

负载均衡 常见问题 产品文档



腾讯云

【 版权声明 】

©2013-2021 腾讯云版权所有

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

【 商标声明 】



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

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

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

文档目录

常见问题

计费相关

负载均衡配置相关

健康检查异常排查

HTTPS 相关

WS/WSS 协议支持相关

HTTP/2 协议支持相关

常见问题

计费相关

最近更新时间：2021-08-26 16:07:52

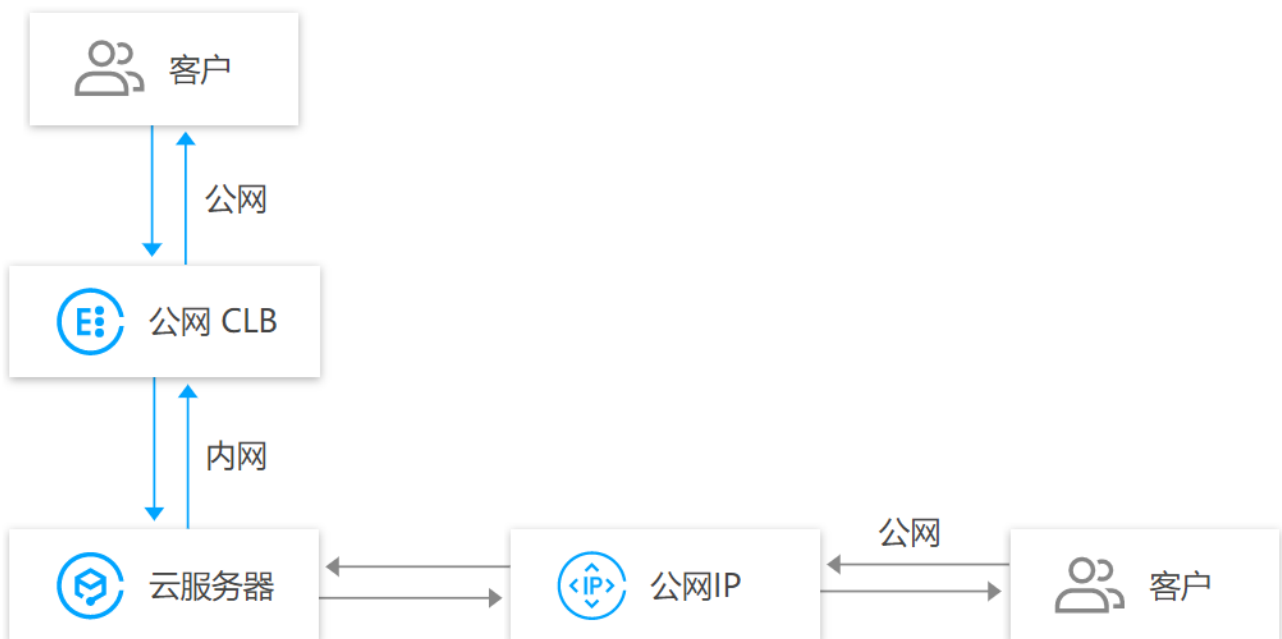
计费相关问题

- CLB 和后端云服务器（CVM）之间是使用公网还是内网通信？
- CLB 如何收费？
- 标准账户类型和传统账户类型可以互相切换吗？
- 跨地域绑定费用如何收取？
- CLB 的带宽上限是多少？

CLB 和后端云服务器（CVM）之间是使用公网还是内网通信？

不论您的账户类型是标准账户类型还是传统账户类型，CLB 和 CVM 之间都是使用内网流量。两种账户类型的网络流量路径皆如下所示：

- 客户端使用公网访问 CLB，CLB 通过内网将流量转发给 CVM，CVM 的响应仍然通过内网返回给 CLB，CLB 再回复给客户端。
- CVM 主动访问公网（或者直接通过公网 IP 被动访问）时，CVM 通过公网 IP（或弹性公网 IP）和客户端交互。



[\[回到顶部\]](#)

CLB 如何收费？

CLB 的费用根据不同类型的账户收费不同，详情请参见 [计费概述](#)。标准账户类型和传统账户类型的主要区别在于计费统计维度不同，其余业务访问和监控等都是是一致的。不同账户类型的差异请参见 [账户类型](#)。

- 标准账户类型的公网网络费用：访问 CLB 的公网流量，其公网网络费仅在 CLB 上收取，不在 CVM 上收取；通过公网 IP 访问的流量，其公网网络费仅在公网 IP 上收取，不在 CVM 上收取。
- 传统账户类型的公网网络费用：访问 CLB 和公网 IP 的公网流量，其公网网络费均 CVM 上收取，不在 CLB 和公网 IP 上收取。

