负载均衡

常见问题

产品文档

腾讯云

文档目录

常见问题
负载均衡配置相关

最近更新时间：2018-06-13 09:59:47

1. 健康检查提示 CVM 实例异常该如何处理

请按以下步骤进行排查：

- 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。

2. 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：这里需要以\0结尾，一共 23 个字节。这里的\0是指一个 accii 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>
```

3. 能否支持获取客户端真实 IP？

腾讯云的 IP 获取能力自动启用，在 X-forwarded-for 的方式下，可获取真实客户端 IP。

4. 可以为哪些 TCP 端口执行负载均衡？

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

5. 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 根据负载平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，恢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。

6. 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。 比如四层的负载均衡，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，比如同一个 Web 服务器的负载均衡，除了根据 VIP 加 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，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。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。

7. 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。

8. 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，那么有可能会造成对后端应用服务器的访问并不是完全相同的，建议您可以暂时关闭会话保持功能再观察一下是否依然存在这种情况。

9. 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。

10. 后端 CVM 需要外网带宽吗？是否会影响负载均衡的服务？

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线，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。

11. 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。但若 `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。

12. 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：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： 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

13. 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，还要注意必须把负载均衡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 clientIP 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：

- 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
```

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。***

关于安全组的更多说明，可见后端云服务器的访问控制

14. CLB 是否可以直接获取 client 端 IP？

公网七层负载均衡提供 X-Forwarded-For 的方式获取访问者真实 IP，LB 侧默认开启，需要后端服务做相应配置来获取 client IP。详情请见负载均衡七层转发获取来访真实 IP 的方法。

公网四层负载均衡（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。

15. 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，这是什么原因呢？

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LB后端物理机上，再转给云服务器。 健康检查探测是在 LB 的后端物理机上，各自探测的。因此，LB 实例设置5秒1次的探测请求，实际上 LB 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 LB 实例所在集群有8台物理机，那么每台机器 5 s 发送一次请求，后端主机可能会在 5 s 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。比如 LB 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（ 比如设置为 15 s 探测一次）。

16. CLB 与后端服务器之间的通讯是走的内网还是外网？

CLB 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。

HTTPS 相关

最近更新时间：2018-03-28 17:21:41

1. 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

2. 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

3. HTTPS 监听使用什么端口？

不强制，建议使用443端口。

4. 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。

5. 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。

6. 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。

7. 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。

8. 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。

9. 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。

10. 证书如何上传？

可以通过API或负载均衡控制台两种方式上传。

11. 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。

12. 证书上传后是否可以删除？

暂时不提供删除功能。

13. 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。

14. 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。

15. 添加证书报错怎么办？

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。

WS/WSS 协议支持相关

最近更新时间：2018-06-01 17:12:02

产品内容

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 使得客户端和服务器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。

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。

产品购买

WS/WSS 如何收费？

CLB 默认支持 WS/WSS，不收取额外费用。

产品实施

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。

支持 WS/WSS 的地域有哪些？

目前 **所有地域** 均已支持 WS/WSS 协议。

公网无固定 IP 型 CLB 升级相关

最近更新时间：2018-10-15 14:35:34

为什么要升级公网无固定 IP 型负载均衡？

升级的目的是为了给您提供更优质的服务。公网无固定 IP 型负载均衡为腾讯云早期的负载均衡版本，现在腾讯云已推出性能更强、特性更多、服务更健壮的负载均衡服务，支持四层（TCP/UDP）和七层（HTTP/HTTPS）转发规则，并且具备监控告警、安全组、日志管理等功能。

升级对我有什么影响？我需要做什么？

此次升级为平滑升级，业务无感知，相关域名、转发规则、实例名称等均会保留，升级后价格为 0.02 元 / 小时，负载均衡实例 ID 会改变。
用户无需做任何操作，腾讯云会将有服务的公网无固定 IP 型负载均衡升级，并在 2018 年 11 月 15 日统一回收无服务的公网无固定 IP 型负载均衡。

判断升级或回收的标准是什么？

- 升级对象为有服务（有转发规则且绑定云服务器）的公网无固定 IP 型负载均衡。
- 回收对象为全网无服务（没有转发规则或者未绑定云服务器）的公网无固定 IP 型负载均衡。

我能不能迁到应用型 CLB，而不是传统型 CLB？

如果您需要保留公网无固定 IP 型 CLB 的域名，则必须使用传统型 CLB；如果您想使用应用型 CLB，可以直接在购买页购买并配置。

为什么公网无固定 IP 型 CLB 转发协议是 HTTP，升级后的传统型公网 CLB 是 TCP？

公网无固定 IP 型 CLB 的 HTTP 监听器实现机制，与传统型公网 CLB 的 HTTP 监听器不完全一致。为了能够平滑地将无固定 IP 型负载均衡升级为传统型公网负载均衡，升级后的监听器协议采用 TCP。在功能上，升级后的 TCP 协议能覆盖老版本的能力，同时您也可以启用功能更完备的 HTTP/HTTPS 协议。

补偿的代金券有哪些使用限制？

代金券为 CLB 定向代金券，只能在购买或按小时结算 CLB 时使用，对购买 CLB 的类型、规格无限制。一张代金券可多次使用，且需在有效期内使用。

注意：
若您有任何问题，请在 工单系统 提交工单与我们联系。