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-51jjji93
SourceListenerId	是	否	String	源监听器ID 示例值： lbl-0nonji93
TargetListenerId	是	否	String	目标监听器ID 示例值： lbl-r4iaji93

参数名称	必选	允许NULL	类型	描述
RewriteInfos	是	否	Array of RewriteLocationMap	转发规则之间的重定向关系 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.SomeRewriteNotFound	一些重定向规则不存在。
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
InvalidParameter.RewriteAlreadyExist	转发规则已绑定重定向关系。
InvalidParameter.ProtocolCheckFailed	监听器协议检查失败，比如相关协议不支持对应操作。
InvalidParameter.FormatError	参数格式错误。

错误码	描述
InvalidParameterValue.Length	参数长度错误。

修改证书备注

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

修改租户端证书备注

默认接口请求频率限制：20次/秒。

接口更新时间：2021-08-18 18:32:08。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyCertAlias
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
CertId	是	否	String	证书ID 示例值： GpW7fKkH
Alias	是	否	String	证书新备注 示例值： cert-2

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InternalError	内部错误
InvalidParameter	参数错误。
InvalidParameterValue.Length	参数长度错误。

修改负载均衡七层监听器转发规则的域名级别属性

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

ModifyDomainAttributes接口用于修改负载均衡7层监听器转发规则的域名级别属性，如修改域名、修改DefaultServer、开启/关闭Http2、修改证书。
本接口为异步接口，本接口返回成功后，需以返回的RequestId为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-06 21:40:04。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyDomainAttributes
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-1wvlji93
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-n8mbji93
Domain	是	否	String	域名（必须是已经创建的转发规则下的域名） 示例值： foo.net

参数名称	必选	允许NULL	类型	描述
NewDomain	否	否	String	要修改的新域名 示例值： www.new.example.com
Certificate	否	否	CertificateInput	域名相关的证书信息，注意，仅对启用SNI的监听器适用。 示例值：查看
Http2	否	否	Bool	是否开启Http2，注意，只有HTTPS域名才能开启Http2。1表示开启，0表示不开启 示例值： true
DefaultServer	否	否	Bool	是否设为默认域名，注意，一个监听器下只能设置一个默认域名。true表示设置为默认域名，0表示不设置 示例值： true
NewDefaultServerDomain	否	否	String	监听器下必须配置一个默认域名，若要关闭原默认域名，必须同时指定另一个域名作为新的默认域名。 示例值： www.yuncloud.example.com

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue	参数取值错误

错误码	描述
UnauthorizedOperation	未授权操作
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。
FailedOperation	操作失败
InternalError	内部错误

修改负载均衡监听器属性

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

ModifyListener接口用来修改负载均衡监听器的属性，包括监听器名称、健康检查参数、证书信息、转发策略等。本接口不支持传统型负载均衡。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2019-10-22 12:17:13。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyListener
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-d1ubji93
ListenerName	否	否	String	新的监听器名称 示例值： newlis
SessionExpireTime	否	否	Int64	会话保持时间，单位：秒。可选值：30~3600，默认 0，表示不开启。此参数仅适用于TCP/UDP监听

参数名称	必选	允许NULL	类型	描述
				器。 示例值： 120
HealthCheck	否	否	HealthCheck	健康检查相关参数，此参数仅适用于TCP/UDP/TCP_SSL监听器 示例值：查看
Certificate	否	否	CertificateInput	证书相关信息，此参数仅适用于HTTPS/TCP_SSL监听器 示例值：查看
Scheduler	否	否	String	监听器转发的方式。可选值：WRR、LEAST_CONN 分别表示按权重轮询、最小连接数， 默认为 WRR。 示例值： LEAST_CONN
SniSwitch	否	否	Int64	是否开启SNI特性，此参数仅适用于HTTPS监听器。注意：未开启SNI的监听器可以开启SNI；已开启SNI的监听器不能关闭SNI。1表示开启，0表示不开启 示例值： 0
TargetType	否	否	String	后端目标类型，NODE表示绑定普通节点 示例值： NODE
DefaultSerSwitch	否	否	Bool	监听器是否支持设置默认域名。0表示不支持，1表示支持，默认为1支持 示例值： false
NewDefaultServerDomain	否	否	String	开启监听器默认域名开关时，指定该监听器下任意域名为默认域名，当DefaultSerSwitch传值为ture时，且该监听器有存量域名时，该参数为必填，并同时生效。 示例值： foo.net

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

修改负载均衡实例的属性

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

修改负载均衡实例的属性。支持修改负载均衡实例的名称、设置负载均衡的跨域属性。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-09-04 14:41:39。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyLoadBalancerAttributes
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡的唯一ID 示例值： lb-6efswuxa
LoadBalancerName	否	否	String	负载均衡实例名称 示例值： newlbname
TargetRegionInfo	否	否	TargetRegionInfo	负载均衡绑定的后端服务的地域信息 示例值：查看
InternetChargeInfo	否	否	InternetAccessible	网络计费相关参数 示例值：查看
LoadBalancerPassToTarget	否	否	Bool	Target是否放通来自CLB的流量。开启放通（true）：只验证CLB上的安全组；不开启放通

参数名称	必选	允许NULL	类型	描述
				（false）：需同时验证CLB和后端实例上的安全组。 示例值： true
ChargeType	否	否	String	负载均衡实例的计费类型，后付费：POSTPAID_BY_HOUR，预付费：PREPAID。 示例值： POSTPAID_BY_HOUR
SwitchFlag	否	否	Uint64	不同计费模式之间的切换：0表示不切换，1表示预付费和后付费切换，2表示后付费之间切换。默认值：0 示例值： 0
PrepaidInfo	否	否	LBChargePrepaid	负载均衡实例的预付费相关属性 示例值：查看
ExclusiveCluster	否	否	ExclusiveCluster	7层集群列表 示例值：查看
SnatPro	否	否	Bool	是否开启跨地域绑定2.0功能（私有云不支持） 示例值： false

3. 输出参数

参数名称	类型	描述
DealName	String	切换负载均衡计费方式时，可用此参数查询切换任务是否成功。 示例值： null
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
LimitExceeded	超过配额限制
MissingParameter	缺少参数错误。

错误码	描述
FailedOperation	操作失败
InvalidParameter	参数错误。
InvalidParameter.FormatError	参数格式错误。
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameterValue.Duplicate	参数值有重复。
ResourceInsufficient	资源不足
UnauthorizedOperation	未授权操作
InternalError	内部错误
InvalidParameterValue	参数取值错误
InvalidParameterValue.Length	参数长度错误。
InvalidParameter.RegionNotFound	地域无效。

修改负载均衡七层监听器的转发规则

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

ModifyRule 接口用来修改负载均衡七层监听器下的转发规则的各项属性，包括转发路径、健康检查属性、转发策略等。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2019-10-22 20:16:49。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyRule
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxw2rm0
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-4fbxq45k
LocationId	是	否	String	要修改的转发规则的 ID。 示例值： loc-9dr7bsl3
Url	否	否	String	转发规则的新的转发路径，如不需修改Url，则不需提供此参数 示例值： /bar

参数名称	必选	允许NULL	类型	描述
HealthCheck	否	否	HealthCheck	健康检查信息 示例值：查看
Scheduler	否	否	String	规则的请求转发方式，可选值：WRR、LEAST_CONN、IP_HASH 分别表示按权重轮询、最小连接数、按IP哈希， 默认为 WRR。 示例值： LEAST_CONN
SessionExpireTime	否	否	Int64	会话保持时间 示例值： 75
ForwardType	否	否	String	负载均衡实例与后端服务之间的转发协议，默认HTTP，可取值：HTTP、HTTPS 示例值： HTTP
TargetType	否	否	String	后端目标类型，NODE表示绑定普通节点 示例值： NODE

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。

错误码	描述
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

修改监听器绑定的后端机器的端口

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

ModifyTargetPort接口用于修改监听器绑定的后端服务的端口。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:37:58。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyTargetPort
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-d1ubji93
LocationId	否	否	String	转发规则的ID，当后端服务绑定到七层转发规则时，必须提供此参数或Domain+Url两者之一 示例值： loc-fi8gji93
Domain	否	否	String	目标规则的域名，提供LocationId参数时本参数不生效 示例值： www.yuncloud.example.com
Url	否	否	String	目标规则的URL，提供LocationId参数时本参数不生效