[\[回到顶部\]](#)

标准账户类型和传统账户类型可以互相切换吗？

- 传统账户类型可以升级为标准账户类型。
- 标准账户类型不能回退为传统账户类型。

[\[回到顶部\]](#)

跨地域绑定费用如何收取？

仅在您的 CLB 使用了跨地域绑定功能时，才会收取跨域费用，否则就不收取。详情请参见 [跨地域绑定计费说明](#)。

- 跨地域1.0：在 CLB 上收取跨地域费用。
- 跨地域2.0：通过云联网来收取跨地域费用，CLB 上不再收取跨地域费用。

[\[回到顶部\]](#)

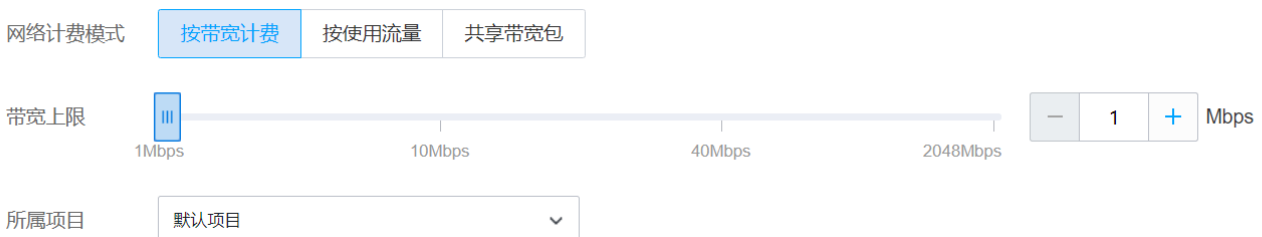
CLB 的带宽上限是多少？

- 标准账户类型：您在购买 CLB 时，需为 CLB 选择带宽上限，当业务带宽超过该上限时，CLB 会自动做丢包处理。

网络计费模式 按带宽计费 按使用流量 共享带宽包

带宽上限 Mbps

所属项目



-
- 传统账户类型：您在购买 CLB 时，无需为 CLB 选择带宽上限，CLB 的带宽受限于后端 CVM 的公网总带宽。

[\[回到顶部\]](#)

负载均衡配置相关

最近更新时间：2021-08-09 10:00:08

概念相关问题

- [四层负载均衡和七层负载均衡有什么区别？](#)
- [UDP 协议与 TCP 协议有什么区别？](#)
- [负载均衡 Cookies 会话保持方式的原理是什么？](#)
- [什么是后端服务器权重？](#)

健康检查相关问题

- [健康检查提示 CVM 实例异常该如何处理？](#)
- [为什么健康检查探测频率过高？](#)

访问相关问题

- [负载均衡中的 HTTP 重定向问题](#)
- [可以为哪些 TCP 端口执行负载均衡？](#)
- [发送 843 的 policy 请求（即 flash server 请求）时，没有返回策略文件，连接直接断掉，该如何处理？](#)
- [负载均衡是否可以直接获取 Client 端 IP？](#)
- [CVM 可通过配置内网型负载均衡，将流量从端口A转发回同一台服务器的其他端口吗？](#)
- [后端 CVM 需要公网带宽吗？是否会影响负载均衡的服务？](#)
- [客户端、服务器端 HTTP 版本不一致时，兼容版本说明](#)
- [支持 Gzip 兼容性](#)
- [负载均衡后端服务器的安全组应该怎么设置？怎样设置访问黑名单？](#)
- [设置访问黑名单](#)
- [负载均衡与后端服务器之间的通讯是走的内网还是外网？](#)
- [关于 Ping 负载均衡的 VIP 说明](#)
- [关于 Telnet 负载均衡监听端口的说明](#)
- [关于内网回环问题的说明](#)
- [关于同一个客户端通过不同的中间节点访问同一个后端 RS 的同一个端口时串流问题的说明](#)
- [为什么后端 CVM 配置安全组禁止公网访问，仅允许负载均衡访问，但却未生效？](#)
- [为什么负载均衡已配置监听器并绑定后端 CVM，当配置域名解析至后端 CVM 的 IP 并访问域名时，负载均衡的监控没有具体的信息？](#)
- [为什么没有创建843监听器，却可以 Telnet 通？](#)

四层负载均衡和七层负载均衡有什么区别？

- [四层均衡能力，是基于 IP + 端口的负载均衡。](#)