参数名称	必选	允许NULL	类型	描述
				示例值： /index
Targets	是	否	Array of Target	要修改端口的后端服务列表 示例值：查看
NewPort	是	否	Int64	后端服务绑定到监听器或转发规则的新端口 示例值： 334

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

修改监听器绑定的后端机器的转发权重

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

ModifyTargetWeight 接口用于修改负载均衡绑定的后端服务的转发权重。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-04-27 18:07:01。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyTargetWeight
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-d1ubji93
LocationId	否	否	String	转发规则的ID，当绑定机器到七层转发规则时，必须提供此参数或Domain+Url两者之一 示例值： loc-fi8gji93
Domain	否	否	String	目标规则的域名，提供LocationId参数时本参数不生效 示例值： www.new.example.com
Url	否	否	String	目标规则的URL，提供LocationId参数时本参数不生效

参数名称	必选	允许NULL	类型	描述
				示例值： /index
Targets	是	否	Array of Target	要修改权重的后端服务列表 示例值：查看
Weight	否	否	Int64	后端服务新的转发权重，取值范围：0~100，默认值10。如果设置了 Targets.Weight 参数，则此参数不生效。 示例值： 8

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。

绑定后端机器到监听器上

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

RegisterTargets 接口用来将一台或多台后端服务绑定到负载均衡的监听器（或7层转发规则），在此之前您需要先行创建相关的4层监听器或7层转发规则。对于四层监听器（TCP、UDP），只需指定监听器ID即可，对于七层监听器（HTTP、HTTPS），还需通过LocationId或者Domain+Url指定转发规则。
本接口为异步接口，本接口返回成功后需以返回的RequestID为入参，调用DescribeTaskStatus接口查询本次任务是否成功。

默认接口请求频率限制：20次/秒。

接口更新时间：2020-01-10 20:37:04。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：RegisterTargets
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
LoadBalancerId	是	否	String	负载均衡实例 ID 示例值： lb-cuxwji93
ListenerId	是	否	String	负载均衡监听器 ID 示例值： lbl-d1ubji93
LocationId	否	否	String	转发规则的ID，当绑定后端服务到七层转发规则时，必须提供此参数或Domain+Url两者之一 示例值： loc-fi8gji93
Domain	否	否	String	目标转发规则的域名，提供LocationId参数时本参数不生效 示例值： www.yuncloud.example.com

参数名称	必选	允许NULL	类型	描述
Url	否	否	String	目标转发规则的URL，提供LocationId参数时本参数不生效 示例值： /index
Targets	是	否	Array of Target	待绑定的后端服务列表，数组长度最大支持20 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
ResourceInsufficient	资源不足
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Length	参数长度错误。
MissingParameter	缺少参数错误。

替换证书

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

使用新证书替换原有证书注意：若原证书在多个region上使用，则同时替换原证书绑定的规则。

默认接口请求频率限制：20次/秒。

接口更新时间：2021-08-23 21:36:44。

接口只能签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ReplaceCert
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
OldCertId	是	否	String	新证书ID 示例值：GpW7fKkH
NewCertId	否	否	String	新证书ID；注：新证书公钥、备注、私钥和域参数不能同时传入 示例值：GpW7fKkH
NewCertContent	否	否	String	新证书公钥；注：新证书ID和域参数不能同时传入 示例值：-----BEGIN CERTIFICATE-----\r\nMIIEqTCCA7WgAwIBAgIQA4ZHUAVOv4ynuI3ILfo3TANBgkqhkiG9w0BAQsFADBy\r\nMQswCQYDVQQGEwIDRjERMA8GA1UECAwIRGVsYXdhcmUxEzARBgNVBAcMCk5ld2Fl\r\nY2FzdGxlMRswGQYDVQQKDBJUcnVzdC1Qcm92aWRlciBMdGQuMSIwIAYDVQQDDBlU\r\nVHJVU1QgRUNDIFJvb3QgQ0EgMSAwHgYDVQQLDBdodHBzOi8vY3ndS3ILmRpZ2ljZXI0LmNvbS9DUFMwCAYGZ4EMAQIBMIGBBggrBgEFBQcBAQR1MHMwVyn/QYGKwYBBQUHMAGGSWh0dHA6Ly9VY3NwMi5kaWdpY2VydC5jb20vSg1fW

负载均衡维度的个性化配置相关操作

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

负载均衡维度的个性化配置相关操作：创建、删除、修改、绑定、解绑

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-24 17:42:43。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetCustomizedConfigForLoadBalancer
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
OperationType	是	否	String	操作类型。 - ADD：添加 - DELETE：删除 - UPDATE：修改 - BIND：绑定 - UNBIND：解绑 示例值： ADD
UconfigId	否	否	String	除了创建个性化配置外，必传此字段，如：pz-j9x7gx3g 示例值： pz-n651fsue
ConfigContent	否	否	String	创建个性化配置或修改个性化配置的内容时，必传此字段 示例值： client_max_body_size 222M;
ConfigName	否	否	String	创建个性化配置或修改个性化配置的名字时，必传此字段 示例值： config_1

参数名称	必选	允许NULL	类型	描述
LoadBalancerIds	否	否	Array of String	绑定解绑时，必传此字段 示例值： [lb-55rh44i6]

3. 输出参数

参数名称	类型	描述
ConfigId	String	个性化配置ID，如：pz-j9x7gx3g 示例值： pz-j9x7gx3g
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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。
InvalidParameterValue	参数取值错误
InternalError	内部错误
UnauthorizedOperation	未授权操作
LimitExceeded	超过配额限制
FailedOperation	操作失败
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameter.FormatError	参数格式错误。
MissingParameter	缺少参数错误。

设置子账号配额

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

通过主租户账号设置子账号clb实例相关配额

默认接口请求频率限制：20次/秒。

接口更新时间：2021-02-22 14:29:33。

接口只验签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：SetSubUinQuotas
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
SubQuota	是	否	Array of SubQuota	子账号配额列表 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 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
FailedOperation	操作失败
InvalidParameter	参数错误。
InternalError	内部错误

上传证书

1. 接口描述

接口请求域名： clb.api3.finance.cloud.tencent.com。

客户端上传ssl证书

默认接口请求频率限制：20次/秒。

接口更新时间：2021-08-18 18:37:39。

接口只能签名不鉴权。

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	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：UpLoadCert
Version	是	否	String	公共参数，本接口取值：2018-03-17
Region	是	否	String	公共参数，地域信息可通过DescribeRegions接口查看产品支持的地域列表
CertContent	是	否	String	证书内容 示例值：-----BEGIN CERTIFICATE-----\r\nMIIEjTCCA3WgAwIBAgIQA4ZHUAVOv4ynuI3LIcJoITANBgkqhkiG9w0BAQsFADByMQswCQYDVQQGEwJDTjElMCMGA1UEChMcVHVhd2VpIFRlY2hub2xvZ2llcywgYy5vSWjLjEdMBsGA1UECxMURG9tYWluIFZhbGlkYXRlZCBTU0wxHTAbBgNVBAMTFFRyYy5vSXNDQXNpYSBUTFMgUNBIENBM84XDTE4MDEwOTAwMDAwMFoXDTE5MDEwOTEyMDAwMFowFjEUMBIGA1UEAxMLZmx5Zmx5cm5hbWUwggEiMA0GCSqGSIb3DQEBAQUAA4IBjyAwDwAwggEKAoIBAQDWsAxgBf4xBAREBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCwwKAYIKwYBBQUHAgEWHGh0dHBzOi8vY3ByLnJlZ2lzLnRlbmNlbnQuY29tL3BzLzAfBgNVHSMEGDAWgBSBkqv8gvBgTBQcBAQR1MHMwKwYIKwYBBQUHMAGGH2h0dHA6Ly9YWNlcnRzLmRpZ2ljZXJ0dmFwaWRhdGUvbi5jb20vYH1/yrc3RBc2hWExTUNBQ2BuY1J0MAkGA1UdEwQCMAAwCCkcMXcpwKB94dyXBLiL4HdSjThVLVM1aArVyrlySS69q55dTUBFtIFP3uh8WdhE3nYRngvoHAAMjlvuBqgGPYbqpnHYjb8fmjwtfYvrC9CZcjkqHmwTSpjXuRjbDLx/BXd1QELTNXevBaiku90EI56W2IH372GmQbJEIoYuYyPREP3BtIBbmfEu4p7+UzwwuQuDBcEUVuGJvTcUN2uAGZGoohydrDRWmBkqBNY9cYyrtYOuRoekxYT4IaIrtSJ4Xkkw=\r\n-----END CERTIFICATE-----\r\n
CertType	是	否	String	证书类型（目前支持CA+ 客户端证书或SVR+服务器证书） 示例值：SVR
CertKey	否	否	String	证书私钥 示例值：-----BEGIN RSA PRIVATE KEY-----\r\nMIIEogIBAAKCAQEApaZ4oAe692ob+wTLkMPSxwfWHbt6nEVG1/RDEcq4hqyW5d/r/nz6REJ/FOLU+DGREr1j0dK+1BhwB1aAv1I8BkMOv5u+wU/3yH+HELRMs+tYKKEQ9WVyrJoKmy0wCIXxhYWYpJzDECL7mGwP5dmMUQxDZfMAYXBa4BVk0Ym5xUgtGz749aLeKVsrJmVDmSGmvZGkApt+0UFAWouoN2AYfh5/YG+xz7PDqByILmAaOmgMjmK/haawPyrJnFvDOq+C6UvlakX54O/mxChhPnbLLF30TAU6NEo6foRI3jPMaro2yvk+ypBfeV/jyn9dsRmLrh/qqj78f4AFvYjKoiLID7g/tkAEZhQgYJn1SQuaYVRI+E8eeVUdQhHcfCyAUbIAEpZzV2TtLd+DFqXbTvTBTLcUA49hUowN3EwSBAoGBAMHwnjWc1y1n+YvBW5yCxFQcsqqqaylwB89H6kdk+p0fDIVZQO80VB3bt6tbWXrOoYAzYAabQeKYunAfNqVQcDEuO3gtZpJTHCI6VBbKaNHG41Ang32VW3XGb+MeBkiZwBk4JfbLrzB9InVynte4M9PjVpYluEQCi2vUjhd+LJRub7TUX0HFLAoGAU0K3pXwaNB5aDgEfXIG9kbUBfuYnteMVPJVpYu