- 七层是基于应用层信息（如 HTTP 头部、URL 等）的负载均衡。

四到七层负载均衡，就是在对后台的服务器进行负载均衡时，依据四层的信息或七层的信息来决定怎么样转发流量。

例如，四层的负载均衡，就是通过发布三层的IP地址（VIP），然后加四层的端口号，来决定哪些流量需要做负载均衡，对需要处理的流量进行 NAT 处理，转发至后台服务器，并记录下这个 TCP 或者 UDP 的流量是由哪台服务器处理的，后续这个连接的所有流量都同样转发到同一台服务器处理。

七层的负载均衡，就是在四层的基础上，再考虑应用层的特征。

例如，同一个 Web 服务器的负载均衡，除了根据 VIP 和80端口辨别是否需要处理的流量，还可根据七层的 URL、浏览器类别、语言来决定是否要进行负载均衡。

七层负载均衡，也称为“内容交换”，也就是主要通过报文中的真正有意义的应用层内容，再加上负载均衡设备设置的服务器选择方式，决定最终选择的内部服务器。

七层负载均衡要根据真正的应用层内容选择服务器，只能先代理最终的服务器和客户端建立连接(三次握手)后，才可能接受到客户端发送的真正应用层内容的报文，然后再根据该报文中的特定字段，以及负载均衡设备设置的服务器选择方式，决定最终选择的内部服务器。负载均衡设备在这种情况下，更类似于一个代理服务器。负载均衡和前端的客户端以及后端的服务器会分别建立 TCP 连接。

[\[回到顶部\]](#)

UDP 协议与 TCP 协议有什么区别？

TCP 是面向连接的协议，在正式收发数据前，必须和对方建立可靠的连接。UDP 是面向非连接的协议，它在数据发送前不与对方先进行三次握手，而是直接进行数据包发送传送。UDP 协议主要适用于关注实时性而相对不注重可靠性的场景，如视频聊天、金融实时行情推送、DNS、物联网等。

[\[回到顶部\]](#)

负载均衡 Cookies 会话保持方式的原理是什么？

在 Cookie 插入模式下，CLB 将负责插入 Cookie，后端服务器无需作出任何修改。当客户进行第一次请求时，客户 HTTP 请求（不带 Cookie）进入 CLB，CLB 根据负载均衡算法策略选择后端一台服务器，并将请求发送至该服务器，后端服务器进行 HTTP 回复（不带 Cookie）被发回 CLB，然后 CLB 插入 Cookie，将 HTTP 回复（带 Cookie）返回到客户端。

当客户请求再次发生时，客户 HTTP 请求（带有上次 CLB 插入的 Cookie）进入 CLB，然后 CLB 读出 Cookie 里的会话保持数值，将 HTTP 请求（带有与上面同样的 Cookie）发到指定的服务器，然后后端服务器进行请求回复，由于服务器并不写入 Cookie，HTTP 回复将不带有 Cookie，回复流量再次经过进入 CLB 时，CLB 再次写入更新后的会话保持 Cookie。

[\[回到顶部\]](#)

什么是后端服务器权重？

用户可以指定后端服务器池内各 CVM 的转发权重，权重比越高的 CVM 将被分配到更多的访问请求，用户可以根据后端 CVM 的对外服务能力和情况来区别设定。

如果您同时开启了会话保持功能，那可能会造成对后端应用服务器的访问并不是完全相同的，建议您暂时关闭会话保持功能观察一下是否依然存在这种情况。

[\[回到顶部\]](#)

健康检查提示 CVM 实例异常该如何处理？

请按如下步骤进行排查：

- 确保您直接通过云服务器访问到您的应用服务。
- 确保后端服务器已开启了相应的端口。
- 检查后端服务器内部是否有防火墙之类的防护软件，可能导致负载均衡系统无法与后端服务器通讯。
- 检查负载均衡检查参数设置是否正确。
- 建议使用静态页面来健康检查。
- 检查后端的云服务器是否有高负载导致云服务器对外响应慢。
- 确保云服务器子机没有做 iptables 限制。

[\[回到顶部\]](#)

为什么健康检查探测频率过高？

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，原因如下：

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（如设置为15s探测一次）。

[\[回到顶部\]](#)

负载转发中的 HTTP 重定向问题

当浏览器访问网站 `http://example.com` 时，对服务器而言需要进行一次重定向，判断需要定向至根目录。而当浏览器访问网站 `http://example.com/` 时服务器会直接返回网站设置的根目录默认页面。同样的，假设

`http://cloud.tencent.com/movie` 被 URL 重写跳转到 `http://cloud.tencent.com/movie/` 上的话，则输入 `http://cloud.tencent.com/movie` 就会多一次 URL 重写的过程，在性能和时间上都有微小的损耗，但在结果上没有差别。若 `http://cloud.tencent.com/product` 被 URL 重写转跳到非 `http://cloud.tencent.com/product/` 同一页面上，则需要考虑是否在二级页面后添加 `/`。

在腾讯云负载均衡中，如果前后端端口号不一致时，为了避免 HTTP 重定向后导致端口号更改，访问二级页面需要加 `/` 保证页面的正常访问。

假设七层转发下，负载均衡实例监听80端口，后端服务器监听 8081 端口。此时客户端访问 `http://www.example.com/movie`，经由负载均衡转发至后端服务器，服务器收到发往 `http://www.example.com/movie` 的请求并会重定向到 `http://www.example.com:8081/movie/`（监听端口为8081），此时客户端访问失败（端口错误）。

因此，建议用户将访问请求改写为带 `/` 的二级页面如 `http://www.example.com/movie/`，这样可以避免 HTTP 重定向，减少一次不必要的判断，降低不必要的负载。如果必须使用 HTTP 重定向时，请保证负载均衡的监听端口和后端服务器的监听端口相同。

[\[回到顶部\]](#)

可以为哪些 TCP 端口执行负载均衡？

您可以为如下 TCP 端口执行负载均衡：21（FTP）、25（SMTP）、80（HTTP）、443（HTTPS），以及 1024 – 65535等端口。

[\[回到顶部\]](#)

发送 843 的 policy 请求（即 flash server 请求）时，没有返回策略文件，连接直接断掉，该如何处理？

负载均衡收到 843 的 policy 请求，会主动回复通用的 `crossdomain` 策略配置文件，如果出现没有返回策略文件，连接直接断掉的情况，可能是 flash server 请求不正确。

请确认发送正确的 flash server 的请求：`\0`。

注意：

这里需要以`\0`结尾，一共23个字节。`\0`是指一个 ASCII 码为 0 的符号，只占用一个字节。

正常的 843 返回结果如下图所示：

```
VM_02_sles10_64:/ # perl -e 'printf "<policy-file-request/>%c",0' | netcat -i 1 101.226.62.63 843
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "/xml/dtds/cross-domain-policy.dtd">
<!-- Policy file for xmlsocket://socks.example.com -->
<cross-domain-policy>
  <!-- This is a master socket policy file -->
  <!-- No other socket policies on the host will be permitted -->
  <site-control permitted-cross-domain-policies="master-only"/>
  <!-- Instead of setting to-ports="*", administrator's can use ranges and commas -->
  <!-- This will allow access to ports 123, 456, 457 and 458 -->
  <allow-access-from domain="*" to-ports="*" />
</cross-domain-policy>
```

[\[回到顶部\]](#)

负载均衡是否可以获取 Client 端 IP?

- IPv6 NAT64 负载均衡不支持获取 Client IP。
- 公网七层 IPv4 和 IPv6 负载均衡提供 X-Forwarded-For 的方式获取访问者真实 IP，负载均衡侧默认开启，需要后端服务做相应配置来获取 Client IP。详情请见 [如何获取客户端真实 IP](#)。
- 公网四层 IPv4 和 IPv6 负载均衡（TCP 协议）服务可以直接在后端 CVM 上获取来访者真实 IP 地址，无需进行额外的配置；内网四层负载均衡自从2016年10月24日起，新购的实例不再进行 SNAT 处理，支持直接从 server 端获取真实的 client IP，无需额外配置。

[\[回到顶部\]](#)

CVM 可通过配置内网型负载均衡，将流量从端口A转发回同一台服务器的其他端口吗？

不可以。对服务器 A（10.66.*.101）端口 a 的访问可通过内网型负载均衡将请求转发至服务器 B（10.66.*.102）的端口 b。但无法将流量转发至同一台服务器 A（10.66.*.101）的另一端口 b。

[\[回到顶部\]](#)

后端 CVM 需要公网带宽吗？是否会影响负载均衡的服务？

- 标准账户类型的负载均衡绑定的后端 CVM 无需配置公网带宽。
- 传统账户类型的负载均衡不收取任何的流量或带宽费用。负载均衡服务产生的公网流量费用，由绑定的后端的 CVM 收取，建议购买后端 CVM 时，公网带宽选择按使用流量计费，并设定合理的最高的带宽峰值上限，这样就无需关注 CLB 出口的总流量的涨跌。互联网 Web 业务的流量起伏较大，无法准确预测。若按带宽计费，带宽买多了不划算，买得太少，业务高峰期会出现丢包的情况。

[\[回到顶部\]](#)