数据结构

Backend

监听器绑定的后端服务的详细信息

被如下接口引用：DescribeTargets

名称	必选	允许NULL	类型	描述
Type	是	否	String	后端服务的类型，可取：CVM、EMS、ENI 示例值：CVM
InstanceId	是	否	String	后端服务的唯一 ID，如 ins-qx3ig9x7 示例值：ins-qx3ig9x7
Port	是	否	Int64	后端服务的监听端口 示例值：80
Weight	是	否	Int64	后端服务的转发权重，取值范围：[0, 100]，默认为 10。 示例值：10
PublicIpAddresses	是	是	Array of String	后端服务的外网 IP 示例值：1.1.1.1
PrivateIpAddresses	是	是	Array of String	后端服务的内网 IP 示例值：10.0.0.1
InstanceName	是	是	String	后端服务的实例名称 示例值：ccm-1
RegisteredTime	是	是	String	后端服务被绑定的时间 示例值：2021-12-29 14:38:50
EniId	是	是	String	弹性网卡唯一ID，如 eni-j9x7gx3g 示例值：eni-j9x7gx3g

Listener

监听器的信息

被如下接口引用：DescribeListeners

名称	必选	允许NULL	类型	描述
ListenerId	是	否	String	负载均衡监听器 ID 示例值：lbl-odt45q4g
Protocol	是	否	String	监听器协议 示例值：HTTP
ProtocolFake	否	否	String	监听器协议(Fake) 示例值：TCP
Port	是	否	Int64	监听器端口 示例值：80
Certificate	是	是	CertificateOutput	监听器绑定的证书信息 示例值：查看
HealthCheck	是	是	HealthCheck	监听器的健康检查信息 示例值：查看
Scheduler	是	是	String	请求的调度方式 示例值：WRR
SessionExpireTime	是	是	Int64	会话保持时间 示例值：0
SniSwitch	是	是	Int64	是否开启SNI特性（本参数仅对于HTTPS监听器有意义） 示例值：0
Rules	是	是	Array of RuleOutput	监听器下的全部转发规则（本参数仅对于HTTP/HTTPS监听器有意义） 示例值：查看
ListenerName	是	是	String	监听器的名称 示例值：Name
CreateTime	是	是	String	监听器的创建时间。 示例值：2021-03-01 15:27:04
EndPort	是	是	Int64	端口段结束端口 示例值：0
TargetType	是	是	String	后端服务器类型 示例值：NODE
TargetGroup	是	是	BasicTargetGroupInfo	绑定的目标组基本信息，当监听器绑定目标组时，会返回该字段 示例值：查看
DefaultServerIp	是	是	Uint64	监听器是否开启设置默认域名标识，0为未开启；1为开启 示例值：0
DeregisterTargetRst	是	是	Bool	解绑后端目标时，是否发RST给客户端，（此参数仅对于TCP监听器有意义）。 示例值：false
Toa	是	是	Bool	仅支持Nat64 CLB TCP监听器 示例值：false
SessionType	否	是	String	会话保持类型，NORMAL表示默认会话保持类型，QUIC_CID 表示根据Quic Connection ID保会话保持。 示例值：NORMAL
KeepaliveEnable	否	是	Int64	是否开启长连接，1开启，0关闭，（本参数仅对于HTTP/HTTPS监听器有意义） 示例值：0

CertificateInput

证书信息

被如下接口引用：CreateListener、CreateRule、ModifyDomainAttributes、ModifyListener

名称	必选	允许NULL	类型	描述
SSLMode	否	否	String	认证类型，UNIDIRECTIONAL：单向认证，MUTUAL：双向认证 示例值：MUTUAL
CertId	否	否	String	服务端CA证书的 ID，如果不填写此项则必须上传证书，包括 CertContent，CertKey，CertName。 示例值：jfkl3sx2
CertCaId	否	否	String	客户端CA证书的 ID，当监听器采用双向认证，即 SSLMode=MUTUAL 时，如果不填写此项则必须上传客户端证书，包括 CertCaContent，CertCaName。 示例值：jfkl3sx2
CertName	否	否	String	上传服务端RSA证书的名称，如果没有 CertId，则此项必传。 示例值：cert-1
CertKey	否	否	String	上传服务端RSA证书的 key，如果没有 CertId，则此项必传。 示例值：-----BEGIN RSA PRIVATE KEY-----\r\n[行93加\r\n]-----END RSA PRIVATE KEY-----\r\n
CertContent	否	否	String	上传服务端RSA证书的内容，如果没有 CertId，则此项必传。 示例值：-----BEGIN CERTIFICATE-----\r\nMIIEJTCCA1WgAwIBAgIQA4ZHUAVO+4ynxI3LfoSTANBgkqhkiG9w0BAQsFADByMQswCQYDVQQGEwJDTjElMCMGA1UEChMcVHVhd2VpIFRlbGVjb20gQ28uLCBMdGQuMUswSQYDVQQLEwJDTjElMCMGA1UEChMcVHVhd2VpIFRlbGVjb20gQ28uLCBMdGQuMUswSQYDVQQD

子账号配额描述

被如下接口引用：SetSubUinQuotas

名称	必选	允许NULL	类型	描述
SubUin	是	否	String	子账号Uin 示例值： 1100000004918
Type	是	否	Uint64	配额类型（4:公网实例配额；7:内网实例配额） 示例值： 4
Quota	是	否	Uint64	配额值 示例值： 10

CertIdRelatedWithListener

证书ID，以及绑定书相关的负载均衡监听器列表

被如下接口引用：DescribeListenerListByCertId

名称	必选	允许NULL	类型	描述
CertId	是	否	String	证书ID 示例值： jfsdjk23x
Listeners	是	否	Array of CertListener	证书相关的监听器列表 示例值：查看

LoadBalancerHealth

负载均衡实例的健康检查状态

被如下接口引用：DescribeTargetHealth

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	负载均衡实例ID 示例值： lb-d3kx902
LoadBalancerName	是	是	String	负载均衡实例名称 示例值： lb-1
Listeners	是	是	Array of ListenerHealth	监听器列表 示例值：查看

MasterZoneInfo

主可用区相关信息

被如下接口引用：DescribeMasterZones

名称	必选	允许NULL	类型	描述
ZoneId	是	是	Uint64	可用区数值形式的唯一ID，如：100001 示例值： 50010001
Zone	是	是	String	可用区字符串形式的唯一ID，如：ap-region1-1 示例值： 50010001
ZoneName	是	是	String	可用区名称，如：可用区1 示例值： 50010001
BackupZoneSet	是	是	Array of ZoneInfo	备可用区列表 示例值：查看
LBType	否	是	String	返回的可用区类型，取值范围：open、internal 示例值： open
AvailableIsps	否	是	Array of AvailableIspInfo	返回的各个运营商可使用情况 示例值：查看