客户端、服务器端 HTTP 版本不一致时，兼容版本说明

转发兼容性

- 前端（client 端），当前支持 HTTP1.0/1.1，向下兼容。
- 后端（server 端），当前腾讯云使用 HTTP1.0 协议，支持 HTTP1.0/1.1，向下兼容。

⚠ 注意：

HTTP/2 只在 HTTPS 中支持，且 client 及 server 端可以向下兼容。当前不支持 HTTP 协议。

支持 Gzip 兼容性

- 前端（client 端），当前支持 HTTP1.0/1.1 向下兼容。（用户无需配置，主流浏览器都支持 Gzip）
- 后端（server 端），在云服务器端，由于腾讯云内部全网支持 HTTP/1.1 协议，因此用户也无需配置，使用 Nginx 默认配置（HTTP/1.1）即可兼容。

⚠ 注意：

HTTP/2 只在 HTTPS 中支持，但 Gzip 可以用在腾讯云所支持的任意 HTTP 版本中。

[\[回到顶部\]](#)

负载均衡后端服务器的安全组应该怎么设置？怎样设置访问黑名单？

负载均衡安全组配置

若后端服务器设置了安全组规则，可能会出现负载均衡实例无法与其通信的状况。因此，在四层转发和七层转发下，建议后端服务器安全组均设置为全放通。若打开了安全组，并默认允许拒绝全协议全ip段的地址访问时，需要配置所有客户端 IP 到本机 IP 的安全组规则。

对于某些恶意 IP，可以设置把恶意IP加在安全组前排规则，禁止其访问后端服务器；再放通所有 IP（0.0.0.0）到本机服务端口，让正常客户端可以访问。（安全组规则是有顺序的，自顶而下进行匹配）