CertIdRelatedWithLoadBalancers

证书ID，以及与该证书ID关联的负载均衡实例列表

被如下接口引用：DescribeLoadBalancerListByCertId

名称	必选	允许NULL	类型	描述
CertId	是	否	String	证书ID 示例值： jfsi3xs2
LoadBalancers	是	是	Array of LoadBalancer	与证书关联的负载均衡实例列表 示例值：查看

RuleInput

HTTP/HTTPS转发规则（输入）

被如下接口引用：CreateRule

名称	必选	允许NULL	类型	描述
Domain	是	否	String	转发规则的域名，长度限制为：1~80。 示例值： www.realdomain.com
Url	是	否	String	转发规则的路径，长度限制为：1~200。 示例值： /local
SessionExpireTime	否	否	Int64	会话保持时间，设置为0表示关闭会话保持，开启会话保持时取值30~3600，单位：秒。 示例值： 30
HealthCheck	否	否	HealthCheck	健康检查信息 示例值：查看
Certificate	否	否	CertificateInput	证书信息 示例值：查看
Scheduler	否	否	String	规则的请求转发方式，可选值：WRR、LEAST_CONN、IP_HASH 分别表示按权重轮询、最小连接数、按IP哈希，默认为 WRR。 示例值： WRR
ForwardType	否	否	String	负载均衡与后端服务之间的转发协议，目前支持 HTTP/HTTPS/TRPC 示例值： HTTP
DefaultServer	否	否	Bool	是否将该域名设为默认域名，注意，一个监听器下只能设置一个默认域名。 示例值： true
Http2	否	否	Bool	是否开启Http2，注意，只有HTTPS域名才能开启Http2。 示例值： true
TargetType	否	否	String	后端目标类型，NODE表示绑定普通节点，TARGETGROUP表示绑定目标组 示例值： NODE
TrpcCallee	否	否	String	TRPC被调服务器路由，ForwardType为TRPC时必填 示例值： trpcall
TrpcFunc	否	否	String	TRPC调用服务接口，ForwardType为TRPC时必填 示例值： trpcFunc

ZoneInfo

可用区相关信息

被如下接口引用：DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc、DescribeMasterZones

名称	必选	允许NULL	类型	描述
ZoneId	是	是	Uint64	可用区数值形式的唯一ID，如：100001 示例值： 100001
Zone	是	是	String	可用区字符串形式的唯一ID，如：ap-region1-1 示例值： ap-region1-1
ZoneName	是	是	String	可用区名称，如：可用区1 示例值： 可用区1
ZoneRegion	否	是	String	可用区所在地域 示例值： ap-region1
LocalZone	否	是	Bool	可用区是否是LocalZone可用区 示例值： false
EnableShared	否	是	Bool	可用区是否有共享集群可用 示例值： true
EnableL4SetLabels	否	是	Array of String	可用区可使用四层集群标签 示例值： ["l4-label"]
Availableisps	否	否	Array of AvailableIspInfo	可用区可使用运营商信息集合 示例值：查看

BatchTarget

批量修改类型

被如下接口引用：BatchDeregisterTargets、BatchRegisterTargets

名称	必选	允许NULL	类型	描述
ListenerId	是	否	String	监听器ID 示例值： lbl-2gaxjl93
InstanceId	否	否	String	子机ID 示例值： ins-1vkjjl93
EniIp	否	否	String	弹性网卡ip 示例值： 10.0.X.X
Port	是	否	Int64	绑定端口 示例值： 80
Weight	否	否	Int64	子机权重，范围0-100。绑定时如果不存在，则默认为10。 示例值： 10
LocationId	否	否	String	七层规则ID 示例值： lbl-4apyjl93

FunctionInfo

SCF云函数（Serverless Cloud Function）相关信息。

被如下接口引用：DescribeTargetHealth、DescribeTargets

名称	必选	允许NULL	类型	描述
FunctionNamespace	否	是	String	函数命名空间 示例值： default
FunctionName	否	是	String	函数名称 示例值： function-1
FunctionQualifier	否	是	String	函数的版本名称或别名 示例值： $latest
FunctionQualifierType	否	是	String	标识 FunctionQualifier 参数的类型，可取值：VERSION（版本）、ALIAS（别名） 示例值： VERSION

LBChargePrepaid

lb实例包年包月相关配置属性

被如下接口引用：DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc、InquiryPriceCreateLoadBalancer、ModifyLoadBalancerAttributes

名称	必选	允许NULL	类型	描述
RenewFlag	否	是	String	续费类型：AUTO_RENEW 自动续费， MANUAL_RENEW 手动续费 示例值： MANUAL_RENEW
Period	否	是	Int64	购买时长，单位：月 示例值： 100

TargetHealth

描述一个Target的健康信息

被如下接口引用：DescribeTargetHealth

名称	必选	允许NULL	类型	描述
IP	是	否	String	Target的内网IP 示例值： 10.0.0.1'

名称	必选	允许NULL	类型	描述
Port	是	否	Int64	Target绑定的端口 示例值： 80
HealthStatus	是	否	Bool	当前健康状态，true：健康，false：不健康（包括尚未开始探测、探测中、状态异常等几种状态），只有处于健康状态（且权重大于0），负载均衡才会向其转发流量。 示例值： true
TargetId	是	否	String	Target的实例ID，如 ins-j9x73lio1 示例值： 'ins-j9x73lio1'
HealthStatusDetial	是	否	String	当前健康状态的详细信息。如：Alive、Dead、Unknown、Alive状态为健康，Dead状态为异常，Unknown状态包括尚未开始探测、探测中、状态未知。 示例值： 'Alive'

ItemPrice

描述了单项的价格信息

被如下接口引用：InquiryPriceCreateLoadBalancer、InquiryPriceModifyLoadBalancer

名称	必选	允许NULL	类型	描述
UnitPrice	是	是	Float	后付费单价 示例值： 10
ChargeUnit	是	是	String	后付计价单元，可取值范围： HOUR：表示计价单元是按每小时来计量。当前涉及该计价单元的场景有：实例按小时后付费（POSTPAID_BY_HOUR）、带宽按小时后付费（BANDWIDTH_POSTPAID_BY_HOUR）； GB：表示计价单元是按每GB来计量。当前涉及该计价单元的场景有：流量按小时后付费（TRAFFIC_POSTPAID_BY_HOUR）。 示例值： HOUR
OriginalPrice	是	是	Float	预支费用的原价 示例值： 50
DiscountPrice	是	是	Float	预支费用的折扣价 示例值： 50
UnitPriceDiscount	是	是	Float	后付费的折扣单价 示例值： 10
Discount	是	是	Float	折扣，如20.0代表2折。 示例值： 100

BasicTargetGroupInfo

监听器或者转发规则绑定的目标组基本信息

被如下接口引用：DescribeListeners、DescribeRewrite

名称	必选	允许NULL	类型	描述
TargetGroupId	是	否	String	目标组ID 示例值： tg-di3kx902
TargetGroupName	是	否	String	目标组名称 示例值： tg-1

Price

表示负载均衡的价格

被如下接口引用：InquiryPriceCreateLoadBalancer、InquiryPriceModifyLoadBalancer

名称	必选	允许NULL	类型	描述
InstancePrice	是	是	ItemPrice	描述了实例价格。 示例值： 查看
BandwidthPrice	是	是	ItemPrice	描述了网络价格。 示例值： 查看

ExclusiveCluster

独占集群

被如下接口引用：CreateLoadBalancer、DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc、ModifyLoadBalancerAttributes

名称	必选	允许NULL	类型	描述
L4Clusters	否	是	Array of ClusterItem	4层独占集群列表 示例值： 查看
L7Clusters	否	是	Array of ClusterItem	7层独占集群列表 示例值： 查看
ClassicalCluster	否	是	ClusterItem	vpcgw集群 示例值： 查看

Filter

过滤器条件

被如下接口引用：DescribeListeners、DescribeLoadBalancers

名称	必选	允许NULL	类型	描述
Name	是	否	String	过滤器的名称 示例值： loadbalancerids
Values	是	否	Array of String	过滤器的值数组 示例值： ["lb-di3kx902"]

ListenerHealth

监听器的健康检查信息

被如下接口引用：DescribeTargetHealth

名称	必选	允许NULL	类型	描述
ListenerId	是	否	String	监听器ID 示例值： lbl-di3kx902
ListenerName	是	是	String	监听器名称 示例值： lbl-1
Protocol	是	否	String	监听器的协议 示例值： TCP
Port	是	否	Int64	监听器的端口 示例值： 80
Rules	是	是	Array of RuleHealth	监听器的转发规则列表 示例值： 查看