私有网络内的七层负载转发若设置了健康检查，必须把负载均衡 VIP 加入到后端服务器的安全组放通规则，否则健康检查可能失效。

设置访问黑名单

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：

⚠ 注意：

如下配置步骤有顺序要求，顺序相反会导致黑名单配置失效。

- 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。

- 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
0.0.0.0/0+port accept
```

关于安全组的更多说明，请参见 [后端云服务器安全组配置说明](#)。

[\[回到顶部\]](#)

负载均衡与后端服务器之间的通讯是走的内网还是外网？

负载均衡与后端服务器的通讯始终走内网，绑定的 CVM 有外网 IP 的情况下也一样。

[\[回到顶部\]](#)

关于 Ping 负载均衡的 VIP 说明

Ping 负载均衡的 VIP：由负载均衡集群响应，不会转发到后端的服务器。

- 公网负载均衡的 VIP 支持 Ping。
- 内网负载均衡的 VIP 仅支持来自本 VPC 的客户端 Ping，不支持其他 VPC、本地 IDC 的客户端 Ping（如使用云联网、对等连接等打通 VPC 的场景，建议您使用 telnet 来探测）。

[\[回到顶部\]](#)

关于 Telnet 负载均衡监听端口的说明

- 创建四层（TCP、UDP、TCP SSL）监听器后，如果不绑定后端服务器，则无法 Telnet 通监听端口；绑定后端服务器后，可以 Telnet 通监听端口。
- 创建七层（HTTP、HTTPS）监听器后，即使不绑定后端服务器，也可以 Telnet 通监听端口，由 CLB 代答。

[\[回到顶部\]](#)

关于内网回环问题的说明

内网负载均衡不支持同一个 CVM 既作为客户端又作为服务器，此时 CLB 看到的 Client IP 和 Server IP 是一样的，会导致访问不通。

当您的客户端需要同时作为服务器时，请至少绑定两个后端服务器。CLB 有自动避免回环的策略，当 Client A 访问负载均衡时，负载均衡会自动调度到非 Client A 的后端服务器上。

[\[回到顶部\]](#)

关于同一个客户端通过不同的中间节点访问同一个后端 RS 的同一个端口时串流问题的说明

问题现象

同一个客户端在同一时刻，通过不同的中间节点访问同一个 RS 的同一个端口会出现串流现象。具体场景如下：

- 同一个客户端，同时通过同一个 CLB 的四层、七层监听器，访问同一个 RS 的同一个端口。
- 同一个客户端，同时通过不同 CLB 的不同监听器，访问同一个 RS 的同一个端口。
- 访问内网 CLB 的客户端比较集中，且后端服务相同时，有较大概率会出现串流。（访问公网 CLB 的客户端来源较广，很少出现串流。）

问题原因

当前 CLB 会透传客户端 IP 到后端 RS，因此会导致 `client_ip:client_port -> vip:vport -> rs_ip:rs_port` 最终变为 `client_ip:client_port --> rs_ip:rs_port`。

解决方案

- 分散客户端：使用多个客户端发起访问。
- 收敛 CLB：在满足业务功能和容灾需求的前提下，减少 CLB 的实例、监听器个数。
- 分散后端服务端口：后端服务使用多个端口提供服务，避免后端端口集中。
- 分散部署：不同 CLB 绑定不同的后端服务端口，如 CLB1 绑定一组 CVM，CLB2 绑定另一组 CVM，两个 CLB 同时提供访问。

[\[回到顶部\]](#)

为什么后端 CVM 配置安全组禁止公网访问，仅允许负载均衡访问，但却未生效？

若需要通过 CLB 访问后端 CVM，需要后端 CVM 和 CLB 两个安全组均放通公网访问，建议先把后端 CVM 的安全组仅放通 CLB 的 VIP 公网访问，CLB 的安全组按需放通公网访问 IP。

[\[回到顶部\]](#)

为什么负载均衡已配置监听器并绑定后端 CVM，当配置域名解析至后端 CVM 的 IP 并访问域名时，负载均衡的监控没有具体的信息？

需通过负载均衡进行访问，才有具体的监控信息，可配置域名解析至负载均衡的 VIP 并访问域名，即可在负载均衡的监控中查看具体的信息。

[\[回到顶部\]](#)

为什么没有创建843监听器，却可以 Telnet 通？

为满足部分用户重置访问 Flash 的需求，CLB 默认放通了843端口。若您想关闭该端口，请配置 TCP:843 监听器后，不绑定后端服务器即可。

[\[回到顶部\]](#)

健康检查异常排查

最近更新时间：2021-09-01 15:04:20

负载均衡（CLB）通过健康检查来判断后端服务的可用性。若您遇到健康检查异常，可参考以下方式进行排查。

说明：

- 当健康检查探测到异常时，CLB 将不再向异常后端服务转发流量。
- 当健康检查探测到所有后端服务都有异常时，请求将会被转发给所有后端服务。
- 健康检查原理可参考 [健康检查](#)。

检查后端服务器的公网带宽

- 传统账户类型，负载均衡绑定的后端 CVM 需要配置公网带宽，否则会导致健康检查异常。因为该账户的带宽属性在 CVM 上，而非 CLB 上。
- 标准账户类型，负载均衡绑定的后端 CVM 无需配置公网带宽，且不会影响负载均衡服务。

说明：

- 若您无法确定账户类型，请参见 [判断账户类型](#)。
- 传统账户类型的负载均衡不收取任何流量或带宽费用。负载均衡服务产生的公网流量费用，由绑定的后端 CVM 收取。
- 您可在不分配公网 IP 的情况下，为 CVM 购买公网带宽。

检查安全组配置

检查负载均衡实例是否开启安全组默认放通功能。如果未开启，则需在 CVM 的安全组上放通来源 IP。如果您的 CLB 服务支持任意 IP 的访问，则在安全组的入站规则中配置来源 IP 为 0.0.0.0/0。详情请参考 [配置负载均衡安全组](#)。

检查四层监听器

说明：

- 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，状态为异常时的排查方法如下：

- 确定 CLB 后端服务器是否配置了安全组导致影响服务。后端服务器可通过安全组进行访问控制从而保证服务正常运行，详情请参考 [后端云服务器安全组配置说明](#)。
- 使用 netstat 命令，检查后端服务器的端口是否有进程在监听。若未发现进程，则重新启动服务。

检查七层协议

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

- 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 之间的正常通信。

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
```

如果可以看到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。

- 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，本例为：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信。

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 系统可以在运行输入firewall.cpl命令关闭。
 - Linux 系统可以输入/etc/init.d/iptables stop命令关闭（CenOS 7.x 系统请运行 systemctl stop firewalld命令）。
- 检查负载均衡健康检查参数设置是否正确，建议参考 [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。不建议使用 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。
- 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。
- 如果同时开启了 TCP 的快速回收 (tcp_tw_recycle) 和时间戳 (tcp_timestamps) 可能导致健康检查异常，建议关闭 tcp_tw_recycle，详见 [原因分析](#)。

健康检查探测频率过高

控制台设置5s接收1次探测包，实际后端 RS 发现1s内收到1次甚至多次健康检查请求，导致健康检查探测频率过高的原因主要是和负载均衡的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，再转发给云服务器。健康检查探测是在 CLB 的各个后端物理机上分别进行探测，因此，CLB 实例设置5s1次的探测请求时，实际上 CLB 后端的每台物理机都会每5s发送一次探测。此时后端云服务器上可能会在5s中收到4次探测请求。