ProjectInfo

证书项目信息

被如下接口引用：DescribeCerts

名称	必选	允许NULL	类型	描述
ProjectId	是	否	String	项目ID 示例值： kdhs2kx9
OwnerUin	是	否	String	项目所有人 示例值： 110000004918
Name	是	否	String	项目名称 示例值： pj1
CreatorUin	是	否	String	创建者 示例值： 110000004918
CreateTime	是	否	String	创建时间 示例值： 2014-08-03 12:00:00
Info	是	否	String	项目信息 示例值： info-1

RewriteTarget

重定向目标的信息

被如下接口引用：DescribeListeners、DescribeRewrite

名称	必选	允许NULL	类型	描述
TargetListenerId	是	是	String	重定向目标的监听器ID 注意：此字段可能返回 null，表示无重定向。 示例值： lbl-di3kx902
TargetLocationId	是	是	String	重定向目标的转发规则ID 注意：此字段可能返回 null，表示无重定向。 示例值： loc-di3kx902
RewriteCode	是	是	Int64	重定向状态码 示例值： 302
TakeUrl	是	是	Bool	重定向是否携带匹配到url 示例值： true
RewriteType	是	是	String	重定向类型，Manual: 手动重定向，Auto: 自动重定向 示例值： Auto

TargetRegionInfo

负载均衡实例所绑定的后端服务的信息，包括所属地域、所属网络。

被如下接口引用：DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc、ModifyLoadBalancerAttributes

名称	必选	允许NULL	类型	描述
Region	是	否	String	Target所属地域，如 ap-region1 示例值： ap-region1
VpcId	是	否	String	Target所属网络，私有网络格式如 vpc-gx1g9x7，如果是基础网络，则为"0" 示例值： vpc-9kcqgj93

IspSet

运营商信息描述

被如下接口引用：DescribeIspInfo

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	运营商ID 示例值： 2
Type	是	否	String	运营商类型 示例值： CMCC
Name	是	否	String	运营商名称 示例值： 移动
IspStatus	是	否	Uint64	运营商IPv4状态 示例值： 1
IspStatusIPv6	是	否	Uint64	运营商IPv6状态 示例值： 1
V4alias	否	否	String	运营商v4别名 示例值： 移动
V6alias	否	否	String	运营商v6别名 示例值： 移动

RewriteLocationMap

转发规则之间的重定向关系

被如下接口引用：DeleteRewrite、ManualRewrite

名称	必选	允许NULL	类型	描述
SourceLocationId	是	否	String	源转发规则ID 示例值： loc-i82kji93

名称	必选	允许NULL	类型	描述
TargetLocationId	是	否	String	重定向至的目标转发规则ID 示例值：loc-lavxji93
RewriteCode	否	否	Uint64	重定向状态码，可取值301,302,307 示例值：302
TakeUrl	否	否	Bool	重定向是否携带匹配的url，配置RewriteCode时必填 示例值：true
SourceDomain	否	否	String	源转发的域名，必须是SourceLocationId对应的域名，配置RewriteCode时必填 示例值：source.com

RuleOutput

HTTP/HTTPS监听器的转发规则（输出）

被如下接口引用：DescribeListeners、DescribeRewrite

名称	必选	允许NULL	类型	描述
LocationId	否	否	String	转发规则的 ID 示例值：loc-jkdsia03
Domain	是	是	String	转发规则的域名。 示例值：www.waldomain.com
Url	是	是	String	转发规则的路径。 示例值：/url1
SessionExpireTime	否	否	Int64	会话保持时间 示例值：0
HealthCheck	否	是	HealthCheck	健康检查信息 示例值：查看
Certificate	否	是	CertificateOutput	证书信息 示例值：查看
Scheduler	否	否	String	规则的请求转发方式 示例值：WRR
ListenerId	是	否	String	转发规则所属的监听器 ID 示例值：lbl-8cnjli93
RewriteTarget	是	是	RewriteTarget	转发规则的重定向目标信息 示例值：查看
HttpGzip	是	否	Bool	是否开启gzip 示例值：true
BeAutoCreated	是	否	Bool	转发规则是否为自动创建 示例值：false
DefaultServer	是	否	Bool	是否作为默认域名 示例值：true
Http2	是	否	Bool	是否开启Http2 示例值：false
ForwardType	是	否	String	负载均衡与后端服务之间的转发协议 示例值：HTTP
CreateTime	是	否	String	转发规则的创建时间 示例值：2024-01-22 14:36:12
TargetType	是	否	String	后端服务器类型 示例值：NODE
TargetGroup	是	是	BasicTargetGroupInfo	绑定的目标组基本信息；当规则绑定目标组时，会返回本字段 示例值：查看
WafDomainId	是	是	String	WAF实例ID 示例值：**
QuicStatus	否	是	String	QUIC状态 示例值：QUIC_INACTIVE
TrpcCallee	否	是	String	TRPC被调服务器路由，ForwardType为TRPC时有效 示例值：**
TrpcFunc	否	是	String	TRPC调用服务接口，ForwardType为TRPC时有效 示例值：**

BindItem

配置绑定关系

被如下接口引用：AssociateCustomizedConfig

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	配置绑定的CLB ID 示例值：lb-4d2yij93
ListenerId	是	是	String	配置绑定的监听器ID 示例值：lbl-ds2yij93
Domain	是	是	String	配置绑定的域名 示例值：foo.net
LocationId	否	是	String	配置绑定的规则 示例值：loc-jdhsji93

SubQuotaRsp

查询子账号配额返回描述

被如下接口引用：DescribeSubUinQuotas

名称	必选	允许NULL	类型	描述
SubUin	是	否	String	子账号Uin 示例值：110000004918
UsedQuota	是	否	Int64	子账号已使用配额 示例值：1
CurQuota	是	否	Int64	子账号当前配额 示例值：4
LastSetTime	是	否	String	子账号修改时间 示例值：2014-08-03 12:00:00

RuleHealth

一条转发规则的健康检查状态

被如下接口引用：DescribeTargetHealth

名称	必选	允许NULL	类型	描述
LocationId	是	否	String	转发规则ID 示例值：loc-di3lsr902
Domain	是	是	String	转发规则的域名 示例值：foo.net
Url	是	是	String	转发规则的Url 示例值：/url1
Targets	是	是	Array of TargetHealth	本规则上绑定的后端的健康检查状态 示例值：查看
FunctionTargets	否	是	Array of FunctionTarget	后端云函数的信息（私有云暂不支持） 示例值：查看

HealthCheck

健康检查信息。
注意，四层父规则相关参数 目前只有少量区域灰度支持。

被如下接口引用：CreateListener、CreateRule、DescribeListeners、DescribeRewrite、ModifyListener、ModifyRule

名称	必选	允许NULL	类型	描述
HealthSwitch	否	否	Int64	是否开启健康检查：1（开启），0（关闭）。 示例值：0
TimeOut	否	是	Int64	健康检查的响应超时时间（仅适用于四层监听器），可选值：2~60，默认值：2，单位：秒。响应超时时间要小于检查间隔时间。 示例值：2
IntervalTime	否	是	Int64	健康检查探测间隔时间，默认值：5，可选值：5~300，单位：秒。 示例值：5
HealthNum	否	是	Int64	健康阈值，默认值：3，表示当连续探测三次健康则表示该转发正常，可选值：2~10，单位：次。 示例值：3
UnHealthNum	否	是	Int64	不健康阈值，默认值：3，表示当连续探测三次不健康则表示该转发异常，可选值：2~10，单位：次。 示例值：3
HttpCode	否	是	Int64	健康检查状态码（仅适用于HTTP/HTTPS转发规则、TCP监听器的HTTP健康检查方式）。可选值：1~31，默认 31。 1 表示探测后返回值 1xx 代表健康，2 表示返回 2xx 代表健康，4 表示返回 3xx 代表健康，8 表示返回 4xx 代表健康，16 表示返回 5xx 代表健康。若希望多种返回码都可代表健康，则将相应的值相加。注意：TCP监听器的HTTP健康检查方式，只支持指定一种健康检查状态码。 示例值：8
HttpCheckPath	否	是	String	健康检查路径（仅适用于HTTP/HTTPS转发规则、TCP监听器的HTTP健康检查方式）。 示例值：/url1
HttpCheckDomain	否	是	String	健康检查域名（仅适用于HTTP/HTTPS转发规则、TCP监听器的HTTP健康检查方式）。 示例值：www.healthcheck.com
HttpCheckMethod	否	是	String	健康检查方法（仅适用于HTTP/HTTPS转发规则、TCP监听器的HTTP健康检查方式），默认值：HEAD，可选值HEAD或GET。 示例值：HEAD
CheckPort	否	是	Int64	自定义探测相关参数。健康检查端口，默认为后端服务的端口，除非您希望指定特定端口，否则建议留空。（仅适用于TCP/UDP监听器）。 示例值：8000
ContextType	否	是	String	自定义探测相关参数。健康检查协议CheckType的值取CUSTOM时，必填此字段，代表健康检查的输入格式，可取值：HEXETEXT：HEX为二进制数据，TEXT为文本数据，文本数据只支持ASCII可见字符。取值为HEX时，SendContext和RecvContext的字符只能在0123456789ABCDEF中选取且长度必须是偶数位。（仅适用于TCP/UDP监听器） 示例值：TEXT
SendContext	否	是	String	自定义探测相关参数。健康检查协议CheckType的值取CUSTOM时，必填此字段，代表健康检查发送的请求内容，只允许ASCII可见字符，最大长度限制500。（仅适用于TCP/UDP监听器）。 示例值：request-info
RecvContext	否	是	String	自定义探测相关参数。健康检查协议CheckType的值取CUSTOM时，必填此字段，代表健康检查返回的结果，只允许ASCII可见字符，最大长度限制500。（仅适用于TCP/UDP监听器）。 示例值：response-info
CheckType	否	是	String	自定义探测相关参数。健康检查使用的协议：TCP
HttpVersion	否	是	String	自定义探测相关参数。健康检查协议CheckType的值取HTTPpt，必传此字段，代表后端服务的HTTP版本：HTTP/1.0、HTTP/1.1；（仅适用于TCP监听器）

RsWeightRule

修改节点权重的数据类型

被如下接口引用：BatchModifyTargetWeight

名称	必选	允许NULL	类型	描述
ListenerId	是	否	String	负载均衡监听器 ID 示例值：lb-cuxwji93
LocationId	否	否	String	转发规则的ID，七层规则时需要此参数，4层规则不需要 示例值：loc-o8cnji93
Domain	否	否	String	目标规则的域名，提供LocationId参数时本参数不生效 示例值：www.demo.example.com
Url	否	否	String	目标规则的URL，提供LocationId参数时本参数不生效 示例值：/index
Targets	是	否	Array of Target	要修改权重的后端机器列表 示例值：查看
Weight	否	否	Int64	后端服务新的转发权重，取值范围：0~100。 示例值：10

InternetAccessible

网络计费模式，最大出带宽

被如下接口引用：CreateLoadBalancer、DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc、InquiryPriceCreateLoadBalancer、InquiryPriceModifyLoadBalancer、ModifyLoadBalancerAttributes

名称	必选	允许NULL	类型	描述
InternetChargeType	否	是	String	TRAFFIC_POSTPAID_BY_HOUR 按流量按小时后计费；BANDWIDTH_POSTPAID_BY_HOUR 按带宽按小时后计费； BANDWIDTH_PACKAGE 按带宽包计费（当前，只有指定运营商时才支持此种计费模式） 示例值：BANDWIDTH_POSTPAID_BY_HOUR

名称	必选	允许NULL	类型	描述
InternetMaxBandwidthOut	否	是	Int64	最大出带宽，单位Mbps，范围支持0到65535，仅对公网属性的LB生效，默认值 10 示例值：1
BandwidthpkgSubType	否	是	String	带宽包的类型，如SINGLEISP，私有云暂不支持 示例值：SINGLEISP

OwnerLabel

用户和标签对应关系

被如下接口引用：DescribeAppIdLabel

名称	必选	允许NULL	类型	描述
Owner	是	否	Uint64	用户AppId 示例值：1270000001
Label	是	否	String	集群标签 示例值：label1
SetType	是	否	String	集群标签类型，取值为L4_LAN_CLB，L4_WAN_CLB，L4_CLB，L7_LAN_CLB，L7_WAN_CLB，L7_CLB 示例值：L4_LAN_CLB

RuleTargets

HTTP/HTTPS监听器下的转发规则绑定的后端服务信息

被如下接口引用：DescribeTargets

名称	必选	允许NULL	类型	描述
LocationId	是	否	String	转发规则的 ID 示例值：loc-dl2kji93
Domain	是	否	String	转发规则的域名 示例值：wagncha.com
Url	是	否	String	转发规则的路径。 示例值：/url1
Targets	是	是	Array of Backend	后端服务的信息 示例值：查看
FunctionTargets	否	是	Array of FunctionTarget	后端云函数的信息（私有云暂不支持） 示例值：查看

TagInfo

负载均衡的标签信息

被如下接口引用：CreateLoadBalancer，DescribeLoadBalancerListByCertId，DescribeLoadBalancers，DescribeLoadBalancersForVpc

名称	必选	允许NULL	类型	描述
TagKey	是	否	String	标签的键 示例值：key-djx983xs
TagValue	是	否	String	标签的值 示例值：value-djx983xs

ConfigListItem

配置内容

被如下接口引用：DescribeCustomizedConfigList

名称	必选	允许NULL	类型	描述
UconfigId	是	否	String	配置ID 示例值：pz-di3kx902
ConfigType	是	否	String	配置类型 示例值：CLB
ConfigName	是	是	String	配置名字 示例值：cm-1
ConfigContent	是	否	String	配置内容 示例值：add_header aaa bbb;\r\n
CreateTimestamp	是	否	String	增加配置时间 示例值：1702303612
UpdateTimestamp	是	否	String	修改配置时间 示例值：1702303612

CertificateOutput

证书相关信息

被如下接口引用：DescribeListeners，DescribeRewrite

名称	必选	允许NULL	类型	描述
SSLMode	是	否	String	认证类型，UNIDIRECTIONAL：单向认证，MUTUAL：双向认证 示例值：UNIDIRECTIONAL
CertId	是	否	String	服务端证书的 ID，（兼容旧版版本，默认RSA证书） 示例值：AL2j93jo
CertCaId	是	是	String	客户端证书的 ID。 示例值：40ytl936
SmCertId	是	是	String	服务端SM证书的 ID。 示例值：fdv2dgxx
EccCertId	是	是	String	服务端ECC证书的 ID。 示例值：fdv2dgxx

ClusterItem

独占集群信息

被如下接口引用：CreateLoadBalancer，DescribeLoadBalancerListByCertId，DescribeLoadBalancers，DescribeLoadBalancersForVpc，ModifyLoadBalancerAttributes

名称	必选	允许NULL	类型	描述
ClusterId	是	否	String	集群唯一ID 示例值：cluste-jd9x30xs
ClusterName	否	是	String	集群名称 示例值：cluster-1
Zone	否	是	String	集群所在可用区，如ap-region1-1 示例值：ap-region1

LoadBalancer

负载均衡实例的信息

被如下接口引用：DescribeLoadBalancerListByCertId，DescribeLoadBalancers，DescribeLoadBalancersForVpc