该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，那么仅此台机器不再转发流量，另外7台仍然正常转发流量。

如果您的业务对负载敏感性高，高频率的健康检查探测可能会对正常业务访问造成影响，您可以通过增大探测时间间隔的方式来降低对业务的影响（例如设置为15s探测一次）。

HTTPS 相关

最近更新时间：2021-08-18 16:27:28

HTTP 相关问题

- [HTTPS 支持的加密套件有哪些？](#)
- [HTTPS 支持哪些版本的SSL/TLS安全协议？](#)
- [HTTPS 监听使用什么端口？](#)
- [为什么需要 HTTPS 双向认证？](#)
- [为什么 HTTPS 协议实际产生的流量会比账单流量多一些？](#)
- [添加 HTTPS 监听器后，负载均衡到后端云服务器间的请求是否依然通过 HTTP 协议传输？](#)

证书问题

- [CLB 目前支持哪些类型的证书？](#)
- [一个监听器可以绑定多少个 HTTPS 证书？](#)
- [一个证书可以应用于多少个负载均衡器，多少个监听器？](#)
- [如何上传证书？](#)
- [证书区分地域吗？](#)
- [证书需要上传到后端 CVM 吗？](#)
- [证书过期后如何处理？](#)
- [添加证书报错如何处理？](#)

HTTPS 支持的加密套件有哪些？

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305:DHE-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

[\[回到顶部\]](#)

HTTPS 支持哪些版本的SSL/TLS安全协议？

负载均衡 HTTPS 目前支持的 ssl_protocols: TLSv1、TLSv1.1、TLSv1.2、TLSv1.3。

[\[回到顶部\]](#)

HTTPS 监听使用什么端口？

不强制，建议使用443端口。

[\[回到顶部\]](#)

为什么需要 HTTPS 双向认证？

有些客户对数据安全要求较高，如涉及到金融服务的客户等。他们不仅需要在服务端进行 HTTPS 认证，在客户端也需要进行 HTTPS 认证，为了满足这些客户的需求，我们推出 HTTPS 双向认证功能。

[\[回到顶部\]](#)

为什么 HTTPS 协议实际产生的流量会比账单流量多一些？

如果用户使用 HTTPS 协议，将会使用一些流量用于协议握手，因此其实际产生的流量会比账单流量更多一些。

[\[回到顶部\]](#)

添加 HTTPS 监听器后，负载均衡到后端云服务器间的请求是否依然通过 HTTP 协议传输？

是的。添加 HTTPS 监听器后，客户端到负载均衡之间的请求将经过HTTPS协议加密，而负载均衡到后端云服务器依然通过HTTP协议传输，因此后端云服务器无需做SSL配置。

[\[回到顶部\]](#)

CLB 目前支持哪些类型的证书？

目前支持服务器证书和 CA 证书的上传，服务器证书需要上传证书内容和私钥，CA 证书只需要上传证书内容；这两种类型的证书都只支持 PEM 编码格式的上传。

[\[回到顶部\]](#)

一个监听器可以绑定多少个 HTTPS 证书？

如果用户使用 HTTPS 单向认证，则一个监听只能绑定一个服务器证书；若用户使用 HTTPS 双向认证，则一个监听需要绑定一个服务器证书 + 一个 CA 证书。

[\[回到顶部\]](#)

一个证书可以应用于多少个负载均衡器，多少个监听器？

一个证书可以应用于一个或多个负载均衡器，或多个监听器。

[\[回到顶部\]](#)

如何上传证书？

可以通过 API 或负载均衡控制台两种方式上传。

[\[回到顶部\]](#)

证书区分地域吗？

区分。考虑到安全和性能，目前用户的证书如需要在多个地域使用，就需要在多个地域上传。

[\[回到顶部\]](#)

证书需要上传到后端 CVM 吗？

不需要，负载均衡 HTTPS 提供证书管理系统管理和存储用户证书，证书不需要上传到后端 CVM，用户上传到证书管理系统的私钥都会加密存储。

[\[回到顶部\]](#)

证书过期后如何处理？

当前证书过期后，需要用户手动更新证书。

[\[回到顶部\]](#)

添加证书报错如何处理？

可能是私钥内容错误，需要用户替换为新的满足需求的证书。

[\[回到顶部\]](#)

WS/WSS 协议支持相关

最近更新时间：2021-08-09 11:07:20

产品内容

- [什么是 WS/WSS?](#)
- [为什么要使用 WS/WSS?](#)

产品购买

- [WS/WSS 如何收费?](#)

产品实施

- [如何在 CLB 上开启 WS/WSS?](#)
- [支持 WS/WSS 的地域有哪些?](#)

什么是 WS/WSS?