名称	必选	允许NULL	类型	描述
LoadBalancerId	否	否	String	负载均衡实例 ID。 示例值：lb-fwzz93x
LoadBalancerName	否	否	String	负载均衡实例的名称。 示例值：Name
LoadBalancerType	否	否	String	负载均衡实例的网络类型： OPEN：公网属性，INTERNAL：内网属性。 示例值：OPEN
Forward	否	否	Uint64	负载均衡类型标识，1：负载均衡，0：传统型负载均衡。 示例值：1
Domain	否	是	String	负载均衡实例的域名，仅公网传统型负载均衡实例才提供该字段 示例值：www.aaa.com
LoadBalancerVips	否	是	Array of String	负载均衡实例的 VIP 列表。 示例值：[43.23.46.32]
Status	否	是	Uint64	负载均衡实例的状态，包括 0：创建中，1：正常运行。 示例值：1
CreateTime	否	是	String	负载均衡实例的创建时间。 示例值：2020-12-08 08:00:00
StatusTime	否	是	String	负载均衡实例的上次状态转换时间。 示例值：2020-12-08 08:00:00
ProjectId	否	否	Uint64	负载均衡实例所属的项目 ID，0 表示默认项目。 示例值：0
VpcId	否	是	String	私有网络的 ID 示例值：vpc-mj65wx2
OpenBgp	否	是	Uint64	高防 LB 的标识，1：高防负载均衡 0：非高防负载均衡。 示例值：0
Snat	否	是	Bool	在 2016 年 12 月前之前的传统型内网负载均衡都是开启了 snat 的。 示例值：false
Isolation	否	是	Uint64	0：表示未被隔离，1：表示被隔离。 示例值：0
Log	否	是	String	用户开启日志的信息，日志只有公网属性创建了 HTTP 、HTTPS 监听器的负载均衡才会有日志。 示例值：null
SubnetId	否	是	String	负载均衡实例所在的子网（仅对内网VPC型LB有意义） 示例值：subnet-bg1q09
Tags	否	是	Array of TagInfo	负载均衡实例的标签信息 示例值：查看
SecureGroups	否	是	Array of String	负载均衡实例的安全组 示例值：sg-hx6dyv9x
TargetRegionInfo	否	是	TargetRegionInfo	负载均衡实例绑定的后端设备的基本信息 示例值：查看
AnycastZone	否	是	String	anycast负载均衡的发布域，对于非anycast的负载均衡，此字段返回为空字符串 示例值：null
AddressIPVersion	否	是	String	IP版本，ipv4
NumericalVpcId	否	是	Uint64	数值形式的私有网络 ID 示例值：77599
VipIsp	否	是	String	负载均衡IP地址所属的ISP 示例值：BGP
MasterZone	否	是	ZoneInfo	主可用区 示例值：查看
BackupZoneSet	否	是	Array of ZoneInfo	备可用区 示例值：查看
IsolatedTime	否	是	String	负载均衡实例被隔离的时间 示例值：2022-02-12 12:15:08
ExpireTime	否	是	String	负载均衡实例的过期时间，仅对预付费负载均衡生效 示例值：2021-02-12 12:15:08
ChargeType	否	是	String	负载均衡实例的计费类型 示例值：POSTPAID_BY_HOUR
NetworkAttributes	否	是	InternetAccessible	负载均衡实例的网络属性 示例值：查看
PrepaidAttributes	否	是	LBChargePrepaid	负载均衡实例的预付费相关属性 示例值：查看
LogSetId	否	是	String	负载均衡日志服务CLS的日志集ID 示例值：c12fc818-e984-414a-b8f5-39858c4c5
LogTopicId	否	是	String	负载均衡日志服务CLS的日志主题ID 示例值：c12fc818-e984-414a-b8f5-39858c4c5
AddressIPv6	否	是	String	负载均衡实例的IPv6地址 示例值：2402:4e00:1000:4e00:0:920b:5519:d96d
ExtraInfo	否	是	ExtraInfo	暂时保留，一般用户无需关注。 示例值：查看

名称	必选	允许NULL	类型	描述
IsDDos	否	是	Bool	是否可响应高防包 示例值： false
ConfigId	否	是	String	负载均衡绑定的个性化配置ID 示例值： px-pbhuk3Dx
LoadBalancerPassToTarget	否	是	Bool	后端服务是否放通来自CLB的流量 示例值： false
ExclusiveCluster	否	是	ExclusiveCluster	内网独占集群 示例值： 查看
IPv6Mode	否	是	String	IP地址版本为ipv6时的字段有意义， IPv6Nat64
SnatPro	否	是	Bool	是否开启SnatPro 示例值： true
SnatIps	否	是	Array of SnatIp	开启SnatPro负载均衡后，SnatIp列表 示例值： 查看
SlaType	否	是	String	性能保障规格 示例值： null
IsBlock	否	是	Bool	vip是否被封堵 示例值： false
VipIspId	否	是	Int64	负载均衡IP地址所属的ISP的ID 示例值： 5
VipIspName	否	是	String	负载均衡IP地址所属的ISP 示例值： BGP
AttributeFlags	否	是	Array of String	属性标签列表 示例值： DeleteProtect
TgwSetLabels	否	是	Array of String	私有云专用，clb实例绑定的四层集群标签 示例值： ["14-label"]
StgwSetLabels	否	是	Array of String	私有云专用，clb实例绑定的七层集群标签 示例值： ["17-label"]
Zones	否	是	Array of String	私有网络内网负载均衡，就近接入模式下规则所指在的可用区 示例值： null
NfvInfo	否	是	String	CLB是否为NFV，空：不是，//nfv：七层是NFV。 示例值： null
IsBlockTime	否	是	String	封禁或解封时间 示例值： 2021-02-12 12:15:08
HealthLogSetId	否	是	String	负载均衡日志服务CLS的健康检查日志集ID 示例值： c32fc818-e984-414a-b8f5-3985b4c51111
HealthLogTopicId	否	是	String	负载均衡日志服务CLS的健康检查日志主题ID 示例值： c32fc818-e984-414a-b8f5-3985b4c52222
LocalBgp	否	是	Bool	IP类型是否是本地BGP 示例值： false
MixIpTarget	否	是	Bool	开启IPv6FullChain负载均衡7层监听器支持混绑IPv4/IPv6目标功能。 示例值： false
ClusterTag	否	是	String	7层独占标签。 示例值： FOR_L7
ClusterIds	否	是	Array of String	7层独占集群ID。 示例值： ["cluster-skdfhk30"]
VipIspAlias	否	是	String	负载均衡IP地址所属的ISP别名 示例值： BGP

QuotaData

主账号及子账号配额信息

被如下接口引用：DescribeSubUinQuotas

名称	必选	允许NULL	类型	描述
Type	是	否	Int64	配额类型（4:公网实例配额，7:内网实例配额） 示例值： 4
UsedQuota	是	否	Int64	已使用配额 示例值： 1
CurQuota	是	否	Int64	主账号配额 示例值： 3
SubQuota	是	是	Array of SubQuotaRsp	该类型的子账号配额列表 示例值： 查看
SubUsedTotalQuota	是	是	Int64	子账户使用配额总和 示例值： 5

CertListener

证书绑定的负载均衡监听器属性

被如下接口引用：DescribeListenerListByCertId

名称	必选	允许NULL	类型	描述
ListenerId	否	否	String	负载均衡监听器 ID 示例值： lbl-jd8k12x3
ListenerName	否	否	String	监听器名称 示例值： 监听器-门户网站
LBId	否	否	String	负载均衡ID 示例值： lb-jd8k3d0b
Protocol	否	否	String	监听器协议 示例值： TCP
Port	否	否	Int64	监听器端口 示例值： 80
SSLMode	否	否	String	认证类型，UNIDIRECTIONAL：单向认证，MUTUAL：双向认证 示例值： UNIDIRECTIONAL
CertId	否	否	String	证书id 示例值： jfdjk23x
CertCaId	否	否	String	客户端证书id 示例值： jfdjk23x
SniSwitch	否	否	Int64	是否开启SNI特性（本参数仅对于HTTPS监听器有意义） 示例值： 0
AddTimestamp	否	否	String	监听器的创建时间。 示例值： 2024-02-21 12:00:00

TargetCountForLoadBalancer

负载均衡实例及其绑定的后端服务总数

被如下接口引用：DescribeTargetCountForLoadBalancers

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	负载均衡ID 示例值： lb-di3kx902
TargetCount	是	否	Uint64	负载均衡实例绑定的后端服务总数 示例值： 2