WebSocket 是一种在单个 TCP 连接上进行全双工通讯的协议。

WebSocket 使得客户端和服务端之间的数据交换变得更加简单，允许服务端主动向客户端推送数据。在 WebSocket API 中，浏览器和服务器只需要完成一次握手，两者之间就直接可以创建持久性的连接，并进行双向数据传输。

[\[回到顶部\]](#)

为什么要使用 WS/WSS?

在 WebSocket 出现之前，客户端获取服务器数据只能通过轮询的方式从服务器拉取(Pull)数据。

这样的数据交换方式存在两个最突出的问题：

1. 效率低。当客户端需要实时数据时，需要频繁的发起 Ajax 请求拉取数据。
2. 服务器无法主动推(Push)数据。

为解决这些问题，WebSocket 诞生了。WebSocket 是伴随 HTML5 发布的一种新协议。它实现了浏览器与服务器全双工通信(full-duplex)，可以传输基于消息的文本和二进制数据。从协议层面上解决了 HTTP 的上述难题。

WebSocket 的主要优点包括：

1. 更小的控制开销。连接建立后，用于控制的包头较小。相对于 HTTP 请求每次都要携带完整的头部，此项开销大大降低。
2. 更强的实时性。WebSocket 是全双工协议，服务器可实时推动数据给客户端。

3. 保持连接状态。

[\[回到顶部\]](#)

WS/WSS 如何收费？

CLB 默认支持 WS/WSS，不收取额外费用。

[\[回到顶部\]](#)

如何在 CLB 上开启 WS/WSS？

默认开启，无需额外配置。

监听器监听在 HTTP，则默认支持 WS；监听器监听 HTTPS，则默认支持 WSS。

使用 WSS 时，CLB 会进行 SSL 卸载。

[\[回到顶部\]](#)

支持 WS/WSS 的地域有哪些？

目前所有地域均已支持 WS/WSS 协议。

[\[回到顶部\]](#)

HTTP/2 协议支持相关

最近更新时间：2021-09-01 11:12:19

产品内容

- [什么是 HTTP/2?](#)
- [为什么要使用 HTTP/2?](#)

产品购买

- [如何收费?](#)

产品实施

- [如何在 CLB 上开启 HTTP/2?](#)
- [支持的 HTTP/2 地域有哪些?](#)

什么是 HTTP/2?

- HTTP/2 (超文本传输协议第2版), 是 HTTP 协议的第二个主要版本, 应用于 Web 服务。
- HTTP/2 的设计目标是, 解决 HTTP1.X 中的性能问题, 更有效的利用网络资源, 减少网络应用的延迟。
- HTTP/2 向下兼容 HTTP1.X。

[\[回到顶部\]](#)

为什么要使用 HTTP/2?

相比于 HTTP1.X, HTTP/2 响应更快, 效率更高, 具备如下优势:

- 多路复用: 并行处理, 响应更快。
- 服务端推送: 服务端主动推动客户端所需资源, 减少请求次数。
- 更多功能包括: 流量控制、请求优先级、头部压缩、二进制分帧等。

[\[回到顶部\]](#)

如何收费?

CLB 支持 HTTP/2 不收取额外费用。

[\[回到顶部\]](#)

如何在 CLB 上开启 HTTP/2?

注意：

1. HTTP 监听器不支持 HTTP/2。主流浏览器和 WebServer 仅支持基于 TLS 的 HTTP/2 协议。
2. CLB 与后端服务器之间仍使用 HTTP1.X 协议。

1. 在 HTTPS 监听器开启 HTTP/2

- 负载均衡型实例：您可以选择开启或关闭 CLB 对 HTTP/2 的支持，详情请参考 [配置 HTTPS 监听器](#)。
- 传统型负载均衡型实例：2018年4月之前创建的 HTTPS 监听器无法启用 HTTP/2，2018年4月后创建的 HTTPS 监听器可以启用 HTTP/2。传统型负载均衡不支持修改 HTTP/2 的开关。

2. 客户端访问时共识协议

当客户端访问已启动 HTTP/2 的监听器时，在 HTTPS 的握手过程中，会进行协议版本的协商。客户端使用 ALPN（应用层协议协商）通知服务端自身可支持的协议列表，服务端根据协议列表选择 HTTP/2 或 HTTP1.X，若客户端不支持 HTTP/2，则自动向下兼容，无需额外配置。

[\[回到顶部\]](#)**支持的 HTTP/2 地域有哪些？**

全部地域均已支持 HTTP/2。

[\[回到顶部\]](#)