CertList

客户端证书列表

被如下接口引用：DescribeCerts

名称	必选	允许NULL	类型	描述
OwnerUin	是	否	String	所有者 示例值： 110000004918
ProjectId	是	否	String	项目ID 示例值： 0
From	是	否	String	证书来源 示例值： upload
CertType	是	否	String	产品类型 示例值： SVR
ProductZhName	是	否	String	产品名称 示例值： zhangsan@gmail.com
Domain	是	否	String	项目域名 示例值： zhangsan@gmail.com
Alias	是	否	String	证书备注或名称 示例值： zhangsan1
Status	是	否	Int64	证书状态 示例值： 1
VulnerAbilityStatus	是	否	String	漏洞状态 示例值： INACTIVE
CertBeginTime	是	否	String	开始时间 示例值： 2024-07-27 16:31:29
CertEndTime	是	否	String	过期时间 示例值： 2025-07-27 16:31:29
ValidityPeriod	是	否	String	有效期 示例值： 12
InsertTime	是	否	String	入库时间 示例值： 2024-10-22 10:21:38
CertID	是	否	String	证书ID 示例值： lz4e5k1n
StatusName	是	否	String	状态名称 示例值： 已签证
ProjectInfo	是	否	ProjectInfo	项目信息 示例值： 查看
Cert	否	否	String	证书内容 示例值： -----BEGIN CERTIFICATE-----\r\nMIIEjTCCA3WgAwIBAgIQA4ZHUAVDv4ynuI3ILfo3TANBgkqhkiG9w0BAQsFADBy\r\nMQswCQYDVQQGEwJDTjEtMCsGA1UEChMoV0l1c3RlbiBHbG9iYWwgVHJ1c3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSAwHgYDVQQDExdXaVRUcnVzdCBHbG9iYWwgUm9vdCBHMzAeFw0yMDEwMDkwMzMxMDFaFw0yNTEwMDkwMzMxMDFaMDAxLjAsBgNVBAMTJXdpVFRydXMgR2xvYmFsIFJvb3QgRzMgU3ViIENBIFNNMjU2IDIwMjAgLSBHMzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCcwKAYIKwYBBQUHAgEWHGh0dHBzOi8vY3ByLndlLnRydXMuY29tL2NwczAfBgNVHSMEGDAWgBRHOhBnBCibVyYndJdiSLLmRpZ2ZZXJDzAdBgNVHQ4EFgQUMBsGA1UdEgQUMBKCEHd3cudHJ1c3QuY29tMA4GA1UdDwEB/wQEAwIBhjCCAQAGCisGAQQB1nkCBAIEgfEEge4A7AB1AMz7D2qFcQll4tiiq7E4sWMNZwRhAAABdNVBWuwAAAQDAEYwRAIgUWYWNlcnRuLmRpZ2ZlPWNpZXJDdmFsaWRhdGUtcjBpZHVhN1YuYnc3RBc2lhVkTUNBQQBuY1XMAIGA1UdIAQrMCkwCAYGZ4EMAQICMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQCJClcMKpxeK894dyXI8JLq/L4h8jTNYcLVM1eAnYynfS6tflgE5xbfUJBPdFKPJuNBWdhE3nYRngqnHAAMjJiu0bqGPYbgpnHYp8mJyetFYcnC9CZcjkqHmwTSpjXuFjbDLx/BXd1Q813TNXwv8aIkvXKfJSW2IHI3TZGmQbBE3oYcrDRWmBkqdNYKYcYnYOuRvokvT4+IaInSLkkKxw=\r\n-----END CERTIFICATE-----\r\n
SignCert	否	是	String	国密证书签名内容 示例值： -----BEGIN CERTIFICATE-----\r\nMIIEjTCCA3WgAwIBAgIQA4ZHUAVDv4ynuI3ILfo3TANBgkqhkiG9w0BAQsFADBy\r\nMQswCQYDVQQGEwJDTjEtMCsGA1UEChMoV0l1c3RlbiBHbG9iYWwgVHJ1c3QgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MSAwHgYDVQQDExdXaVRUcnVzdCBHbG9iYWwgUm9vdCBHMzAeFw0yMDEwMDkwMzMxMDFaFw0yNTEwMDkwMzMxMDFaMDAxLjAsBgNVBAMTJXdpVFRydXMgR2xvYmFsIFJvb3QgRzMgU3ViIENBIFNNMjU2IDIwMjAgLSBHMzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMCcwKAYIKwYBBQUHAgEWHGh0dHBzOi8vY3ByLndlLnRydXMuY29tL2NwczAfBgNVHSMEGDAWgBRHOhBnBCibVyYndJdiSLLmRpZ2ZZXJDzAdBgNVHQ4EFgQUMBsGA1UdEgQUMBKCEHd3cudHJ1c3QuY29tMA4GA1UdDwEB/wQEAwIBhjCCAQAGCisGAQQB1nkCBAIEgfEEge4A7AB1AMz7D2qFcQll4tiiq7E4sWMNZwRhAAABdNVBWuwAAAQDAEYwRAIgUWYWNlcnRuLmRpZ2ZlPWNpZXJDdmFsaWRhdGUtcjBpZHVhN1YuYnc3RBc2lhVkTUNBQQBuY1XMAIGA1UdIAQrMCkwCAYGZ4EMAQICMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQCJClcMKpxeK894dyXI8JLq/L4h8jTNYcLVM1eAnYynfS6tflgE5xbfUJBPdFKPJuNBWdhE3nYRngqnHAAMjJiu0bqGPYbgpnHYp8mJyetFYcnC9CZcjkqHmwTSpjXuFjbDLx/BXd1Q813TNXwv8aIkvXKfJSW2IHI3TZGmQbBE3oYcrDRWmBkqdNYKYcYnYOuRvokvT4+IaInSLkkKxw=\r\n-----END CERTIFICATE-----\r\n
SubjectAltName	是	是	Array of String	备用域名列表 示例值： ["domain2.com"]
CertAlgorithm	是	是	String	取值类型：rsa：ecc：sm2. 默认为 rsa 示例值： rsa

ExtraInfo

暂保留，一般用户无需关注。

被如下接口引用：DescribeLoadBalancerListByCertId，DescribeLoadBalancers，DescribeLoadBalancersForVpc

名称	必选	允许NULL	类型	描述
ZhTong	是	是	Bool	是否开通VIP直通 示例值： 0
TgwGroupName	是	是	String	TgwGroup名称 示例值： tg-1

BindDetailItem

绑定关系，包含监听器名字、协议、url、vport。

被如下接口引用：DescribeCustomizedConfigAssociateList

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	配置绑定的CLB ID 示例值：lb-4d2yji93
ListenerId	是	是	String	配置绑定的监听器ID 示例值：lbl-4qeyji93
Domain	是	是	String	配置绑定的域名 示例值：foo.net
LocationId	是	是	String	配置绑定的规则 示例值：loc-jdhxji93
ListenerName	是	是	String	监听器名字 示例值：lbl-1
Protocol	是	是	String	监听器协议 示例值：HTTP
Vport	是	是	Int64	监听器端口 示例值：80
Url	是	是	String	location的url 示例值：/loc1
UconfigId	是	是	String	配置ID 示例值：pz-h98dsl9dx

ListenerBackend

监听器上绑定的后端服务的信息

被如下接口引用：DescribeTargets

名称	必选	允许NULL	类型	描述
ListenerId	是	否	String	监听器 ID 示例值：lbl-dl3lx902
Protocol	是	否	String	监听器的协议 示例值：TCP
Port	是	否	Int64	监听器的端口 示例值：80
Rules	是	是	Array of RuleTargets	监听器下的规则信息（仅适用于HTTP/HTTPS监听器） 示例值：查看
Targets	是	是	Array of Backend	监听器上绑定的后端服务列表（仅适用于TCP/UDP/TCP_SSL监听器） 示例值：查看
EndPort	否	是	Int64	若支持端口段，则为端口段终束端口，若不支持端口段，则为0 示例值：80

SnatIp

SnatIp的信息结构

被如下接口引用：DescribeLoadBalancerListByCertId、DescribeLoadBalancers、DescribeLoadBalancersForVpc

名称	必选	允许NULL	类型	描述
SubnetId	是	否	String	私有网络子网的唯一标识，如subnet-jlix73io1 示例值：412
Ip	否	否	String	IP地址，如192.168.0.1 示例值：1.1.1.1

错误码

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 cor
rect."
    },
    "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
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。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。

错误码	说明
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
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
MissingParameter	缺少参数错误。
InvalidParameter.LBIdNotFound	负载均衡实例ID错误。
InvalidParameterValue.Range	参数取值范围错误。
InvalidParameter.RewriteAlreadyExist	转发规则已绑定重定向关系。

错误码	说明
InvalidParameter.SomeRewriteNotFound	一些重定向规则不存在。
InvalidParameter.LocationNotFound	查找不到符合条件的转发规则。
FailedOperation	操作失败
InvalidParameter.FormatError	参数格式错误。
InvalidParameterValue.Duplicate	参数值有重复。
ResourceInsufficient	资源不足
UnauthorizedOperation	未授权操作
InvalidParameterValue.InvalidFilter	Filter参数输入错误。
InvalidParameter	参数错误。
LimitExceeded	超过配额限制
InvalidParameter.PortCheckFailed	监听器端口检查失败，比如端口冲突。
InternalError	内部错误
InvalidParameter.ListenerIdNotFound	监听器ID错误。
InvalidParameterValue	参数取值错误
InvalidParameter.ProtocolCheckFailed	监听器协议检查失败，比如相关协议不支持对应操作。
InvalidParameterValue.Length	参数长度错误。
InvalidParameter.RegionNotFound	地域无效。